# EXHIBIT L

# DEPARTMENT OF HOMELAND SECURITY

## HOMELAND SECURITY INVESTIGATIONS

### REPORT OF INVESTIGATION

~~OFFICIAL USE ONLY | LAW ENFORCEMENT SENSITIVE~~

02/26/2018 09:41 EST



**CASE NUMBER**
(b)(7)(E)

**CASE OPENED**
8/24/2010

**CURRENT CASE TITLE**
1 BY LAND. 2 BY SEA

**REPORT TITLE**
INTERVIEW: (b)(6);(b)(7)(C)
(b)(6);(b)(7)(C) (OTM POE)

**REPORTED BY**
(b)(6);(b)(7)(C)
SPECIAL AGENT

**APPROVED BY**
(b)(6);(b)(7)(C)
OI GRP SUPERVISOR

**DATE APPROVED**
4/22/2013

**SYNOPSIS**

Intelligence information has linked (b)(6);(b)(7)(C) and (b)(6);(b)(7)(C) to multiple methamphetamine, cocaine, marijuana, currency, and ammunition smuggling events. This investigation will focus on (b)(6);(b)(7)(C) as mid-level DTO members in an effort to target current narcotics smugglers and to disrupt and dismantle their corresponding DTO. On 11/06/2012, at approximately 1632 hours, (b)(6);(b)(7)(C) crossed into the United States as a pedestrian through the Otay Mesa Port of Entry. (b)(6);(b)(7)(C);(b)(7)(E) (b)(7)(E) Customs & Border Protection contacted Homeland Security Investigations, who in turn responded to the port to conduct an interview. This report documents the interview.

| Current Case Title | ROI Number | Date Approved |
|---|---|---|
| 1 BY LAND. 2 BY SEA | (b)(7)(E) | 4/22/2013 |



This document is loaned to you for official use only and remains the property of the Department of Homeland Security. Any further request for disclosure of this document or information contained herein should be referred to HSI Headquarters together with a copy of the document.

# DEPARTMENT OF HOMELAND SECURITY

## HOMELAND SECURITY INVESTIGATIONS

### REPORT OF INVESTIGATION

~~OFFICIAL USE ONLY | LAW ENFORCEMENT SENSITIVE~~



## DETAILS OF INVESTIGATION

DETAILS OF THE INVESTIGATION:

CUSTOMS & BORDER PROTECTION STOP OF (b)(6);(b)(7)(C)

On 11/06/2012, at approximately 1632 hours, (b)(6);(b)(7)(C) crossed into the United States as a pedestrian through the Otay Mesa Port of Entry (POE). (b)(6);(b)(7)(C);(b)(7)(E) A Customs & Border Protection (CBP) officer contacted Homeland Security Investigations (HSI) Special Agent (S/A) (b)(6);(b)(7)(C) S/A (b)(6);(b)(7)(C) and HSI S/A (b)(6);(b)(7)(C) responded to the POE.

INTERVIEW OF (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C);(b)(7)(E)

| Current Case Title | ROI Number | Date Approved |
|---|---|---|
| 1 BY LAND. 2 BY SEA | (b)(7)(E) | 4/22/2013 |



This document is loaned to you for official use only and remains the property of the Department of Homeland Security. Any further request for disclosure of this document or information contained herein should be referred to HSI Headquarters together with a copy of the document.

# DEPARTMENT OF HOMELAND SECURITY

## HOMELAND SECURITY INVESTIGATIONS

### REPORT OF INVESTIGATION

~~OFFICIAL USE ONLY | LAW ENFORCEMENT SENSITIVE~~



(b)(6);(b)(7)(C);(b)(7)(E)

UNDEVELOPED LEADS: To Be Determined By DSAC, San Ysidro, CA.

| Current Case Title | ROI Number | Date Approved |
|---|---|---|
| 1 BY LAND. 2 BY SEA | (b)(7)(E) | 4/22/2013 |



This document is loaned to you for official use only and remains the property of the Department of Homeland Security. Any further request for disclosure of this document or information contained herein should be referred to HSI Headquarters together with a copy of the document.

# EXHIBIT M

~~DELIBERATIVE PROCESS PRIVILEGE//PRE-DECISIONAL//FOR OFFICIAL USE ONLY~~

# Civil Rights/Civil Liberties Impact Assessment

# Border Searches of Electronic Devices

December 29, 2011

Reviewing Official:
Margo Schlanger
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
(202) 357-7765

**Table of Contents**

**I. Introduction ..... 1**
**II. Facts ..... 4**
A. Primary Inspection and Referral ..... 4
B. Secondary Inspection and Electronic Device Searches ..... 6
**III. Legal and Policy Analysis ..... 9**
A. Authority to Search Electronic Devices at the Border ..... 10
B. First Amendment ..... 17
C. Equal Protection and Religious/Ethnicity Discrimination ..... 18
D. Time Limits ..... 20
E. Privileged Materials ..... 21
F. Improved Notice about Redress ..... 22
**IV. Conclusion ..... 22**

~~DELIBERATIVE PROCESS PRIVILEGE//PRE-DECISIONAL//FOR OFFICIAL USE ONLY~~

# I. Introduction

This Civil Rights/Civil Liberties Impact Assessment, conducted by the Office for Civil Rights and Civil Liberties (CRCL) of the Department of Homeland Security (DHS), focuses on the Department's policies guiding the border search of electronic devices, how those searches occur, and related civil rights and civil liberties issues. Without finding any existing constitutional violation in policy or practice, we make several recommendations to further safeguard travelers' civil rights and civil liberties with respect to electronic device searches by improving accountability and oversight structures, and providing better notice to travelers about the availability of redress if they have complaints related to such searches.

The issue is an important one, even though it affects only a very small proportion of the many millions of travelers who enter the United States each month. The table below summarizes the relevant statistics; as it shows, only a few hundred people each month are subjected to any kind of electronic device search (which vary in their comprehensiveness), and of that number, only a small minority have their electronic devices detained for any length of time.

**Table: CBP Electronic Device Searches—Number Impacted**

| | Monthly Averages | |
|---|---|---|
| | FY 2009 | FY 2010 |
| Travelers through all Ports of Entry | 21,641,667 | 29,357,163 |
| Travelers in Secondary Screening | 466,667 | 518,059 |
| Travelers Subjected to Electronic Device Searches | 302 | 383 |
| Detentions or Seizures of Electronic Devices | 25 | 16 |

Notwithstanding the low rate of searching, we recognize that for the several thousand people affected each year, electronic devices searches may pose a significant concern. In August 2009, Secretary Napolitano announced revised U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) policies with respect to searches of electronic devices in response to public and congressional concern, and as part of the continuing evolution of border security policy. At the same time, the Secretary 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 policies might be improved. For this resulting Civil Rights/Civil Liberties Impact Assessment, we have reviewed the CBP and ICE policies guiding the border search of electronic devices; consulted with CBP and ICE personnel to understand implementation of the policies and ascertain how searches occur; and considered legal, policy, and practical concerns raised by advocacy groups and the public. Because border searches of electronic devices ordinarily occur only in conjunction with a secondary inspection, this Impact Assessment first briefly discusses the process by which CBP refers travelers to secondary inspection. It then focuses on the electronic device search policies and their implementation, describing the relevant legal authority and assessing the impact on individual rights. Finally, the Impact Assessment offers policy advice to Department and Component leadership about how to improve accountability, oversight, and notice about redress. This assessment does not address training. CBP's relevant training content and processes were the

subject of a separate review jointly conducted by the DHS Privacy Office, CRCL, and CBP, issued August 20, 2010, and available at http://www.dhs.gov/xlibrary/assets/privacy/privacy-report-cbp-training-border-searches-electronic-devices.pdf.

In addition, CBP's Office of Internal Affairs, Management Inspection Division (MID), conducted its own review of CBP's electronic device search policies. That review, completed in November 2010, found that while CBP officers were executing searches of electronic devices and documents with appropriate care and infrequency, there were some conditions warranting additional attention. Specifically, and relevant to the current analysis, MID found that:

1) CBP's system for entering the results of electronic device searches did not allow analysts to accurately identify incidents and seizures related to electronic device search activity, thus hindering CBP's ability to monitor and evaluate performance and making it difficult to provide accurate operational data concerning searches of electronic devices;
2) some CBP supervisors and officers were confused about their obligation to track information related to searches of electronic devices that had been transferred to ICE for forensic analysis versus those that had been transferred to ICE for translation or encryption services;
3) many supervisors and officers incorrectly believed that supervisory approval was required for device searches, and this belief hindered CBP's enforcement mission by discouraging officers from searching electronic devices; and
4) many supervisors interpreted CBP's supervisory presence requirement to require only that a supervisor be somewhere in the general area, not that a supervisor be physically present for the search.[1]

CBP addressed concerns (2)-(4) to MID's satisfaction in a Muster issued in October 2010[2] and is in the process of amending data systems to address the first concern. We discuss the relevant provisions of these CBP policies in detail and provide additional information regarding MID's findings and recommendations later in this report (*see infra* Part II.B.).

We note at the outset of this Assessment that two lawsuits currently pending before federal district courts concern some of the same issues considered in this Assessment. In *Abidor v. Napolitano*, No. 1:20-cv-04059 (E.D.N.Y. filed Sept. 7, 2010), the individual plaintiff alleges that he was searched on board an Amtrak train at the port of entry between Quebec and New York and that his laptop and external hard drive were detained for further inspection. The National Association of Criminal Defense Lawyers and National Press Photographers Association are also plaintiffs in the *Abidor* case. The plaintiffs allege that the individual search, and 2009 CBP and ICE policies, violate the Fourth Amendment by permitting the suspicionless search, copying, and detention of electronic devices and the First Amendment by permitting the suspicionless search, copying, and detention of electronic devices containing expressive materials. Complaint at 33, *Abidor v. Napolitano*. In *House v. Napolitano*, No. 1:2011cv10852 (D. Mass. filed May 13, 2011), the plaintiff states that he

[1] *See* Management Inspections Division, Office of Internal Affairs, U.S. Customs and Border Protection, Border Search of Electronic Devices and Documents, Report Number MID-10-003 (November 19, 2010) [hereinafter MID Report].

[2] U.S. Customs and Border Protection, Dep't of Homeland Sec., Muster, Border Search of Electronic Devices Directive 3340-049 (October 25, 2010) [hereinafter October 2010 Muster].

has been targeted for surveillance and investigation by various agencies of the U.S. government and alleges that a 2010 search and detention of his laptop, USB device, and video camera violated the First and Fourth Amendments. *See* Complaint at 9, *House v. Napolitano*. As explained below, we do not believe that the 2009 policies violate either the First or Fourth Amendment. *See* discussion *infra* Parts III.A.1-B.

ICE and CBP exercise longstanding constitutional and statutory authority permitting suspicionless and warrantless searches of merchandise at the border and its functional equivalent. But we conclude that the 2009 Directives impose useful requirements governing use of this authority in searching, reviewing, retaining, and sharing information contained in electronic devices. The management controls imposed on these activities include limitations on how long devices should generally be retained for completion of a border search, requirements that notice be provided the device owners regarding the process, and supervisory oversight to help prevent abuse of discretion by individual officers. To further protect the individual liberty of travelers, however, we make five recommendations, each related to the decision to conduct an electronic device search. All but one are directed only to CBP, because nearly all such decisions are made by CBP:

1. *Rationale:* **CBP officers who decide to conduct a device search generally should record the reason for the search in a TECS field. The reason should specifically relate to the decision to inspect an electronic device, not merely the selection for secondary screening (although the reason for both may be the same). To be clear, we are not recommending that officers demonstrate reasonable suspicion for the device search; rather we recommend that officers simply record the actual reason they are conducting the search, whatever that reason is. This recommendation exceeds constitutional requirements, but should facilitate CBP's operational supervision and oversight.**

2. *Antidiscrimination Policy:* **CBP and ICE should state explicitly in policy that it is generally impermissible for officers to discriminate against travelers—including by singling them out for specially rigorous searching—because of their actual or perceived religion, and that officers may use race, religion, or ethnicity as a factor in conducting discretionary device searches only when (a) based on information (such as a suspect description) specific to an incident, suspect, or ongoing criminal activity, or (b) limited to situations in which Component leadership has found such consideration temporarily necessary based on their assessment of intelligence and risk, because alternatives do not meet border security needs**.

3. *Regular Monitoring:* **CBP should improve monitoring of the distribution of electronic device searching by race and ethnicity, by conducting routine analysis, including annual examination of electronic device searches by port of entry. After controlling for known relevant and permissible factors, such as port traveler demographics, and** (b)(7)(E) (b)(7)(E) **the analysis should assess whether travelers of any particular ethnicity—estimated using nationality/country of birth and name analysis—at any port of entry are being chosen for electronic device searches in substantial disproportion to that ethnicity's portion of all travelers through the port. The analysis should also consider U.S. citizens separately from others. Data and results should be shared with CRCL.**

4. *Subsequent Supervision:* **If it appears that electronic device searching in any port has a substantial unexplained skew towards travelers of one or more ethnicity, CBP should work with CRCL on developing appropriate oversight mechanisms. Subsequent steps generally should include a requirement of supervisory approval for searches (absent exigent circumstances) or enhanced training, and may include other responses.**

5. *Improved Notice:* **CBP should improve the notice given to travelers subjected to electronic device searches by updating tear sheets to refer travelers to DHS TRIP if they seek redress.**

DHS is required by law to execute its border security mission in a manner that protects civil rights and civil liberties. The Department's authorizing statute explains that among the "primary mission[s] of the Department is to … ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland." 6 U.S.C. § 111(b)(1) (2006). This requirement goes beyond simply ensuring minimal civil rights and civil liberties compliance. This Office and the Department as a whole are committed to building systems that protect civil rights and civil liberties in both policy design and practice, and to enhancing protections when there is no countervailing harm to the Department's law enforcement efforts. Our recommendations are in this spirit. They are intended as the Office for Civil Rights and Civil Liberties' advice to the Secretary, who requested this Impact Assessment, and do not purport to state the current position of the Department. Nor are the policy recommendations, in particular, intended to create any judicially enforceable rights or remedies.

## II. Facts

### A. Primary Inspection and Referral

Both ICE and CBP are charged with deterring, detecting, and apprehending the importation of contraband, enforcing laws controlling the flow of persons and goods across the borders, and assisting myriad other federal enforcement agencies when those agencies' enforcement activities have a border nexus. CBP is responsible for securing United States borders and determining the admissibility of all persons or goods seeking to travel across the border at 327 ports of entry; ICE, among its other responsibilities, is the agency that investigates criminal activity relating to border crimes. Together they confront illegal activity at the border to detect evidence relating to terrorism and other national security matters, as well as, for example, narcotics, human and bulk cash smuggling, contraband, and child pornography.[3] Congress has long recognized, and the Supreme Court has repeatedly affirmed, the importance of these missions and the broad authority ICE and CBP customs officers[4] have to protect our borders.[5] (Rather than distinguishing between CBP

[3] U.S. Customs and Border Protection, Dep't of Homeland Sec., Directive No. 3340-049, Border Search of Electronic Devices Containing Information (Aug. 20, 2009), *available at* http://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf [hereinafter CBP Directive]; U.S. Immigration and Customs Enforcement, Dep't of Homeland Sec., Directive No. 7-6.1, Border Searches of Electronic Devices § 4 (Aug. 18, 2009), *available at* http://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf [hereinafter ICE Directive].

[4] 19 U.S.C. § 1401(i) (defining "customs officer").

Officers and ICE Agents, this Impact Assessment uses "officer" as a generic description for the relevant CBP and ICE personnel.) As already summarized, the volume of the resulting ICE and CBP activities is vast: CBP encounters more than 22 million travelers each month at its 327 ports of entry. The range of contraband seized from these travelers runs a broad gamut. Officers search persons, goods, and commercial and personal containers for contraband, daily detaining on average 1903 individuals for illegal entry, making on average 75 criminal arrests, and seizing 11,435 pounds of illegal narcotics.[6] Although narcotics and weapons seizures are the interdictions that most frequently make headlines, and forbidden agricultural products are the most frequently seized items, contraband also include documents such as child pornography or fraudulent passports. Still other seized documents may not be contraband per se, but constitute evidence of crimes relating to terrorism, immigrant smuggling, immigration fraud, narcotics, trafficking, illegal technology transfer, financial crimes, and other crimes falling under DHS jurisdiction.[7]

The decision to search a traveler is based on the totality of information available to an officer; the immensity of the flow of travelers and goods into and out of the United States shapes CBP and ICE search policies and practices. Resources for performing detailed and time-consuming border searches, including laptop searches, are limited, making the efficient allocation of resources critical for officers and supervisors. For each traveler arriving at any port of entry—land, air, or sea—the first step is to undergo primary immigration examination and customs inspection. During the primary examination, a CBP officer asks questions to establish whether the traveler is admissible into the United States; if that determination cannot be made quickly, the passenger will be referred to secondary inspection. (For air and sea passengers, the process actually starts with prescreening—an (b)(7)(E) (b)(7)(E) of a traveler upon arrival, or to further evaluate admissibility of an alien.)

Officers performing primary inspection do not follow a set script, instead asking questions (b)(7)(E) (b)(7)(E) support the discretionary decision to clear travelers directly from primary inspection or instead refer them to secondary inspection.

Referrals to secondary inspection may be made for any reason. Yet the techniques officers apply to make referral decisions channel their broad discretion (b)(7)(E)

---

[5] *See United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country.").

[6] U.S. Customs and Border Protection, Dep't of Homeland Sec., On a Typical Day in Fiscal year 2010, CBP … (Feb. 25, 2011) http://www.cbp.gov/xp/cgov/about/accomplish/typical_day_fy2010.xml.

[7] CBP Directive, *supra* note 3; ICE Directive, *supra* note 3.

(b)(7)(E) These are described in the 2004 CBP *Personal Search Handbook*[8] and in CBP officer Primary Training, as well as in other procedural guidance and training documents. In addition to (b)(7)(E) mentioned above, some referrals to secondary inspection may result from (b)(7)(E) (b)(7)(E) CBP also conducts a limited number of random compliance examinations, denominated "COMPEX" searches.[9] Nearly 98% of travelers are admitted/cleared into the United States directly from primary inspection. The small group for which this is not true are referred to secondary inspection, and may be subject to further interview, personal search, agricultural inspection or duties assessment, or more detailed baggage inspection—which can include search of electronic devices.

**B. Secondary Inspection and Electronic Device Searches**

CBP and ICE do not target electronic devices alone; such devices are one of many types of items or containers that may be searched, usually during secondary inspection. And an electronic device may be subjected to one or more types of scrutiny. These include:

- A brief physical inspection by an officer, including the traveler opening a case, or perhaps turning a device on, in order to demonstrate that the device is what it purports to be and not a container for tangible contraband (e.g., illegal drugs). This type of inspection is not considered to be an electronic device search for the purposes of the border search policy.[10]
- Search of the device's contents.
- Detention of a device, or of a copy of information contained on the device, for the completion of forensic examination. ICE and CBP policies provide guidance on the length of time electronic devices may generally be detained. The guidance is flexible in light of operational requirements, and differs between the two Components based upon their differing missions. Minimizing the length of time a device is detained is a goal of both policies, but encryption, large volumes of documents, password protections, and the need for computer forensic assistance may cause detention to last up to several months, and the policies deal with this delay in different ways, discussed immediately below.
- Seizure of a device as evidence of a crime, or for civil forfeiture under applicable law. A seized device is ordinarily retained through trial as evidence, subject to normal evidentiary handling rules. (If a device is subject to forfeiture, appropriate forfeiture proceedings are initiated as provided by law. *See* 19 U.S.C. §§ 1600-1617 (2006).)
- Retention of a device, or of a copy of information contained on the device, for evidence of continued or future admissibility.

[8] Office of field Operations, U.S. Customs and Border Protection, Personal Search Handbook (2004) [hereinafter Personal Search Handbook].

[9] *See* U.S. Customs and Border Protection, Dep't of Homeland Sec., Random Exams, http://www.cbp.gov/xp/cgov/travel/admissibility/random_exams.xml.

[10] CBP Directive, *supra* note 3, at § 3.4.

As the front-line law enforcement agency, CBP restricts more tightly than ICE does the length of time a device can be detained. If CBP detains a device for more than five days, a port director or equivalent manager must approve the detention extension, and any detention past 15 days requires approval from senior CBP management, such as the Director of the Office of Field Operations.[11]

ICE's role is to run longer-term investigations. If a device is turned over to ICE for such an investigation, ICE policy gives officers up to 30 calendar days to complete border searches without seeking supervisory approval. Searches exceeding 30 days are to be documented in ICE information systems, and must be approved by the relevant Group Supervisor, with continuing approval required every 15 days thereafter. To limit the length of time a device may be detained, ICE has identified specific factors to be considered by the investigating officer to ensure that the time taken to conduct the search is "reasonable" given the facts and circumstances of the particular search: (1) the amount of information needing review; (2) whether the traveler was deprived of his property and, if so, whether the traveler was given the option of continuing his journey with the understanding that his property would be returned once the border search was complete or a copy could be made; (3) the elapsed time between the detention, the initial border search, and the continued border search, including any demand for assistance; (4) whether the traveler has taken affirmative steps to prevent speedy search; (5) whether and when ICE or CBP followed up with the agency or entity providing assistance to ensure timely review; and (6) any unanticipated exigency that may arise.[12]

CBP and ICE policies both direct officers to conduct electronic device searches in the presence of the traveler unless there are special national security or operational considerations (such as preserving the integrity of an investigation) that would make it inappropriate for the traveler to observe the search.[13] Furthermore, for CBP, although express supervisory approval is not required, electronic device searches are to occur in the presence of a supervisor unless contacting a supervisor is not practicable, and in such instances the officer is required to notify a supervisor about the search and any results as soon as possible.[14] Several officers, both in the field and at Headquarters, have told CRCL that the supervisory presence requirement means, in practice (though not as a matter of national policy), that supervisors are asked to permit a search of an electronic device, and that supervisors may require an articulated reason for that search. As noted above, MID found a significant degree of confusion regarding the issues of supervisory presence and approval in the field. CBP has now clarified that supervisory approval is required only for detaining devices or copies of information contained therein, and that when performing a manual border search of an electronic device a supervisor need not be present or approve the search, although officers are advised that the better practice is to have a supervisor present during such searches.[15] ICE Special Agents are authorized to make investigative decisions based on the particular facts and circumstances of each case and do not require supervisory approval.[16]

---

[11] CBP Directive, *supra* note 3, at § 5.3.1.1.

[12] ICE Directive, *supra* note 3, at § 8.3.

[13] CBP Directive, *supra* note 3, at § 5.1.4; ICE Directive, *supra* note 3, at § 8.1.2.

[14] CBP Directive, *supra* note 3, at § 5.1.3.

[15] October 2010 Muster, *supra* note 2.

[16] ICE Directive, *supra* note 3, at § 6.1; ICE Special Agents are required to obtain supervisory approval for detentions that exceed 30 days (any detention exceeding 30 calendar days must be approved by a supervisor, and approved again every 15 calendar days thereafter).

For CBP searches, the fact of the search and information about it is recorded in the TECS system[17]; currently, information collected includes the general reason for the referral to secondary inspection and, in a "remarks" section, what was searched, and what, if anything, resulted from that search. Officers in both agencies are required to record any secondary examination of an electronic device[18] by completing an after-action report—including in TECS all information related to the search through the final disposition including supervisory approvals and extensions when appropriate—entered into TECS.[19] MID found, however, that these systems were inadequate. It recommended that CBP identify and implement actions required to ensure data extraction methods provide precise statistics on the number of searches, detentions, and seizures of documents and electronic devices recorded in TECS; and that CBP develop and implement a new TECS module, or enhance existing modules, to facilitate the accurate recording of electronic device search enforcement actions, allow for automatic notification of required supervisory approvals; and enable the tracking of detained documents and electronic devices.[20] CBP concurred with both of these recommendations and is in the process of implementing them.

When examining an electronic device, if an officer determines that probable cause exists to believe that the device contains evidence of violation of a law that CBP or ICE is authorized to enforce, officers may seize and retain the device, or may create and retain a copy of relevant information.[21] If the officer determines that there is no probable cause to seize the device or retain a copy, the device is returned to the traveler within seven business days of that determination, unless a supervisor authorizes an extension of up to 14 additional days.[22] If any information was copied, it is destroyed on the same schedule—except that even in the absence of probable cause, ICE or CBP may retain copied information that relates to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained.[23]

During the course of a border search, ICE or CBP officers may discover that they need subject matter assistance to understand the significance of the information discovered, or technical assistance to translate or decrypt information on the device. While not required by law, both ICE and CBP policies require that requests for subject matter assistance from outside agencies be premised upon reasonable suspicion of activities in violation of the laws enforced by CBP and ICE. Requests for technical assistance, such as translation or decryption, are permitted without such a threshold showing.[24] CBP's policies state that a traveler's presence on the government-operated and

---

[17] TECS is a user interface that permits users to check and add to law enforcement-related database records about travelers. *See* 73 Fed. Reg. 77778 (Dec. 19, 2008).

[18] CBP Directive, *supra* note 3, at §5.5; ICE Directive, *supra* note 3, at § 8.2(2)-(3).

[19] CBP Directive, *supra* note 3, at § 5.5.1; U.S. Immigration and Customs Enforcement, Dep't of Homeland Sec., Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices (Dec. 12, 2008).

[20] MID Report, *supra* note 1, at 12-13.

[21] CBP Directive, *supra* note 3, at § 5.4.1.1; ICE Directive, *supra* note 3, at § 8.5(1)(a).

[22] CBP Directive, *supra* note 3, at § 5.3.1.2; ICE Directive, *supra* note 3, at § 8.5(1)(e).

[23] CBP Directive, *supra* note 3, at § 5.4.1.2; ICE Directive, *supra* note 3, at § 8.5(1)(b).

[24] CBP Directive, *supra* note 3, at § 5.3.2; ICE Directive, *supra* note 3, at § 8.4.

government-vetted watchlist is sufficient to support a determination of reasonable suspicion.[25] The October 2010 Muster notes the importance of documenting electronic device searches and clarifies the contrasting documentation requirements that apply when CBP transfers a device to ICE for subject matter assistance versus those that apply when ICE detains a device on its own authority.[26]

Once the requested assistance is provided to CBP or ICE, both require that all information shared with an outside agency be returned and copies be destroyed as expeditiously as possible, unless the assisting agency has independent legal authority to retain a copy of information, in which case both ICE and CBP request that the retaining agency notify ICE or CBP that it is retaining information.[27] CBP (but not ICE) policy requires that travelers be notified of any information sharing unless notice would be contrary to national security, law enforcement, or other operational interests.[28]

(b)(7)(E) when CBP detains an electronic device, CBP provides each traveler whose electronic device is searched with a "tear sheet" listing the legal authority for the search of his electronic device and explaining some possible reasons why travelers may be selected for such a search, what the traveler should expect, and information regarding how to seek redress.[29] This form also provides information concerning DHS and CBP privacy policy, a web address for the DHS Office for Civil Rights and Civil Liberties, and contact information for the CBP Info Center. Additionally, whenever they detain or seize an electronic device, CBP and ICE provide the traveler with a chain of custody form.[30] If a device is detained, the traveler receives Form 6051D; if the device is seized, the traveler receives Form 6051S. These forms serve as notice and a receipt for seized/detained property.

## III. Legal and Policy Analysis

This section examines the lawfulness of the CBP and ICE policies governing searches of electronic devices at the border, concluding that they do not violate the Fourth or First Amendments or the Equal Protection Clause. Nonetheless, although we conclude that these policies are lawful and represent marked improvement over past policies, the protection of civil rights and civil liberties is more than upholding a constitutional floor for government behavior. The Department's activities to enforce the laws and provide security necessarily involve detection and deterrence of crimes facilitated by electronic devices, and therefore require intrusion into aspects of people's lives that would otherwise remain unscrutinized. But it is incumbent on the Department to exercise its power carefully, accomplishing its mission in a manner that observes individual rights and protects the

[25] CBP Directive, *supra* note 3, at § 5.3.2.3; ICE Directive, *supra* note 3, at § 8.4(2).

[26] October 2010 Muster, *supra* note 2.

[27] CBP Directive, *supra* note 3, at §§ 5.4.2.2-5.4.2.3; ICE Directive, *supra* note 3, at §§ 8.5(2)(b)-(c). The October 2010 Muster reemphasizes the destruction requirement and clarifies that "destruction" refers to the deleting, shredding, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C. October 2010 Muster, *supra* note 2.

[28] CBP Directive, *supra* note 3, at § 5.3.2.6.

[29] CBP Directive, *supra* note 3, at § 5.3.1.3; U.S. Customs and Border Protection, Dep't of Homeland Sec., Inspection of Electronic Devices, 0204-0709 (2009), *available at* http://www.cbp.gov/linkhandler/cgov/travel/admissibility/msa_tearsheet.ctt/msa_tearsheet.pdf.

[30] CBP Directive, *supra* note 3, at § 5.3.1.4; ICE Directive, *supra* note 3, at §§ 8.2(1-4).

dignity of those whom we serve. Accordingly, in addition to evaluating the lawfulness of DHS policies governing the border search of electronic devices, we have evaluated a number of policy ideas, most directed at the Department in various forms by civil rights and immigration advocacy groups, to determine whether additional civil rights and civil liberties protections are necessary or useful. Our five recommendations have already been set out in the introduction to this Assessment, above, and are discussed below. Note, however, that as a result of our law and policy review, we reach the following conclusions about steps that we believe *need not* be taken:

- CBP and ICE need not institute a policy requirement of reasonable suspicion as a predicate for electronic device searches.
- CBP and ICE electronic border search policies do not violate travelers' First Amendment rights as defined by the courts.
- Additional time limits on electronic searching are not necessary; current policy ensures reasonable efforts at promptness.
- Additional safeguards are not needed with respect to privileged or sensitive information; current policy and training are sufficient.

The rationales underlying both our recommendations and our decision against particular recommendations are set forth in the following sections.

## A. Authority to Search Electronic Devices at the Border

### *1. Fourth Amendment*

*Border Search Authority*

(b)(5)

~~DELIBERATIVE PROCESS PRIVILEGE//PRE-DECISIONAL//FOR OFFICIAL USE ONLY~~

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5) Indeed, both the CBP and ICE directives contain a number of rights protections beyond those that have been required by courts. In particular, as already mentioned, CBP and ICE policies require the following:

- Searches of electronic devices are conducted with the traveler's knowledge and presence, unless there are particular national security or law enforcement considerations that make it inappropriate to permit the individual to remain present.[34]

[33] CBP Directive, *supra* note 3, at § 5.3.2.2; ICE Directive, *supra* note 3, at § 8.4.

[34] CBP Directive, *supra* note 3, at § 5.1.4; ICE Directive, *supra* note 3, at § 8.1(2).

- Searches of electronic devices are documented in appropriate systems of records.[35]
- Retention of data is forbidden in the absence of probable cause to believe a crime has been committed, unless the retained data pertains to immigration, customs, or other enforcement matters. In any event, such retention must be consistent with the privacy and data protection standards of the system of records in which such information is being retained.[36]
- Data destruction requirements are specified and quite strict. If data is not being retained, CBP and ICE generally have seven days to destroy the data. A certified forensic agent with specialized expertise destroys any electronic evidence. If circumstances require additional time, supervisor approval is required to obtain an extension to no more than 21 days.[37]
- Data is safeguarded and stored[38] to comply with detailed reporting and management requirements.[39]
- Device detention periods are limited, unless an extension of time is approved. Subject to applicable extensions, CBP generally has up to five days to conduct the search of the electronic device while ICE has up to 30 days.[40]
- Supervisory oversight is emphasized. CBP requires supervisors to be present for electronic devices searches where practicable and requires supervisory approval to detain the device or image its memory so that the search might continue after the traveler departs from the port of entry.[41]
- Reasonable suspicion is required for searches that seek subject matter assistance from federal or non-federal agencies outside DHS.[42]

These polices address many of the civil rights and civil liberties concerns raised by the public and Congress about border examinations of electronic devices.

In sum, the overall authority to conduct border searches without suspicion or warrant is clear and long-standing, and courts have not treated searches of electronic devices any differently from searches of other objects. CRCL concludes that CBP's and ICE's current border search policies comply with the Fourth Amendment. We also recognize that the law regarding searches of electronic devices will continue to develop. Therefore, CRCL will continue to work with DHS

---

[35] CBP Directive, *supra* note 3, at § 5.1.3; U.S. Immigration and Customs Enforcement, Office of Investigations (OI) Guidance, Dep't of Homeland Sec., Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices (Dec. 12, 2008); ICE Directive, *supra* note 3, at § 8.2(1).

[36] CBP Directive, *supra* note 3, at § 5.4.1.2; ICE Directive, *supra* note 3, at § 8.5(1).

[37] CBP Directive, *supra* note 3, at §§ 5.3.1.2 & 5.4.1.2; ICE Directive, *supra* note 3, at § 8.5(e).

[38] CBP Directive, *supra* note 3, at § 5.4.1.5; ICE Directive, *supra* note 3, at § 8.5(1)(d).

[39] CBP Directive, *supra* note 3, at §§ 5.5 & 5.6.

[40] CBP Directive, *supra* note 3, at § 5.3.1; ICE Directive, *supra* note 3, at § 8.3(1).

[41] CBP Directive, *supra* note 3, at §§ 5.2-5.3.1.4. By contrast, ICE Special Agents are empowered to make investigative decisions based on the particular facts and circumstances of each case and do not require supervisory approval. ICE Directive, *supra* note 3, at § 6.1.

[42] CBP Directive, *supra* note 3, at § 5.3.2.2; ICE Directive, *supra* note 3, at § 8.4.

component agencies to ensure that civil rights and civil liberties are protected in this as in other areas.

### *2. A Suspicion-Based Rule Is Not Advisable*

Notwithstanding the case law that suspicionless searching of electronic devices at the border is constitutionally permissible, some critics have advocated increased traveler protections as a matter of policy, in the form of a firm administrative standard requiring the presence of reasonable suspicion that a crime has been committed prior to any electronic device search. One specific model that has been suggested[43] as an alternative to the current ICE and CBP policies is a 1986 policy, Customs Directive 3340-006, *Review, Copying and Seizing of Documents* (June 12, 1986). We do not believe that this 1986 approach, or a reasonable suspicion requirement in any other form, would improve current policy.

At the outset, we note that CBP and ICE are charged with exercising far broader authorities at the border than was the former U.S. Customs Service. As renamed and reorganized in 2003, CBP enforces a broad range of customs, immigration, agriculture, and other federal laws at the border. Perhaps most importantly, CBP stands as the first line of defense in furtherance of the Department's national security and anti-terrorism responsibilities, articulated in the Homeland Security Act of 2002, as amended, 6 U.S.C. § 201 (2006), and elsewhere. Similarly, ICE, which received part of the former Customs Service, was created in 2003 to house all customs and immigration investigators, and is responsible for investigating all crimes relating to the border.

In addition, we note that although the 1986 policy directed that "Customs Officers should not read personal correspondence contained in travelers' baggage or on the person," it simultaneously authorized warrantless, suspicionless inspection procedures permitting extensive reading to allow officers to ascertain the content of the documents. Officers were directed to first read the document or paper by "scanning,"[44] in order to determine what action was appropriate."[45] Next, the officer was permitted, without suspicion or warrant, to fully read any documents that "appear[ed] to relate" to any one of the Customs Service's enforcement, regulatory or administrative functions listed within the policy. Then, if it was not "immediately apparent whether the document [was] admissible or subject to seizure," a document could be detained for a reasonable period of time upon reasonable suspicion that it belonged to a category of goods and subject to customs enforcement, regulation, or administration.[46] In short, like the current ICE and CBP policies, the 1986 policy allowed multiple warrantless, suspicionless readings of documents, in varying degrees of detail, to ensure compliance with applicable law.

---

[43] Ellen Nakashima, *Expanded Powers to Search Travelers at Border Detailed*, Washington Post, September 23, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/22/AR2008092202843.html.

[44] U.S. Customs Serv., Directive 3340-006, *Review, Copying and Seizing of Documents* (June 12, 1986), § 5(b) [hereinafter Directive 3340-006].

[45] Seditious materials were included among the types of documents that could be examined further. These were defined in the 1986 policy as materials "inciting or producing imminent lawless action, or prohibited matter being imported in violation of 19 U.S.C. § 1305." Directive 3340-006, *supra* note 44 at § 5(a)(v).

[46] Directive 3340-006, *supra* note 44 at § 5(e).

Whatever the parameters of the 1986 policy, adding a heightened threshold requirement could be operationally harmful without concomitant civil rights/civil liberties benefit. First, commonplace decisions to search electronic devices might be opened to litigation challenging the reasons for the search. In addition to interfering with a carefully constructed border security system, the litigation could directly undermine national security by requiring the government to produce sensitive investigative and national security information to justify some of the most critical searches. Even a policy change entirely unenforceable by courts might be problematic; we have been presented with some noteworthy CBP and ICE success stories based on hard-to-articulate intuitions or hunches based on officer experience and judgment. Under a reasonable suspicion requirement, officers might hesitate to search an individual's device without the presence of articulable factors capable of being formally defended, despite having an intuition or hunch based on experience that justified a search. Although this Office does not advocate arbitrary decision-making, we understand that there may be occasions where officers have only a few seconds to make important decisions about admissions and searches, and where they lack the opportunity to use routine criminal investigative techniques to develop reasonable suspicion or probable cause to justify the inspection of containers. Officers must therefore frequently make important choices based on inadequate and imperfect information. We note that officers very likely do have reasonable suspicion in most searches of electronic devices based on existing screening methods and objective factors; however, in light of the diminished expectations of privacy at the border and the government's paramount interest in border security, as well as the methods and objective factors ordinarily applied in making decisions, we conclude heightened suspicion requirements for searches of electronic devices at the border are not appropriate.

At the same time, the absence of information about *why* a particular search was performed renders supervision more difficult. The information could be used by supervisors or managers to understand whether the authority is being overused, in light of resources and priorities. Accordingly, our first recommendation is:

1. ***Rationale:*** **CBP officers who decide to conduct a device search generally should record the reason for the search in a TECS field. The reason should specifically relate to the decision to inspect an electronic device, not merely the selection for secondary screening (although the reason for both may be the same). To be clear, we are not recommending that officers demonstrate reasonable suspicion for the device search; rather we recommend that officers simply record the actual reason they are conducting the search, whatever that reason is. This recommendation exceeds constitutional requirements, but should facilitate CBP's operational supervision and oversight.**

**B. First Amendment**

(b)(5)

(b)(5)

(b)(5) The laptop border searches in the ICE and CBP policies do not violate travelers' First Amendment rights as defined by the courts.

**C. Equal Protection and Religious/Ethnicity Discrimination**

Civil rights and civil liberties advocacy groups have also raised concerns that particular religious and ethnic communities are being improperly singled out at the border for undue law enforcement attention in general and electronic media searches in particular.

Neither CBP nor ICE has an explicit written policy or training forbidding use of known or perceived religion as a screening criterion, although leadership within both Components has stated in less

formal ways that religious discrimination is unacceptable. With respect to race and ethnicity, there is extant written guidance. Pursuant to the Department of Justice's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies[48] and DHS's 2004 Commitment to Race Neutrality in Law Enforcement Activities,[49] ICE and CBP personnel are permitted to use race or ethnicity as factors in a decision to search a person or object only based on information that is specific to an incident, suspect, or ongoing criminal activity, or as part of a narrowly tailored response to a compelling state interest involving national security or border integrity. During interviews, ICE and CBP personnel explained that officers are affirmatively taught not to rely on these constitutionally suspect classifications in searching electronic devices except based on information specific to particular suspects, incidents, or ongoing criminal activities, and that they are reminded regularly of the prohibition.

(b)(5)

(b)(5) Our second recommendation would further consistency, and provide additional civil rights and civil liberties protection:

2. ***Antidiscrimination Policy:*** **CBP and ICE should state explicitly in policy that it is generally impermissible for officers to discriminate against travelers—including by singling them out for specially rigorous searching—because of their actual or perceived religion, and that officers may use race, religion, or ethnicity as a factor in conducting**

[48] Civil Rights Division, U.S. Dep't of Justice, Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (2003), *available at*: http://www.justice.gov/crt/about/spl/documents/guidance_on_race.pdf.

[49] U.S. Dep't of Homeland Sec., The Department of Homeland Security's Commitment to Race Neutrality in Law Enforcement Activities (2004), *available at:* http://www.dhs.gov/xlibrary/assets/CRCL_MemoCommitmentRaceNeutrality_June04.pdf.

(b)(5)

**discretionary device searches only when (a) based on information (such as a suspect description) specific to an incident, suspect, or ongoing criminal activity, or (b) limited to situations in which Component leadership has found such consideration temporarily necessary based on their assessment of intelligence and risk, because alternatives do not meet border security needs**.

Some advocacy organizations have also suggested that electronic device searching has very disproportionate effects on travelers whose ethnic or national background is Arab or Middle Eastern and that these effects are onerous and unjustified. To explore the factual premises that underlie this concern, CRCL and CBP have analyzed two years of data on electronic device searches. We have together concluded that if a port with a relatively high volume of device searches concentrates those searches among travelers within particular demographic groups, enhanced training and supervision can help to ensure that such concentration is not the result of bias or other inappropriate decision-making. Through the data analysis, CRCL and CBP have developed a framework for appropriate ongoing collection of statistical information to enable periodic review of this possibility. Our third and fourth recommendations are based on this analysis, and in accordance with this agreed-upon framework:

3. *Regular Monitoring:* **CBP should improve monitoring of the distribution of electronic device searching by race and ethnicity, by conducting routine analysis, including annual examination of electronic device searches by port of entry. After controlling for known relevant and permissible factors, such as port traveler demographics, and inclusion in watchlists, lookouts, and targeting rules, the analysis should assess whether travelers of any particular ethnicity—estimated using nationality/country of birth and name analysis—at any port of entry are being chosen for electronic device searches in substantial disproportion to that ethnicity's portion of all travelers through the port. The analysis should also consider U.S. citizens separately from others. Data and results should be shared with CRCL.**

4. *Subsequent Supervision:* **If it appears that electronic device searching in any port has a substantial unexplained skew towards travelers of one or more ethnicity, CBP should work with CRCL on developing appropriate oversight mechanisms. Subsequent steps generally should include a requirement of supervisory approval for searches (absent exigent circumstances) or enhanced training, and may include other responses.**

**D. Time Limits**

Some critics of electronic border searches have also suggested stringent time limits for completion of searches. Again, they point to the 1986 Customs policy as a model. But whereas the 1986 policy relied on a brief perusal of documents to determine if reasonable suspicion or probable cause existed, the continuous evolution and advancement of technology requires a more flexible approach for officers to evaluate electronic devices. The main difference between the 1986 policy and current policy is that under the current policy, if a border search of an electronic device requires more than a very brief period of time, officers are permitted, without articulating a reason for suspicion, to detain the device or copy its contents to complete the search. The 1986 policy envisioned an officer paging through the travelers' documents, looking them over quickly to determine if reasonable suspicion (or probable cause) was present, and reading them in more depth if circumstances warranted it. This

approach is not tenable in the context of modern electronic devices. Gigabytes of information may be stored in password-protected files, encrypted portions of hard drives, or in a manner intended to obscure information from observation. An on-the-spot perusal of electronic devices following the procedures established in 1986 could well result in a delay of days or weeks; even a cursory examination of the contents of a laptop might require a team of officers to spend days or weeks skimming the voluminous contents of the device. At the same time, a firm time limit for completing a search risks allowing a wrongdoer to "run out the clock" by encrypting and password-protecting his device, or traveling with voluminous amounts of documents, or other measures to make the search very time consuming.

The 2009 policies address the government's interest in enforcement of the laws and the traveler's interest in personal autonomy and convenience by permitting a broad search, while taking steps to decrease traveler inconvenience where the search is time-consuming. Although the time limits are somewhat flexible, it seems likely that the firm requirements for officers to seek and receive increasing levels of supervisory approval for extended detention push officers to ensure that detailed searches are completed as quickly as possible. Various computer-assisted search methods aim to balance comprehensiveness against timeliness. In light of the ever-increasing amounts of data stored on electronic devices and ever-more-complex storage and encryption methods, we believe ICE and CBP are making reasonable efforts to ensure border searches are completed as promptly as possible; no further policy change is recommended.

**E. Privileged Materials**

Some critics have suggested that officers should be prohibited from searching communications for which a traveler claims legal privileges, such as attorney-client privilege. Such a restriction would create an obvious safe harbor for the smugglers of child pornography, for terrorist conspirators, and any criminals relying on the transfer of information across borders. We note that the current policies safeguard sensitive material with procedural protections. The directives address attorney-client privileged materials and attorney work product by requiring an officer who suspects that the content of a traveler's privileged document may constitute evidence of a crime or otherwise pertains to a determination within ICE and CBP jurisdiction, to consult with ICE or CBP counsel.[51] For other types of sensitive information—business or commercial information, trade secrets, and medical records, for example—the directives state that officers should comply with applicable statutory provisions and regulatory guidelines, and should ask counsel for assistance if necessary.[52] This is fully covered in the mandatory training that all CBP officers take. None of the complaints currently pending before or known to CRCL present concerns related to the discovery or sharing of privileged material.[53] We conclude that current safeguards in these areas are sufficient.

[51] CBP Directive, *supra* note 3, at § 5.2.1; ICE Directive, *supra* note 3, at § 8.6(2)(b).

[52] CBP Directive, *supra* note 3, at § 5.4.2.2-5.4.2.3; Ice Directive, *supra* note 3, at § 8.5(2)(b)-(c).

[53] The plaintiff in *House v. Napolitano* asserts as a factual matter that materials seized from him were "privileged," *see* Complaint at 8, *House v. Napolitano*, but does not claim that the materials in question were protected by a recognized legal privilege.

### F. Improved Notice about Redress

Following release of the August 2009 policies, CBP improved its airport signage and began providing a "tear sheet" to individuals whose electronic devices are searched. The airport signs better explain border search authority, provide Privacy Act information regarding electronic device searches, and explain the consequences for failure to provide information upon CBP questioning. The tear sheet explains to travelers whose devices are searched why they may have been selected, the legal authority for the device search, and what the traveler should expect from CBP.[54] The information provided about how to seek redress, however, is limited. The tear sheet includes contact information for the CBP info center, and it also states:

> The DHS Office for Civil Rights and Civil Liberties investigates complaints alleging a violation by DHS employees of an individual's civil rights or civil liberties. Additional information about the Office is available at www.dhs.gov/civilliberties.

More could be done to increase transparency and provide improved notice to travelers (at the very least, the form should provide the most up-to-date URL for CRCL's website: www.dhs.gov/crcl). At the same time, it is difficult to get all the relevant information on a short tear sheet. Our final recommendation is, therefore:

5. ***Improved Notice:*** **CBP should improve the notice given to travelers subjected to electronic device searches by updating tear sheets to refer travelers to DHS TRIP if they seek redress.**

We note in this regard that (at CRCL's request) TSA has recently updated DHS TRIP to give travelers a larger list of options from which to choose when seeking redress. Specifically, a traveler may now use the DHS TRIP system to complain that he/she was discriminated against on the basis of race, ethnicity, religion, disability, or gender; that he/she received questioning or treatment during screening that was abusive or coercive; and that a search of his/her person violated freedom of speech or press.

## IV. Conclusion

Electronic device searching at the border is an important issue, presenting several potentially competing concerns. The traveling public is entitled to cross our borders without Fourth and First Amendment violations or invidious discrimination on the basis of race, ethnicity, religion, or other protected characteristic. The 2009 Directives guide CBP and ICE in lawfully fulfilling their responsibilities to safeguard against, for example, overly intrusive, discriminatory, and excessively time-consuming searches of electronic devices.

We conclude that, in accordance with established case law, officers may, as a matter of both constitutional law and sound policy, search electronic devices at the border without reasonable suspicion of wrongdoing. We further conclude that electronic device searches conducted in

[54] U.S. Customs and Border Protection, Dep't of Homeland Sec., Publication 0204-0709, Inspection of Electronic Devices, *available at:* http://www.cbp.gov/linkhandler/cgov/travel/admissibility/msa_tearsheet.ctt/msa_tearsheet.pdf.

accordance with the 2009 Directives do not violate travelers' First Amendment rights or the Equal Protection clause, contain reasonable (if flexible) time limits, and contain sufficient safeguards to protect privileged communications. However, we have offered several recommendations for improved oversight and communication about redress; we believe that these recommendations can augment civil rights protections without impeding operational requirements and effectiveness.

Margo Schlanger
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
December 29, 2011

# EXHIBIT N

Below is the information retrieved so far. We haven't heard back yet from OFO to know if there was an official response from the field

(b) (6), (b) (7)(C) was processed inbound on July 14, 2016 through (b) (7)(E) (b) (6), (b) (7)(C), (b) (7)(E)
(b) (7)(E)

Last Name
(b) (6), (b) (7)(C) First (Given) Name
(b) (6), (b) (7)(C)
Birth Date (Day/Mo/Yr)
(b) (6), (b) (7)(C) Age
Gender
(b) (6), (b) (7)(C) Race

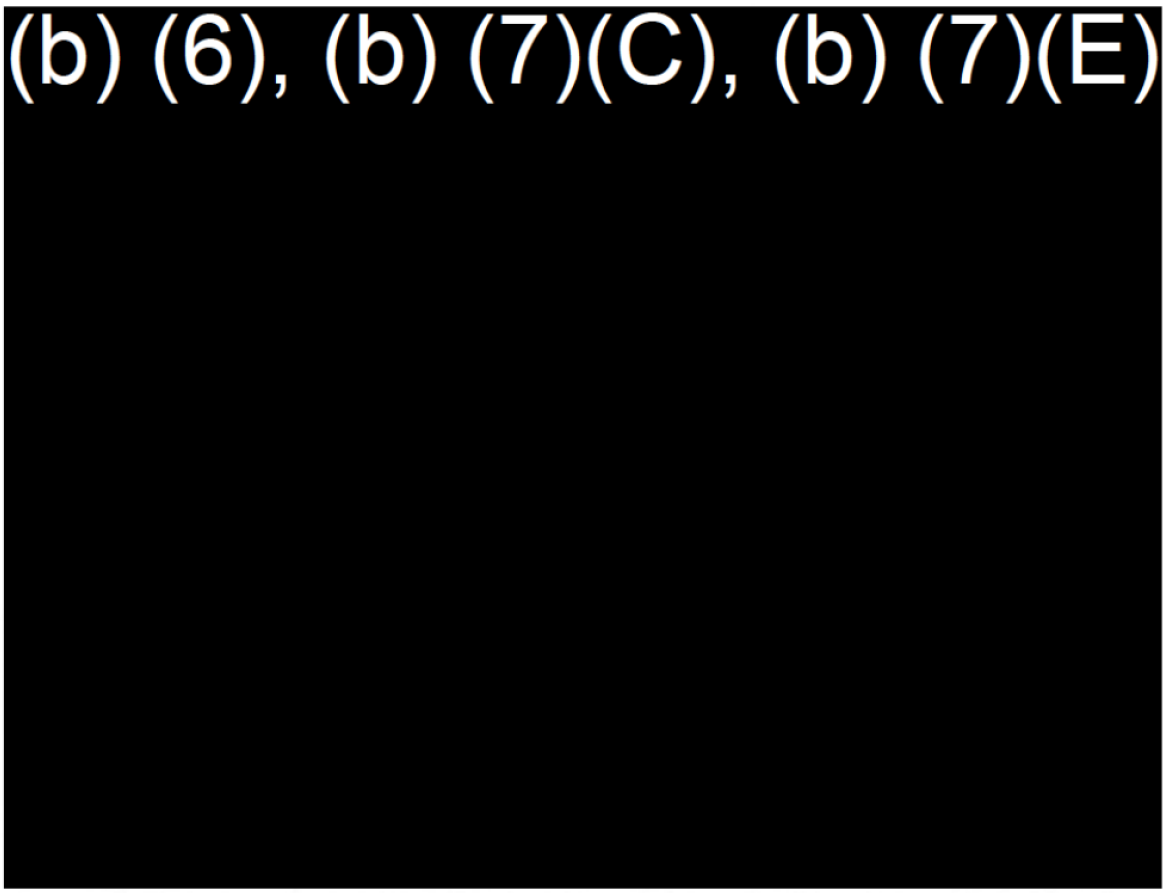
Document Country
(b) (6), Document Number
(b) (6), (b) (7)(C) Document Type
PASSPORT NUMBER (P)

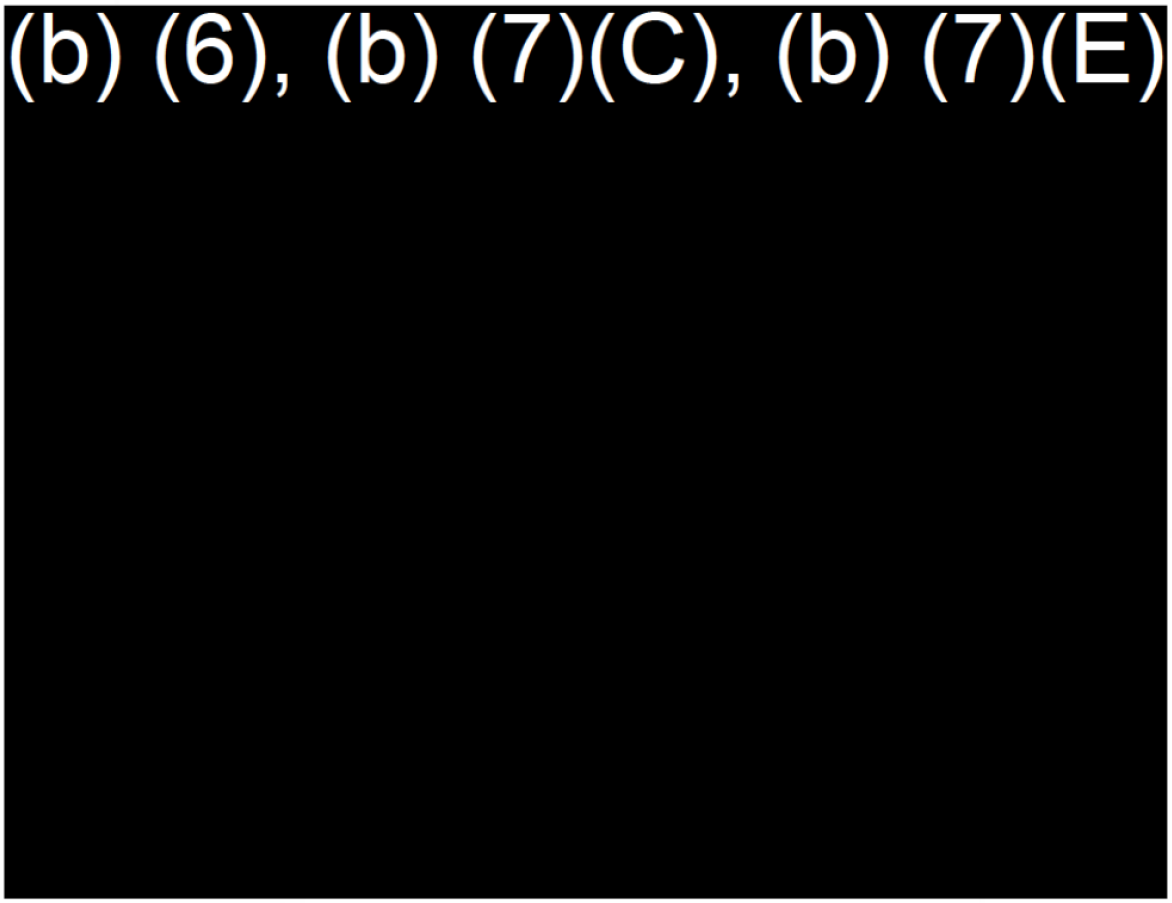
Location Information

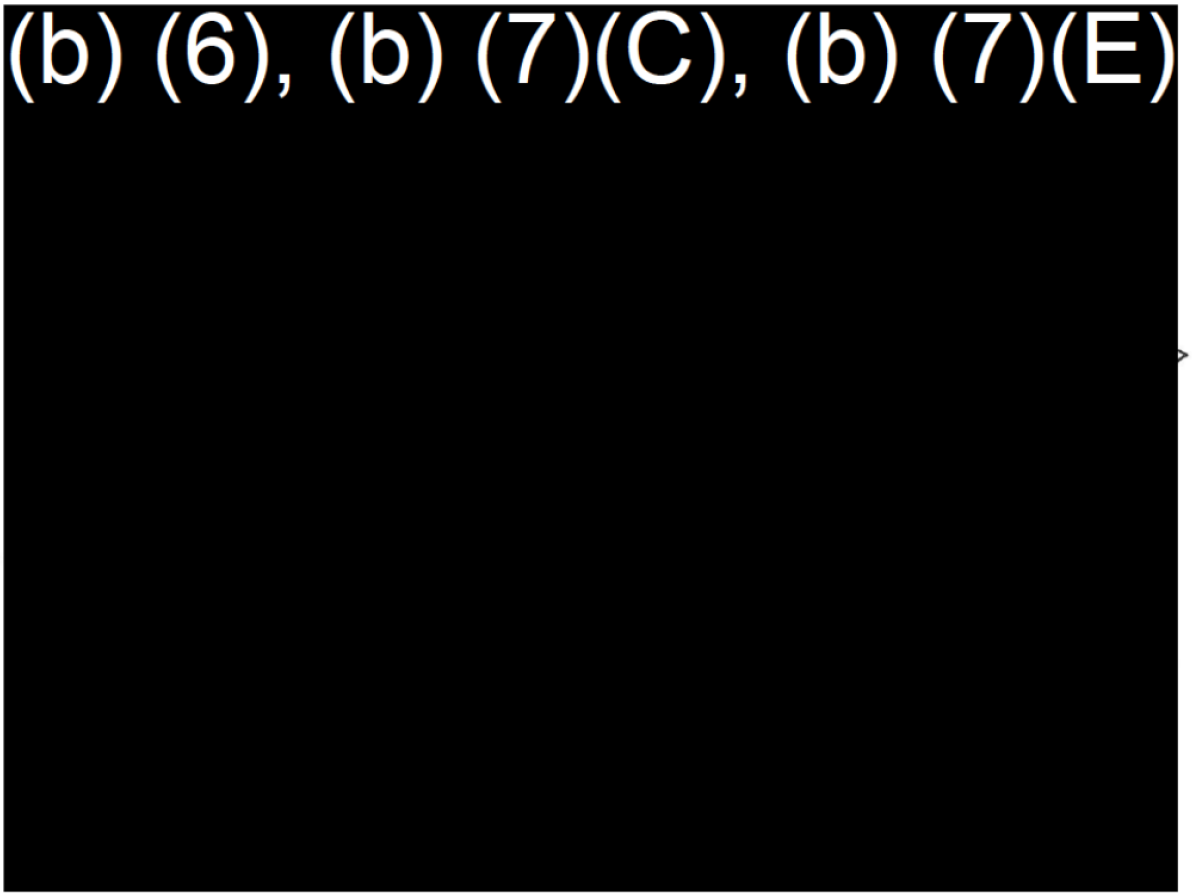
(b) (6), (b) (7)(C), (b) (7)(E)

Remarks
(b) (7)(E)

(b) (6), (b) (7)(C), (b) (7)(E)


(b) (6), (b) (7)(C), (b) (7)(E)


(b) (6), (b) (7)(C), (b) (7)(E)




50 minutes

# EXHIBIT O

**Muster 2009-17**

**Week of Muster:** Upon Receipt

**Headquarters POC:** Operations, Tactical Operations Division
(b)(6);(b)(7)(C) (b)(6);(b)(7)(C)

**SUBJECT:** (b) (7)(E)

Certain ports of entry currently use (b)(7)(E)
when conducting a Border Search of Electronic Devices Containing Information. (b) (7)(E)
(b) (7)(E)

Effective January 17, 2009 (b) (7)(E)
(b) (7)(E)

(b) (7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

You are reminded that all border searches of information contained in electronic devices must be performed in accordance with CBP Directive 3340-049, "Border Search of Electronic Devices Containing Information" dated August 20, 2009. Copies information must be handled, and destroyed if required, in accordance with section 5.4.1.2 of the

~~FOR OFFICIAL USE ONLY~~

(b)(7)(E)

# EXHIBIT P

**Lally, Claire M.**

**From:** Wilkens, Scott B.
**Sent:** Friday, June 23, 2017 12:07 PM
**To:** Katie.Fallow@knightcolumbia.org; alex.abdo@knightcolumbia.org
**Cc:** Jameel.Jaffer@knightcolumbia.org; DeCell, Caroline M.; Stewart, Michael E.
**Subject:** Fwd: Knight: Item 5: Civil & Criminal Complaints

Begin forwarded message:

From: "Glass, David (CIV)" <David.Glass@usdoj.gov<mailto:David.Glass@usdoj.gov>>
Date: June 22, 2017 at 5:25:50 PM EDT
To: "Wilkens, Scott B." <SWilkens@jenner.com<mailto:SWilkens@jenner.com>>
Subject: RE: Knight: Item 5: Civil & Criminal Complaints

Scott –

Here is a list of the four civil actions of which ICE is aware in which its authority to conduct border searches of electronic devices has been challenged:

Kam-Almaz v. United States, 96 Fed. Cl. 84 ( 2011) (No. 09-7C), appeal docketed, No. 2011-2059 (Fed. Cir. July 22, 2011) Abidor v. Napolitano, 990 F. Supp.2d 260 (E.D.N.Y 2013) (No. 1:10-CV-04059) House v. Napolitano, 2012 WL 1038816 (D. Mass. Mar. 28, 2012) (No. 1:11-CV-10852) Anibowei v. Lynch, No. 3:16-CV-3495 (N.D. Tex. filed Dec. 23, 2016)

David

From: Wilkens, Scott B. [mailto:SWilkens@jenner.com]
Sent: Friday, June 09, 2017 5:13 PM
To: Glass, David (CIV) <DGlass@CIV.USDOJ.GOV<mailto:DGlass@CIV.USDOJ.GOV>>
Subject: RE: Knight: Item 5: Civil & Criminal Complaints

David,

Thanks. Plaintiff is interested in the criminal as well as civil actions. With respect to the proposal regarding PACER, could you please advise about the number of civil and the number of criminal actions?

Thanks,
Scott

From: Glass, David (CIV) [mailto:David.Glass@usdoj.gov]
Sent: Friday, June 09, 2017 2:12 PM
To: Wilkens, Scott B. <SWilkens@jenner.com<mailto:SWilkens@jenner.com>>
Subject: Knight: Item 5: Civil & Criminal Complaints

Scott –

ICE advises that it knows of several civil actions in which searches of electronic devices have been challenged but that numerous motions have been filed in criminal actions to suppress evidence obtained from searches of electronic devices. Is plaintiff interested in the criminal actions? We propose with respect to both the civil and criminal actions merely to identify the actions and to leave it to plaintiff to obtain from PACER whatever filings it wants.

David

_____

Scott B. Wilkens

Jenner & Block LLP
1099 New York Avenue, N.W.
Suite 900, Washington, DC 20001-4412 | jenner.com<http://protect-us.mimecast.com/s/ESYtCYElEOIgEkG7uVbCAH?domain=jenner.com>
+1 202 639 6072 | TEL
SWilkens@jenner.com<mailto:SWilkens@jenner.com>
Download V-Card<https://protect-us.mimecast.com/s/vgBhCZ6m6PsxrPO6cxCwpa?domain=svcs.jenner.com> | View Biography<http://protect-us.mimecast.com/s/6vW0C1wBwKUO2nv4u1HMc1?domain=jenner.com>

CONFIDENTIALITY WARNING: This email may contain privileged or confidential information and is for the sole use of the intended recipient(s). Any unauthorized use or disclosure of this communication is prohibited. If you believe that you have received this email in error, please notify the sender immediately and delete it from your system.

_____

# EXHIBIT Q

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

June 23, 2017

SENT BY ELECTRONIC MAIL TO: katie.fallow@knightcolumbia.org

Katherine Fallow
Knight First Amendment Institute
535 West 116th Street
314 Low Library
New York, NY 10027

RE: CBP-2017-042463; *Knight First Amendment Institute v. DHS*, No. 1:17-cv-00548-TSC (D.D.C.)

Dear Attorney Fallow:

This is an electronic interim response to your Freedom of Information Act (FOIA) request to U.S. Customs and Border Protection (CBP), dated March 20, 2017, and received by this office on March 24, 2017. You 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 instance 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
   b. ICE Directive No. 7-6.1

4. The following documents relating to any reviews of CBP's or ICE's polices 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 of Civil Rights and Civil Liberties, DHS's OIIG and CBP's Office of Internal Affairs, Management Inspection Division;
   b. Any policies, practices, procedures, and/or training material adopted as a result of any audits, impact assessments, or other reviews of how CBP and ICE conduct electronic device searches; and
   c. Any document 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 journalist," as referenced in § 5.2 of the CBP Directive.

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

A further search of CBP databases produced a total of three pages of records responsive to your request. Per the June 6, 2017 Joint Status Report in *Knight First Amendment Institute at Columbia University v. DHS, et al.*, this release includes records responsive to request numbers 4 and 7. CBP has determined that three pages are partially releasable pursuant to Title 5 U.S.C. § 552 (b)(6), (b)(7)(C) and (b)(7)(E).

Enclosed are three pages with certain information withheld as described below:

**FOIA Exemption (b)(6)** exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a

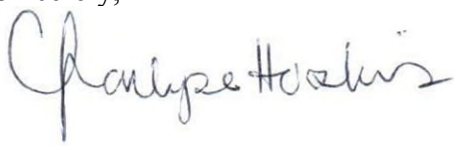
balancing of the public's right to disclosure against the individual's right privacy. The types of documents and/or information that we have withheld may consist of birth certificates, naturalization certificates, driver license, social security numbers, home addresses, dates of birth, or various other documents and/or information belonging to a third party that are considered personal. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

**FOIA Exemption (b)(7)(C)** protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. This exemption takes particular note of the strong interests of individuals, whether they are suspects, witnesses, or investigators, in not being unwarrantably associated with alleged criminal activity. That interest extends to persons who are not only the subjects of the investigation, but those who may have their privacy invaded by having their identities and information about them revealed in connection with an investigation. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate.

**FOIA Exemption (b)(7)(E)** protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or 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. CBP has determined that disclosure would disclose techniques or procedures for law enforcement investigations, and/or would disclose guidelines for law enforcement investigations that could reasonably be expected to risk circumvention of the law.

If you need to contact CBP about this matter, please contact the Department of Justice Attorney, David Glass at David.Glass@usdoj.gov.

Sincerely,



Charlyse Hoskins
Government Information Specialist

Enclosures

# EXHIBIT R

## Lally, Claire M.

**From:** Wilkens, Scott B.
**Sent:** Tuesday, October 10, 2017 3:19 PM
**To:** Carrie DeCell; 'Katie Fallow'
**Cc:** Stewart, Michael E.
**Subject:** FW: Knight: CBP: Item 5

FYI

-----Original Message-----
From: Wilkens, Scott B.
Sent: Wednesday, October 04, 2017 4:18 PM
To: 'Glass, David (CIV)' <David.Glass@usdoj.gov>
Subject: RE: Knight: CBP: Item 5

David,

Yes, this proposal is fine with Plaintiff. If CBP runs the search described in your September 27, 2017 email below and produces all non-exempt portions of any responsive records that it identifies, Plaintiffs will consider CBP to have complied in full with Item 5 of its request.

Scott

-----Original Message-----
From: Glass, David (CIV) [mailto:David.Glass@usdoj.gov]
Sent: Wednesday, October 04, 2017 2:27 PM
To: Wilkens, Scott B. <SWilkens@jenner.com>
Subject: FW: Knight: CBP: Item 5

Scott –

I'm not sure we closed the loop on this. Is this proposal OK with your side?

David

-----Original Message-----
From: Glass, David (CIV)
Sent: Wednesday, September 27, 2017 11:55 AM
To: Wilkens, Scott B. <SWilkens@jenner.com>
Cc: Stewart, Michael E. <MStewart@jenner.com>
Subject: RE: Knight: CBP: Item 5

Scott –

CBP proposes in view of your email dated September 20, 2017, to search its complaint management system for records dating from January 1, 2012, relating to the CBP Office of Field Operations, frequent searches or delays, CBP's procedures and policies, and CBP's search authority using the following search terms: "electronic device," "phone," "cellphone," "laptop," "iPad," "mobile device," "computer," "cellular device," "tablet," "mobile phone," and "PDA."

Please let me know whether plaintiff will consider CBP to have complied in full with Item 5 of its request if it conducts the above search and produces all non-exempt portions of any responsive record that it identifies, i.e., any record that contains one or more of the above search terms and contains or relates to complaints about CBP's search, review, retention, or sharing of the information on travelers' electronic devices.

David

-----Original Message-----
From: Wilkens, Scott B. [mailto:SWilkens@jenner.com]
Sent: Wednesday, September 20, 2017 9:17 AM
To: Glass, David (CIV) <DGlass@CIV.USDOJ.GOV>
Cc: Stewart, Michael E. <MStewart@jenner.com>
Subject: Re: Knight: CBP: Item 5

David,

Plaintiff will consider CBP to have complied in full with Item 5 if its search includes the following additional search terms in its search, and it produces all non-exempt portions of any records it identifies:

computer
cellular device
tablet
mobile phone
PDA

Please let me know if that is agreeable to CBP.

Thanks,
Scott

On Sep 15, 2017, at 2:13 PM, Glass, David (CIV) <David.Glass@usdoj.gov<mailto:David.Glass@usdoj.gov>> wrote:

Scott –

CBP advises that it can use single-term searches to search the complaint management system for records relating to the CBP Office of Field Operations, frequent searches or delays, CBP's procedures and policies, and CBP's search authority. It therefore proposes to conduct a search for records in those categories dating from January 1, 2012, using the following search terms: "electronic device," "phone," "cellphone," "laptop," "iPad," and "mobile device."

Please let me know whether plaintiff will consider CBP to have complied in full with Item 5 of its request if it conducts the above search and produces all non-exempt portions of any responsive records that it identifies.

David

_____
Scott B. Wilkens

Jenner & Block LLP
1099 New York Avenue, N.W.
Suite 900, Washington, DC 20001-4412 | jenner.com<http://protect-us.mimecast.com/s/ESYtCYElEOIgEkG7uVbCAH?domain=jenner.com>

+1 202 639 6072 | TEL
SWilkens@jenner.com<mailto:SWilkens@jenner.com>
Download V-Card<https://protect-us.mimecast.com/s/vgBhCZ6m6PsxrPO6cxCwpa?domain=svcs.jenner.com> | View Biography<http://protect-us.mimecast.com/s/6vW0C1wBwKUO2nv4u1HMc1?domain=jenner.com>

CONFIDENTIALITY WARNING: This email may contain privileged or confidential information and is for the sole use of the intended recipient(s). Any unauthorized use or disclosure of this communication is prohibited. If you believe that you have received this email in error, please notify the sender immediately and delete it from your system.

_____

# EXHIBIT S

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

September 15, 2017

SENT BY ELECTRONIC MAIL TO: carrie.decell@knightcolumbia.org

Katherine Fallow
Knight First Amendment Institute
535 West 116th Street
314 Low Library
New York, NY 10027

RE: CBP-2017-042463; *Knight First Amendment Institute v. DHS*, No. 1:17-cv-00548-TSC (D.D.C.)

Dear Attorney Fallow:

This is an electronic interim response to your Freedom of Information Act (FOIA) request to U.S. Customs and Border Protection (CBP), dated March 20, 2017, and received by this office on March 24, 2017. You 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 instance 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
   b. ICE Directive No. 7-6.1

4. The following documents relating to any reviews of CBP's or ICE's polices 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 of Civil Rights and Civil Liberties, DHS's OIIG and CBP's Office of Internal Affairs, Management Inspection Division;
   b. Any policies, practices, procedures, and/or training material adopted as a result of any audits, impact assessments, or other reviews of how CBP and ICE conduct electronic device searches; and
   c. Any document 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 journalist," as referenced in § 5.2 of the CBP Directive.

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

A further search of CBP databases produced a total of 178 pages of records responsive to your request. Per the August 14, 2017 Second Joint Status Report in *Knight First Amendment Institute at Columbia University v. DHS, et al.*, this release includes records responsive to request numbers 1, 4, and 7. CBP has determined that 178 pages are partially releasable pursuant to Title 5 U.S.C. § 552 (b)(6), (b)(7)(C) and (b)(7)(E).

Enclosed are 178 pages with certain information withheld as described below:

**FOIA Exemption (b)(6)** exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a

balancing of the public's right to disclosure against the individual's right privacy. The types of documents and/or information that we have withheld may consist of birth certificates, naturalization certificates, driver license, social security numbers, home addresses, dates of birth, or various other documents and/or information belonging to a third party that are considered personal. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

**FOIA Exemption (b)(7)(C)** protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. This exemption takes particular note of the strong interests of individuals, whether they are suspects, witnesses, or investigators, in not being unwarrantably associated with alleged criminal activity. That interest extends to persons who are not only the subjects of the investigation, but those who may have their privacy invaded by having their identities and information about them revealed in connection with an investigation. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate.

**FOIA Exemption (b)(7)(E)** protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or 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. CBP has determined that disclosure would disclose techniques or procedures for law enforcement investigations, and/or would disclose guidelines for law enforcement investigations that could reasonably be expected to risk circumvention of the law.

If you need to contact CBP about this matter, please contact the Department of Justice Attorney, David Glass at David.Glass@usdoj.gov.

Sincerely,

Charlyse Hoskins
Government Information Specialist

Enclosures

# EXHIBIT T

*Freedom of Information Act Office*

**U.S. Department of Homeland Security**
500 12th St SW, Stop 5009
Washington, DC 20536

U.S. Immigration and Customs Enforcement

June 16, 2017

Katherine Fallow
Knight First Amendment Institute
at Columbia University
314 Low Library
535 West 116th Street
New York, NY 10027

**RE: ICE FOIA Case Number 2017-ICLI-00011; *Knight First Amendment Institute v. Department of Homeland Security* (17-cv-548-TSC)**

Dear Ms. Fallow:

This letter responds to the Freedom of Information Act (FOIA) request to U.S. Immigration and Customs Enforcement (ICE), submitted by your client Knight First Amendment Institute, dated March 15, 2017. In the FOIA request your client has requested copies of the following records:

1. Documents 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 fiscal year 2012
2. Documents relating to each instance since fiscal year 2012 in which CBP or ICE searched, detained, retained or shared an electronic device or the information accessible on it
3. Revisions of or documents supplementing or superseding the CBP and ICE directives concerning border searches of electronic devices
4. Certain documents relating to any reviews of CBP's or ICE's policies or practices concerning electronic device searches
5. Documents concerning or relating to complaints filed by individuals or organizations about CBP's or ICE's search, review, retention or sharing of the information on travelers' electronic devices
6. Documents reflecting policies, practices or procedures concerning how CBP officers handle "privileged or other sensitive materials," including "work-related information carried by journalists" as described in the CBP directive concerning border searches of electronic devices
7. Documents reflecting policies, practices and procedures concerning CBP's anti-discrimination policy as applied to discretionary electronic device searches.

**This Production**

ICE has processed for release, and encloses, 108 pages and seven (7) excel spreadsheets, located by a search of ICE Offices of Homeland Security Investigations (HIS), Professional Responsibility (OPR), Office of Policy and Office of Principal Legal Advisors (OPLA). Per the June 5, 2017 Joint Status Report, these documents are responsive to item numbers one (1) and four (4). These documents have been Bates numbered 2017-ICLI-00011 1 through 2017-ICLI-00011 108. Portions of these documents have been withheld pursuant to FOIA Exemptions 5, 6, 7(C) and 7(E) of the FOIA.

ICE has applied FOIA Exemption 5 to withhold draft documents under the deliberative process privilege, the general purpose of which is to prevent injury to the quality of agency decisions, as well as the attorney-client privilege and the attorney work product privilege.

**FOIA Exemption (5)** exempts from disclosure inter-agency or intra-agency memorandums or letters, which would not be available by law to a party other than an agency in litigation with the agency.

ICE has applied FOIA Exemptions 6 and 7(C) to protect from disclosure the names, e-mail addresses, and phone numbers of ICE and DHS employees contained within the documents, as well as the names, and other personally identifiable information of other individuals contained within the records.

**FOIA Exemption 6** exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

**FOIA Exemption 7(C)** protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. This exemption takes particular note of the strong interests of individuals, whether they are suspects, witnesses, or investigators, in not being unwarrantably associated with alleged criminal activity. That interest extends to persons who are not only the subjects of the investigation, but those who may have their privacy invaded by having their identities and information about them revealed in connection with an investigation. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, I have determined that the privacy interest in the identities of individuals in the records you have requested clearly outweigh any minimal public interest in disclosure of the information. Please note that any private interest you may have in that information does not factor into this determination.

ICE has applied FOIA Exemption 7(E) to protect from disclosure internal agency law enforcement case numbers, internal codes, agency software and hardware information, and instructional manuals, user manuals, and training materials related to a law enforcement system and database which contain law enforcement sensitive techniques and procedures that are not well known to the public.

**FOIA Exemption 7(E)** protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or 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. I have determined that disclosure of certain law enforcement sensitive information contained within the responsive records could reasonably be expected to risk circumvention of the law. Additionally, the techniques and procedures at issue are not well known to the public.

If you need to contact ICE about this matter, please contact the Department of Justice Attorney, David Glass at David.Glass@usdoj.gov.

Sincerely,

Catrina M. Pavlik-Keenan
FOIA Officer

Enclosure(s): 108 page(s)
7 Excel sheets

# EXHIBIT U

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 1, 2017

Jenner & Block, LLP
Scott Wilkens
1099 New York Ave, NW
Suite 900
Washington, DC 200001

**Re: 17-cv-00548 (2017-HQFO-00585)**
**Knight First Amendment Institute v. DHS**
**First Interim Release**

Dear Mr. Wilkens:

This is our first interim response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated March 15, 2017.

For this month's production DHS reviewed 56 documents consisting of 653 pages of which 120 pages are released in full; 97 pages are withheld in full pursuant to FOIA exemption 5; 43 pages are released in part pursuant to FOIA exemption 5 and 6; 41 pages were duplicates and 237 pages were non-responsive. DHS also located 125 pages that need to be referred to other components for review and release, 51 pages to CBP (Customs and Border Protection) and 74 pages to the (DOJ) Department of Justice. The 260 pages for release are bates stamped DHS-001-585-000001 to DHS-01-585-000260.

Sincerely,

Kevin L. Tyrrell
Director FOIA Appeals and Litigation

Enclosure

# EXHIBIT V

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 30, 2018

Knight First Amendment Institute of Columbia University
475 Riverside Drive
Suite 302
New York, NY 10115

**Re: 17-cv-00548 (2017-HQFO-00585)**
**Knight First Amendment Institute v. DHS**
**Third Interim Release**

Dear Mr. Wilkens:

This is our third interim release to your Freedom of Information Act (FOIA) request to the U.S. Department of Homeland Security (DHS), dated March 7, 2017. This letter describes the agency's processing efforts to date. We understand that this information will be provided to the Court supervising the civil litigation concerning this FOIA request.

***DHS's Searches and Production***

For this month's production DHS reviewed 848 pages of which 250 pages are released in full, 89 pages are released in part with redactions made pursuant to FOIA Exemptions 5 and 6, 414 pages are withheld in full pursuant to FOIA Exemptions 5 and/or 7(E) and 44 pages are non-responsive. An additional 14 pages were duplicates and 37 pages have been referred to U.S. Customs and Border Protection (CBP) for review and a direct response to you. CBP contact information is provided below.

CBP FOIA Officer/Public Liaison: Sabrina Burroughs
1300 Pennsylvania Avenue, NW, Room 3.3D
Washington, D.C. 20229

The 753 pages for release are attached and bates stamped DHS-001-513-000351 to DHS-01-513-001103. If you need to contact our office about this matter, please refer to **2017-HQFO-00585**. You may contact this office at 1-866-431-0486 or 202-343-1743.

Sincerely,

Kevin L. Tyrrell
Director FOIA Appeals and Litigation