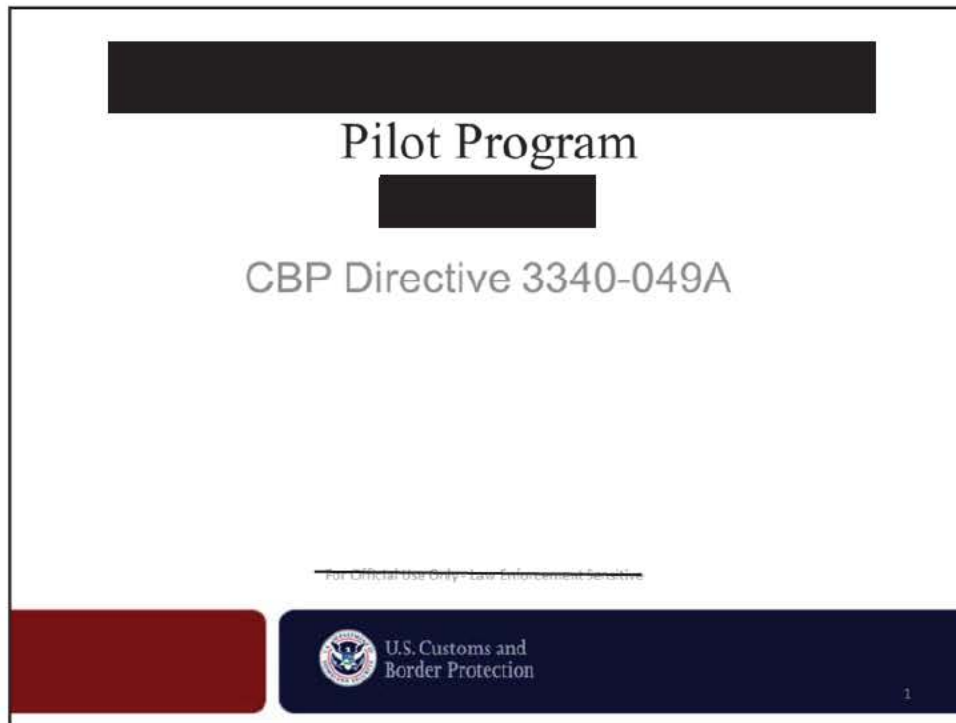


EXHIBIT 31




As more and more travelers carry information in electronic form, the frequency of examining electronic devices naturally tends to increase. Even with this, these types of searches occur in extremely small percentage of border crossings. The vast majority of travelers who cross the border with a laptop or other electronic device enter the United States without CBP ever inspecting their device.

- For FY 2017, there were 388,379,188 total passengers and only 30,150 Border Searched of Electronic Devices. Statics show that on the average xx of electronic devices were search

TECS Mod Electronic Media Report

- February 18, 2016
- IOEM is required
- Narrative
 - Supervisor witness/notification
 - Tear Sheet
 - “Media Screening Equipment”
- Supervisor Approval

For Official Use Only - Law Enforcement Sensitive



U.S. Customs and
Border Protection

11

In order to effectively monitor electronic media searches, the Office of Information Technology, in conjunction with Tactical Operations Division, developed the function in TECS to capture the specifics of these very sensitive searches.

TECS Mod Electronic Media Report went into production on February 18, 2016.

- IOEM is required
- Narrative should identify witnessing supervisor or supervisory notification information.
- Narrative must include a statement that the tear sheet was presented to the individual or an articulation of why the tear sheet was not provided
- Narrative must NOT include the term [REDACTED] or specific names of equipment, example is to use “media screening equipment”
- Supervisor must approve IOEM by the end of work shift.

Inspection of Operations Electronic Media Tracking (IOEM)- Background

- On January 1, 2012, IOEM became the primary function for capturing the search of electronic devices.
- The IOEM is a TECS transaction used to track and record searches of electronic media devices, such as cell phones and laptop computers, which are detained, seized, destroyed, transferred to another agency, or returned to the traveler during a secondary inspection.
- The tracking and recording of electronic media/devices is completed as part of a traveler’s inspection when entering and/or exiting the United States. Email notifications are generated throughout this process to notify record owners (and their supervisors), that actions have been or need to be completed to close an IOEM report.
- The IOEM functionality was developed in response to a Management Inspection Division recommendation that was further endorsed by the DHS’s Civil Rights Civil Liberties Unit.

EXHIBIT 32

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS**

GHASSAN ALASAAD, NADIA ALASAAD,)
SUHAIB ALLABABIDI, SIDD BIKKANAVAR,))
JÉRÉMIE DUPIN, AARON GACH, ISMAIL)
ABDEL-RASOUL AKA ISMA'IL)
KUSHKUSH, DIANE MAYE, ZAINAB)
MERCHANT, MOHAMMED AKRAM SHIBLY,)
AND MATTHEW WRIGHT,)

Plaintiffs,)

v.)

Civil Action No. 17-cv-11730-DJC

KIRSTJEN NIELSEN, SECRETARY OF)
THE U.S. DEPARTMENT OF HOMELAND)
SECURITY, IN HER OFFICIAL CAPACITY;)
KEVIN MCALEENAN, ACTING)
COMMISSIONER OF U.S. CUSTOMS AND)
BORDER PROTECTION, IN HIS OFFICIAL)
CAPACITY; AND THOMAS HOMAN, ACTING)
DIRECTOR OF U.S. IMMIGRATION AND)
CUSTOMS ENFORCEMENT, IN HIS OFFICIAL)
CAPACITY,)

Defendants.)

MEMORANDUM IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

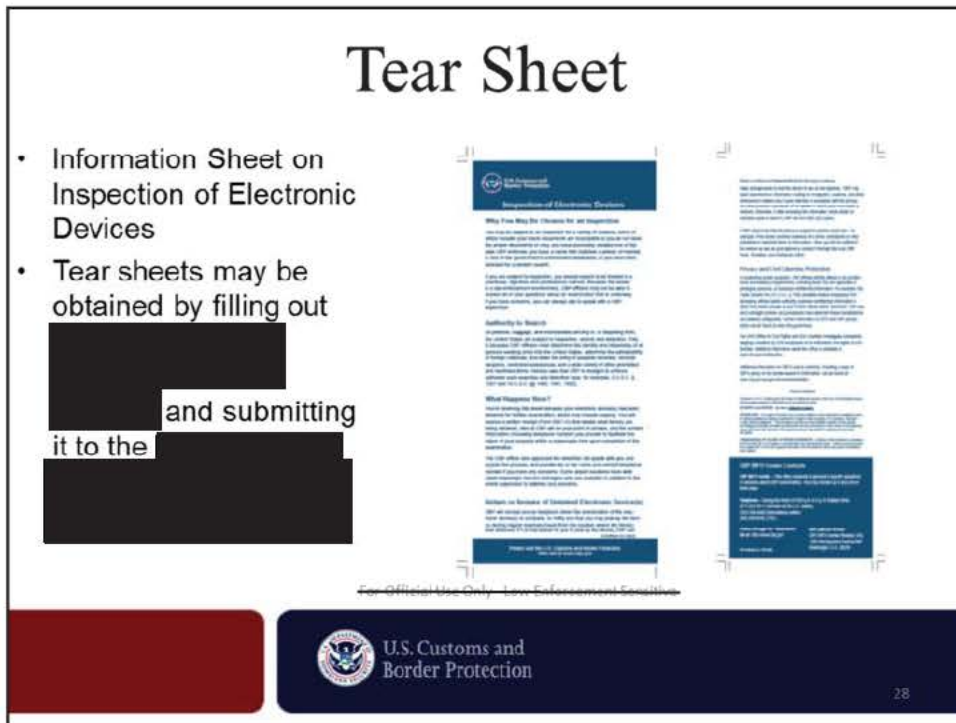
‘substantial risk’ that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper v. Amnesty Int’l*, 568 U.S. 398, 414 n.5 (2013)). “[A]llegations of possible future injury are not sufficient.” *Clapper*, 568 U.S. at 409 (citation omitted).

By limiting the judicial power to instances where specific individuals have suffered concrete injuries, standing requirements “serve[] to prevent the judicial process from being used to usurp the powers of the political branches.” *Id.* at 408. A court’s standing inquiry should, therefore, be “especially rigorous when reaching the merits of the dispute” would compel it “to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional.” *Id.* (citation omitted).

Plaintiffs base their claim to Article III standing on three types of purported injury. First, Plaintiffs state that they all “face a likelihood of future injury,” because when Plaintiffs travel internationally they will “be subject to” Defendants’ policies and practices, and are therefore allegedly at risk of a future device border search. Am. Compl. ¶ 156. Second, Plaintiffs claim they “are suffering the ongoing harm” of Defendants retaining (a) content copied from their devices or records reflecting content observed during searches, (b) content copied from their cloud-based accounts, (c) their social media identifiers “and/or,” (d) their device passwords. Am. Compl. ¶ 157. Finally, Plaintiffs contend that they “will be chilled from exercising their First Amendment rights of free speech and association[.]” Am. Compl. ¶162.⁵ None of these

⁵ Plaintiffs separately claim that Suhaib Allababidi has standing because Defendants are still allegedly in possession of his cellphone. Am. Compl. ¶ 158. However, Mr. Allababidi’s phone was in fact returned to him on December 13, 2017, as indicated by the signed acknowledgement attached hereto as Exhibit A. Because the return of the phone does not implicate any of Plaintiffs’ legal claims, and only the existence of injury, the Court “is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case.” *Torres-Negron v. J & N Records, LLC*, 504 F.3d 151, 163 (1st Cir. 2007) (citation omitted). And since Plaintiff can no longer claim that he is “suffering the ongoing harm of the confiscation of his device,” nor that he

EXHIBIT 33



MUST be presented to all individuals that have an electronic device detained or seized, **EXCLUDING** those instances involving [redacted] operations.

The reality...

<http://www.cbp.gov/xp/cgov/travel/admissibility/>

Tear sheets may be obtained by filling out CBP form [redacted] and submitting it to the [redacted]

(Return or Seizure of Detained Electronic Device(s) continue)

CBP can make arrangements to ship the device to you at our expense. CBP may retain documents or information relating to immigration, customs, and other enforcement matters only if such retention is consistent with the privacy and data protection standards of the system in which such information is retained. Otherwise, if after reviewing the information, there exists no probable cause to seize it, CBP will not retain any copies.

If CBP determines that the device is subject to seizure under law – for example, if the device contains evidence of a crime, contraband or other prohibited or restricted items or information – then you will be notified of the seizure as well as your options to contest it through the local CBP Fines, Penalties, and Forfeitures Office.

Privacy and Civil Liberties Protection

In conducting border searches, CBP officers strictly adhere to all constitutional and statutory requirements, including those that are applicable to privileged, personal, or business confidential information. For example, the Trade Secrets Act (18 U.S.C. § 1905) prohibits federal employees from disclosing, without lawful authority, business confidential information to which they obtain access as part of their official duties. Moreover, CBP has strict oversight policies and procedures that implement these constitutional and statutory safeguards. Further information on DHS and CBP privacy policy can be found at www.dhs.gov/privacy.

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.

Additional information on CBP's search authority, including a copy of CBP's policy on the border search of information, can be found at: www.cbp.gov/xp/cgov/travel/admissibility/.

Privacy Act Statement

Pursuant to 5 U.S.C. § 552a (e)(3), this Privacy Act Statement serves to inform you of the following concerning the possible collection of information from your electronic device

AUTHORITY and PURPOSE: See above, [Authority to Search](#).

ROUTINE USES: The subject information may be made available to other agencies for investigation and/or for obtaining assistance relating to jurisdictional or subject matter expertise, or for translation, decryption, or other technical assistance. This information may also be made available to assist in border security and intelligence activities, domestic law enforcement and the enforcement of other crimes of a transnational nature, and shared with elements of the federal government responsible for analyzing terrorist threat information.

CONSEQUENCES OF FAILURE TO PROVIDE INFORMATION: Collection of this information is mandatory at the time that CBP or ICE seeks to copy information from the electronic device. Failure to provide information to assist CBP or ICE in the copying of information from the electronic device may result in its detention and/or seizure.

CBP INFO Center Contacts

CBP INFO Center – This office responds to general or specific questions or concerns about CBP examinations. You may contact us in any one of three ways:

Telephone – During the hours of 8:30 a.m. to 5 p.m. Eastern time:
 (877) 227-5511 (toll-free call for U.S. callers)
 (703) 526-4200 (international callers)
 (866) 880-6582 (TDD)

Online through the "Questions" tab at:
<http://www.cbp.gov>

Mail address format:
 CBP INFO Center (Rosslyn, VA)
 1300 Pennsylvania Avenue NW Washington, D.C. 20229

CBP Publication 0204-0709

EXHIBIT 34

WRITTEN STATEMENT FOR THE RECORD OF
U.S. Customs and Border Protection
For A Hearing Entitled “Examining Warrantless Smartphone Searches at the Border”
U.S. Senate
Committee on Homeland Security and Governmental Affairs
Subcommittee on Federal Spending Oversight and Emergency Management
July 11, 2018, Washington, DC

Introduction

Chairman Paul, Ranking Member Peters, and Members of the Subcommittee: Thank you for the opportunity to testify before you today on U.S. Customs and Border Protection’s (CBP) authorities on border searches of electronic devices. Keeping Americans safe by enforcing our nation’s laws in an increasingly digital world depends on our ability to lawfully inspect all materials—electronic or otherwise—entering the United States.

All persons, baggage, and merchandise arriving in or departing from the United States are subject to inspection, search, and detention by CBP—and signage posted throughout the port areas informs travelers of this fact. These border searches further CBP’s customs, immigration, law enforcement, and homeland security responsibilities, and ensure compliance with customs, immigration, and other laws that CBP is authorized to administer and enforce. All individuals crossing the border, regardless of citizenship, must present themselves and their effects for border inspection. CBP’s search authority is essential to enforcing the law at the U.S. border, preserving our national security, ensuring public safety, and protecting our country’s economic interests.

CBP’s authority to engage in border searches has been repeatedly affirmed by the Supreme Court of the United States. In addition to longstanding federal court precedent recognizing the constitutional authority of the U.S. government to conduct border searches, numerous federal statutes and regulations also authorize CBP to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property, which would include electronic devices. Congress’ long-standing recognition of the vital importance of inspections at the border reaches back to the First Congress. The long history of statutes authorizing CBP and its predecessor agencies to inspect and examine all individuals and merchandise entering or departing the United States demonstrates the importance of this authority. Congress has entrusted CBP with conducting border inspections to interdict threats to our nation, and we take this responsibility very seriously.

CBP Border Searches of Electronic Devices

Electronic devices are defined as any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, and music and other media players—and there is no question that these devices are prevalent in this digital age. In the past, someone might bring a briefcase across the border. This briefcase might contain pictures of their friends or family, work

materials, personal notes, diaries or journals, or any other type of personal information. Today, all of that material can fit neatly in a smartphone. As the world of information technology evolves, techniques used by CBP and other law enforcement agencies must also evolve to identify, investigate, and prosecute individuals who use new technologies to commit crimes.

Because of CBP's authority to inspect electronic devices at the border, CBP personnel have uncovered evidence related to terrorism, bulk cash smuggling, contraband, human trafficking, and child pornography. Our CBP personnel have also uncovered information about financial and commercial crimes, such as those relating to copyright, trade, and export control violations. Through these search authorities, CBP has gained vital information that has helped us assess and analyze terrorist threat information. Furthermore, searches at the border are often integral to determining an individual's intentions upon entry into the United States, providing additional information relevant to their admissibility under our country's immigration laws.

CBP personnel are trained to assess a "totality of circumstances" when determining appropriate actions to take during a border inspection. CBP may engage in various actions during a border inspection, such as an examination of the travelers' belongings including their personal vehicle, suitcase, briefcase, and now, electronic devices. In the context of border searches of electronic devices, a search may be conducted for a variety of reasons. For example, if the traveler is suspected of illegal activity, that traveler may be referred for additional scrutiny and a search of their device. A search of an electronic device may also assist CBP personnel in verifying information that may be pertinent to the admissibility of a foreign national who is applying for admission.

CBP takes the responsibility associated with these search authorities seriously. On January 5, 2018, CBP released an update to the agency Directive governing Border Searches of Electronic Devices, superseding the previous Directive released in August 2009. The January 2018 Directive, *Border Search of Electronic Devices*, includes updated guidance and standard operating procedures on searching, reviewing, retaining, and sharing information contained on electronic devices. It also furthers our commitment to a culture of transparency, accountability, and oversight of electronic device border searches performed by CBP.

The Directive governs border searches of electronic devices—including any inbound or outbound search pursuant to longstanding border search authority—conducted by CBP at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy.

With respect to border searches of information contained in electronic devices, the original 2009 policy did not differentiate between the types of searches that CBP conducts on an electronic device. Under the new 2018 policy, CBP has updated the definitions of these searches and outlined the procedures that apply to each respective type of search. CBP now follows different procedures depending on whether the search is a "basic search" or an "advanced search." A basic search may be conducted with or without suspicion, while the Directive requires, strictly as a matter of policy, additional justification for an advanced search.

EXHIBIT 35

Instructor Guide – P180C [REDACTED] Overview

Why Search Electronic Media?

Search of electronic media can detect evidence related to [REDACTED] such as:

- Possible evidence of surveillance
- Human/cash smuggling
- Narcotics and contraband
- Financial and commercial crimes



U.S. Customs and
Border Protection

For Official Use Only

2-25

Instructor Guidance

Read to Trainees:

[REDACTED]

Electronic Media

CBP's search of electronic media is essential to enforcing law at the U.S. border.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

CBP’s authority in electronic media

*Border Search of Electronic Devices Directive
3340-049A, January 4, 2018*

- In the course of a border search, with or without individualized suspicion
- A CBP officer may examine electronic devices and may review and analyze the information encountered at the border, subject to the requirements provided in the Border Search of Electronic Devices Directive
- Any action taken with an electronic device or storage media must be captured and recorded utilizing [REDACTED]



U.S. Customs and
Border Protection

For Official Use Only

2-27

Instructor Guidance

CBP border search authority is derived from federal statutes and regulations, including 19 CFR 162.6:

“All persons, baggage and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection by a CBP officer.”

Have trainees refer to Inspection of Electronic Devices Tear Sheet located in P180C folder on iPad.

An information sheet on Inspection of Electronic Devices **MUST** be presented to all travelers having an electronic device detained or seized, **EXCLUDING** those involving instances of **NATIONAL SECURITY** or ongoing **INVESTIGATIONS**.

Border Search Authority:

- CBP Officers
- Border Patrol Agents
- Air Interdiction Agents
- Marine Interdiction Agents
- Other Employees Authorized to Perform Searches at the Border

Note: U.S. Immigration and Customs Enforcement (ICE) exercises concurrently-held border search authority that is covered by their own policy and procedures.

All actions must be documented in IOEM and require the following information:

- Number of and type of electronic media
- Make, Model, and Serial Number of every device
- Notations of any time the media were turned on and off
- Narrative including all pertinent details relating to BSI actions (Refer to BSI Job Aid)

EXHIBIT 36

PRIORITY REQUESTS:

Homeland Security Investigations

1. For 2015, 2016, and 2017 please identify the number of basic searches of electronic devices were conducted by HSI. **HSI does not track the basic searches of electronic devices conducted pursuant to border search authority. Since HSI's role is investigative and an advanced search is preferable for the judicial process, HSI generally conducts advanced searches and tracks such searches when it has opened an investigation. HSI is less likely to encounter a device in an interdiction role when a basic search would be more likely.**
 - a. Of those searches, how many were of:
 - i. USCs
 - ii. LPRs
 - iii. Others (i.e. foreign nationals) HSI does not track the citizenship, nationality, or immigration status of the individuals who possess the electronic devices searched. Border search is a customs authority and the citizenship, nationality, or immigration status of the individual whose property is searched is irrelevant to HSI's exercise of that authority.
2. For 2015, 2016, and 2017 please identify the number of advanced searches of electronic devices were conducted by HSI.
 - a. Of those searches, how many were of:
 - i. USCs
 - ii. LPRs
 - iii. Others (i.e. foreign nationals)

ADDITIONAL REQUESTS:

Homeland Security Investigations

1. Please describe the role that HSI plays in screening of electronic devices? **During a border search, HSI can encounter a myriad of electronic devices like phones, tablets, thumb drives and SD Cards. HSI does not screen devices but will conduct a basic or advanced search of any devices depending on operational and investigative needs.**
 - a. Does HSI conduct both basic and advanced screening of electronic devices? **HSI conducts either a basic or advanced search of the electronic device based on the particular circumstances of each situation, including the limitations of the device to be searched. For example, some devices may require particular software or hardware to be accessed and searched.**
2. What are the factors that determine if and when a basic and/or advanced search of an electronic device is conducted? **The particular circumstances of each situation will determine how a search will be conducted. Factors considered may include the particular device to be searched, its accessibility, its capacity, any encryption, the individual searched, the information sought, the level of suspicion, and the status of the investigation.**

3. By year, please identify the number of referrals made to other law enforcement agencies (by agency) based upon, in part, the screening of an individual's electronic device. **HSI does not track this and does not have the requested data.**

4. By year, please identify the number of criminal arrests, indictments by nearly, search warrants, and/or seizures occurred based upon, in part, the screening of an individual's electronic device. **There is no feasible way to produce meaningful statistics for this request. While a number could be produced that identified cases where a border search of an electronic device was conducted, that may not be indicative that the search supported any particular arrest, indictment, search warrant, or seizure. HSI Investigations involve a myriad of factors that would justify an arrest, indictment, or search warrant of which a border search would only be one factor of many. For example, if an individual is encountered smuggling methamphetamine into the US he would be arrested for smuggling and a border search would be conducted on his devices for co-conspirators. HSI arrest would not be as a result of the border search but may contribute to the follow-on investigation for co-conspirators.**

EXHIBIT 37

~~FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE~~

Homeland Security and Governmental Affairs Committee

EXECUTIVE SUMMARY

U.S. Customs and Border Protection (CBP) participated in a briefing for staff of the Homeland Security and Governmental Affairs Committee (HSAGC), Senators Ron Johnson, Steve Daines, Patrick Leahy, and Claire McCaskill on April 30, 2018. Deputy Executive Assistant Commissioner Wagner briefed the group on CBP's policies and practices regarding border searches of electronic devices. Director [REDACTED] of CBP's National Targeting Center, Counterterrorism Division, provided examples of border searches of electronic devices – that were undertaken without any requirement of probable cause or reasonable suspicion – that resulted in the identification of information relevant to CBP's counterterrorism mission.

BACKGROUND

The Government has well-established, plenary authority to conduct searches and inspections of persons and merchandise crossing our nation's borders; control of the border is a fundamental attribute of sovereignty. As the Supreme Court has explained, "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). The Supreme Court has recognized that the Government's "interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). In addition to the long-standing Supreme Court precedent recognizing border search authority, numerous federal statutes explicitly authorize searches of people and things entering the United States. *See, e.g.*, 19 U.S.C. §§ 482; 1461; 1496; 1581; 1582.

These authorities are essential to CBP's ability to fulfill its statutory responsibilities, including among others, to "ensure the interdiction of persons and goods illegally entering or exiting the United States"; "detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States"; "safeguard the borders of the United States to protect against the entry of dangerous goods"; "enforce and administer all immigration laws"; "deter and prevent terrorists and terrorist weapons from entering the United States"; and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons." 6 U.S.C. § 211.

On January 4, 2018, U.S. Customs and Border Protection (CBP) issued CBP Directive No. 3340-049A, Border Search of Electronic Devices (The Directive) to provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in electronic devices subject to inbound and outbound border searches. The Directive superseded and updated CBP's prior guidance, which was issued in 2009. The Directive fulfilled the requirement in the Trade Facilitation and Trade Enforcement Act of 2015, codified at 6 U.S.C. § 211(k), to review and update the standard operating procedures for searching, reviewing, retaining, and sharing information contained in communication, electronic, or digital devices encountered by CBP personnel at United States ports of entry, a requirement that must be fulfilled every three years. The Directive also took into account the evolution of the operating environment since the 2009 guidance was issued, along with advances in technology and continuing developments.

~~FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE~~

~~FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE~~

- j. Number of referrals made to a law enforcement agency (by agency) as a result of a secondary screening that included a basic screening of an electronic device
 - i. Identify the law enforcement agencies and the number of referrals sent to each
- k. Number of referrals made to a law enforcement agency (by agency) as a result of a secondary screening that included an advanced screening of an electronic device
 - i. Identify the law enforcement agencies and the number of referrals sent to each

1.j-k CBP coordinates with FBI and HSI, as appropriate, when encountering matters within their subject matter expertise, including terrorism, drug trafficking, child pornography.

See chart below.

IOEM Incident Count - (10/1/2015 - 9/30/2017)
[REDACTED]

~~FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE~~

EXHIBIT 38



Privacy Impact Assessment
for the

U.S. Border Patrol
Digital Forensics Programs

DHS/CBP/PIA-053

April 6, 2018

Contact Point

Carla Provost

Acting Chief

United States Border Patrol

(202) 344-3159

Reviewing Official

Philip S. Kaplan

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) U.S. Border Patrol (USBP) conducts searches of electronic devices to identify violations of the laws CBP enforces or administers, including laws relating to the detection and apprehension of illicit goods and individuals entering and exiting the United States. Depending on the circumstances, CBP searches of electronic devices are conducted pursuant to different legal authorities. CBP is conducting this Privacy Impact Assessment (PIA) to analyze standalone information technology systems designed to retain and analyze information collected from electronic devices collected pursuant to a warrant, abandonment, or when the owner consented to a search of the device, and to identify trends and patterns of illicit activities. ***This PIA does not include searches conducted pursuant to border search authority.*** CBP is publishing this PIA because the USBP digital forensic program collects, retains, and analyzes personally identifiable information (PII) obtained from electronic devices.

Overview

CBP is responsible for securing the borders of the United States while facilitating lawful international trade and travel. CBP employs various technologies to enforce and administer hundreds of U.S. laws and regulations at the border, including immigration and narcotics enforcement laws. CBP is charged with enforcing compliance with numerous federal laws at the border to prevent contraband, other illegal goods, and inadmissible persons from entering and exiting the United States. CBP enforces these laws both at and between Ports of Entry (POE).

CBP works to identify, interdict, and apprehend individuals with ties to terrorism, as well as individuals facilitating operations involving: human, drug, weapon, bulk cash, and other contraband smuggling activities. Consistent with this mission, CBP Officers and Agents collect information from a variety of sources to conduct interdiction operations and support criminal investigations. As part of CBP's border security duties, CBP may search and extract information from electronic devices, including but not limited to: laptop computers; thumb drives; compact disks; digital versatile disks (DVDs); mobile phones; subscriber identity module (SIM) cards; digital cameras; and other devices capable of storing electronic information.¹

CBP Officers and Agents may search electronic devices in a variety of scenarios, including:

- **Border Search.** ***This PIA does not include searches conducted pursuant to border search authority.*** All travelers and the items they carry, including electronic devices, are subject to search by CBP when crossing the U.S. border. These searches apply to

¹ Unlike under CBP's border search authority, in certain circumstances USBP may access information from the cloud if the search of the electronic device is conducted pursuant to a warrant or consent. If cloud-based information is not specifically mentioned in the warrant, then USBP would not extract data from the cloud.

This PIA does not include searches conducted pursuant to border search authority.



Homeland Security

individuals seeking entry into or exit from the United States at the border or its functional equivalent, including at land, air, or sea POEs or at a location between POEs. CBP is authorized to conduct these searches to enforce immigration, customs, and other federal laws at the border. CBP provides notice and a thorough discussion of border searches of electronic devices in a newly updated PIA published in January 2018.² ***This PIA does not include searches conducted pursuant to border search authority.***

- **Warrant Search.** Warrants issued by a judge or magistrate may authorize CBP to search electronic devices. Such searches generally occur in furtherance of a criminal investigation, subsequent to a finding of probable cause by a judge or magistrate.
- **Consent Search.** Consent provided by the owner/possessor of the device may also authorize CBP to search the individual's electronic device. These searches usually are based on the belief that the device may contain information relevant to a law enforced or administered by CBP. The individual's consent may provide CBP authority to conduct the search in the absence of a warrant or other applicable authority. In this scenario, CBP generally requires written consent from the owner or individual in possession of the device. All consent must be voluntarily given, depending on the totality of the circumstances. To the extent that CBP has encountered individuals who do not speak English, CBP will follow all applicable policies.³ In the event that an individual declines to provide his or her consent, CBP may pursue a warrant authorizing a search of the device or determine if other legal options apply.
- **Abandonment Search.** CBP Officers and Agents regularly encounter abandoned property,⁴ including electronic devices. In some cases, CBP may suspect that the unclaimed property may be associated with a criminal act, whereas in others, CBP Officers and Agents may find an abandoned device under unusual circumstances (such as between POEs in the border zone). CBP may retrieve and search abandoned devices without any level of suspicion required.

When CBP encounters an electronic device pursuant to one of the scenarios listed above, the Officer or Agent may submit the electronic device for digital forensic analysis in accordance with

² See DHS/CBP/PIA-008(a) Border Searches of Electronic Devices (January 4, 2018), available at <https://www.dhs.gov/privacy>.

³ It is the policy of CBP to make reasonable efforts to provide meaningful access, free of charge, to persons with limited English proficiency to its operations, services, and other conducted activities and programs without unduly burdening the Agency's fundamental mission. This obligation applies to any medium of communication and to interactions with the public, including but not limited to, in-person or telephonic contact; written correspondence, including email; use of websites and newsletters; community engagement events and activities; and documents explaining CBP programs. See <https://www.cbp.gov/about/language-access>.

⁴ Generally, abandoned property in this context refers to personal property that a CBP Officer or Agent finds in the field or at the scene of a law enforcement action, and the individuals present disavow ownership of the property.

This PIA does not include searches conducted pursuant to border search authority.

EXHIBIT 39

H A N D B O O K

International Mail Operations and Enforcement Handbook



CIS HB 3200-06A
August 2001

Office of Field Operations
Trade Programs
Commercial Processing Division

U.S. CUSTOMS SERVICE

The USPS often asks that certain mail be cleared first, usually Express Mail (EMS), letters in trays from Western Europe, and any other mail that may be part of a special program. [REDACTED]

[REDACTED]. Giving processing priority to certain types of mail is [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5. LETTER CLASS MAIL SCREENING (19 CFR 145.1)

Letter class mail covers a range of articles including postcards, aerogrammes, letter packets, etc. mailed at the letter class rate or equivalent class or category of postage. All letter class mail, however, should be regularly examined to determine whether it contains anything other than correspondence. Letter class mail is not opened unless it appears to contain matter in addition to or other than correspondence, provided there is reasonable cause to suspect the presence of merchandise or contraband. When letter class mail is opened the correspondence is not to be read unless there is probable cause to believe that it may provide additional information concerning a violation and is therefore needed for further investigation or use in court.

Except in cases where the sender or addressee has given written consent (19 CFR 145-3), a search warrant shall be obtained before any correspondence is read, seized, or referred to another agency. For example, if there was [REDACTED], Customs would need to get a search warrant based on coherent facts before the correspondence could be read and used as evidence in the case. This does not affect Customs' right to seize the contraband and we may detain the correspondence while waiting for a search warrant.

When sealed letter class mail is opened for any reason, a Postal Service employee must be present and observe the opening. 19 CFR 145 Policy Statement (I) contains specific information regarding the handling of letter class mail.

[REDACTED]
[REDACTED] The officer examining the envelope also stamps the envelope "Opened by U.S. Customs" in a conspicuous place, but not over the postage cancellation or address if possible. The code for the reason the mail was opened must be recorded on the envelope that was opened and on the [REDACTED] (19 CFR 145 Policy Statement (G)). [REDACTED]:

EXHIBIT 40



Personal Search Handbook

Office of Field Operations

CIS HB 3300-04B

July 2004



U.S. Customs and
Border Protection

Chapter 2 What You Need to Know for a Personal Search

the 2-hour notification be made to an attorney, the detainee will not be given an opportunity to consult with counsel at any time before Miranda warnings are given by CBP officers and invoked by the detainee (see chapter 10, part II).

A CBP officer shall make the notification on behalf of the detainee. This should be accomplished by the supervisor or a passenger service representative (see Attachment 2).

The narrative of the TECS and/or IDENT/ENFORCE report shall include information on the person notified (friend or relative), what time the notification was made, and phone number of the person contacted. Should the detained person decide not to have someone contacted by CBP, the TECS and/or IDENT/ENFORCE report will note that decision.

p. Prolonged Detentions for Medical Examinations

Prolonged detentions are those lasting 8 hours or longer. You must notify the Port Director in all cases of prolonged detentions.

Prior to the enactment of actions which will result in a prolonged detention, the local Associate/Assistant Chief Counsel must be consulted for legal advice by the Port Director (GS-13 or above), acting Port Director, or the Director, Field Operations during normal working hours. After normal working hours, the Port Director will contact the Situation Room (SITROOM) (1-877-748-7666). The SITROOM will provide the Port Director with an on-call attorney from the Office of Chief Counsel. Port directors are not required to consult with counsel prior to moving a traveler to a medical facility if that traveler has confessed to carrying narcotics internally.

In all circumstances, when a person has been detained 8 hours from the time that supervisory approval was first given for any personal search or that a personal search was initiated, the ICE duty agent and/or the CBP prosecution officer will contact the U.S. Attorney's office.

The ICE duty agent and/or the CBP prosecution officer shall advise the U.S. Attorney's Office of the detention. If the Assistant U.S. Attorney (AUSA) believes that probable cause has been established, the ICE duty agent and/or the CBP prosecution officer will work with the AUSA to obtain an arrest or search warrant before a magistrate. If the AUSA determines that probable cause does not yet exist but believes that reasonable suspicion exists, he will so advise CBP. In such situations, it is the sole responsibility of CBP to determine whether the detention will be continued. If the AUSA believes that reasonable suspicion does not exist, CBP will release the detained person. The ICE duty agent and/or the CBP prosecution officer shall document on the TECS and/or IDENT/ENFORCE report any decision or guidance provided by the AUSA. The CBP may continue to detain a person while awaiting a response from the AUSA and/or the magistrate if reasonable suspicion is not dispelled. **NOTE:** Where certain judicial circuits, such as the Second and Fifth, require different time frames, CBP and the local U.S. Attorney's Office will ensure that those time frames are met in addition to the requirements set forth in this Handbook.

q. Written Reports

The written reports, either IDENT/ENFORCE, IOIL, or the SEACATS Incident Menu Selection (IOAA) will include both required data (indicated by an asterisk in TECS) and detailed narratives regarding the circumstances surrounding the search and/or detention.

h. Involuntary X-Rays

Involuntary searches require a court order.

Involuntary X-ray searches will be conducted **only** under the most extraordinary circumstances, and **never** on a pregnant woman or a woman who refuses a pregnancy test.

Port directors will consult with the local Associate/Assistant Chief Counsel and the duty ICE agent or CBP prosecution officer to determine whether to seek a court order for an involuntary X-ray search. If it is determined to proceed with such an X-ray search, and the duty ICE agent or CBP prosecution officer will contact the U.S. Attorney and request that a warrant be obtained to authorize the X-ray search.

i. Pregnancy Checks

Under no circumstances will a pregnant woman or a woman who refuses a pregnancy test be subjected to an X-ray search, either voluntarily or involuntarily.

When a woman is taken to the medical facility, be sure to advise medical personnel that a pregnancy check **must** be performed prior to an X-ray.

If a woman is pregnant or refuses a pregnancy check, a decision must be made by the Port Director after obtaining legal advice from CBP counsel as to whether or not to continue to detain the woman for a medical examination, which may include an MBM (see chapter 8).

j. Reading the X-Ray

Only medical personnel may read the X-ray and interpret whether it indicates the presence of foreign objects that may be merchandise. The CBP officers may **not** render an opinion regarding the interpretation of the X-ray.

If the on-duty physician is uncertain whether the person has a foreign object in his body following the reading of the X-ray, you may seek a radiologist to read the X-ray, if one is reasonably available. Record the conclusion of the medical person in the S/A/S, IOIL, or IDENT/ENFORCE report.

k. Foreign Objects Not Found

When medical personnel have determined that foreign objects are not present in the body, release the person and immediately transport him back to the CBP facility, **unless** medical personnel determine that a medical condition requires the person to remain at the medical facility **and** the person consents to remain. Document these circumstances in the narrative of the search report. Also, you must advise the person that he is responsible for the costs of additional medical treatment.

l. Inconclusive X-Ray

If medical personnel deem the X-ray inconclusive, a decision must be made by the port director after obtaining legal advice from CBP counsel as to whether to continue to detain the person for an MBM.

Chapter 8

Further Medical Examinations

Further medical examinations include body cavity searches and monitored bowel movements.

I. BODY CAVITY SEARCH

a. Body Cavity Search Defined

A *body cavity search* is any visual or physical intrusion into the rectal or vaginal cavity.

Body cavity searches shall be made **only** under the most exceptional circumstances.

b. Who May Conduct a Body Cavity Search

Only medical personnel may conduct a body cavity search. The CBP officers are prohibited from conducting body cavity searches themselves, or from causing a body cavity search to be conducted at a CBP facility.

c. Consent

If the person consents to the body cavity search or a pelvic examination, use the consent form (Appendix F) to document consent.

Thoroughly and carefully explain the language in the form. If the person writes anything on the form other than a signature, the consent may not be voluntary. The supervisor must review the consent form to ensure that it is properly signed. If there is any question as to the validity of the signed consent, contact the Associate/Assistant Chief Counsel for legal advice.

You must document your observations concerning the person's maturity, intelligence, education, and training in the TECS or IDENT/ENFORCE report. This information is important in proving that consent was voluntary.

d. Court-Ordered Involuntary Body Cavity Searches

Involuntary body cavity searches require a court order.

Port Directors (GS-13 or above) will consult with the local Associate/Assistant Chief Counsel and the duty ICE agent or CBP prosecution officer to determine whether to seek a court order for an involuntary body cavity search. If it is determined to proceed with a body cavity search, the duty ICE agent or CBP prosecution officer will contact the U.S. Attorney's office and request that a warrant be obtained to authorize the body cavity search.

II. MONITORED BOWEL MOVEMENT

a. Monitored Bowel Movement (MBM) Defined

An *MBM* is the detention of a person for the purpose of determining whether contraband or other material evidence is concealed in the alimentary canal.

EXHIBIT 41

**AMO Guidance on Conducting Searches of Electronic Devices
Under Authority Other Than Border Search Authority**

- 1 **PURPOSE.** Outline U.S. Customs and Border Protection (CBP) Air and Marine Operations (AMO) policy governing the search of electronic devices by AMO agents under authority other than border search authority.
- 2 **PROCEDURES.** AMO agents (herein after referred to as agents) authorized to conduct [REDACTED] operations will ensure conformity to this addendum when conducting activities that do not qualify as a border search.
- 3 **POLICY.**
 - 3.1 Agents utilizing [REDACTED] should obtain a search warrant when practicable prior to retrieving data from electronic devices, even when other legal authorities apply.
 - 3.2 **Consent**
 - 3.2.1 In the absence of a search warrant, agents may utilize the CBP "Consent to Search Electronic Device" form when retrieving data from electronic devices under voluntary consent of a subject.
 - 3.2.2 A consent search of information is permitted only to the extent of the scope of the particular consent provided. If consent is withdrawn prior to completing review of information on an electronic device, the agent will retain only the data reviewed up to the time that consent was withdrawn.
 - 3.3 Exigent circumstances may also permit an agent to conduct a warrantless search of an electronic device if he/she has probable cause and the exigent circumstances require immediate action. Depending on the circumstances, exigent circumstances may justify a warrantless search of an electronic device if there is a need to prevent the imminent destruction of evidence, or there is an imminent threat to the safety of the public or to the law enforcement officer.
 - 3.4 The Fourth Amendment allows for the warrantless search and seizure of abandoned property. Property is considered abandoned if: (1) the owner no longer intends to retain an expectation of privacy in the property; and (2) the abandonment is voluntary.
 - 3.5 Plain View Doctrine is an exception to the warrant requirement exists if an

EXHIBIT 42

1300 Pennsylvania Avenue NW
Washington, DC 20229




**U.S. Customs and
Border Protection**

FEB 14 2017

Information

MEMORANDUM FOR: Executive Director, Operations
Regional Director, Southeast Region
Regional Director, Southwest Region
Regional Director, Northern Region
All Directors, Air Operations
All Directors, Marine Operations
Director, Investigations

FROM: Edward E. Young 
Acting Executive Assistant Commissioner

SUBJECT: Air and Marine Cyber Investigations Team - Limited Operations

This memorandum serves as guidance for the initial roll-out of the Air and Marine Cyber Investigations Team (AMCIT). This guidance will be in effect for 6 months, immediately following approval of the AMCIT policy. During this 6-month period, the AMCIT will [REDACTED] collect data from electronic devices under the following legal authorities:

- Search warrant^{1 2}
- Abandonment exception³
- Consent exception⁴

Only AMO agents who have completed the [REDACTED]

¹ Limited to assisting other federal, state and local law enforcement agency partners in executing court orders applied for by that agency. AMO will not apply for any electronic device search warrants during Restricted Operations.

² [REDACTED]

³ The Fourth Amendment allows for the warrantless search and seizure of abandoned property. Property is considered abandoned if: (1) the owner no longer intends to retain an expectation of privacy in the property; and (2) the abandonment is voluntary.

⁴ A consent search of information is permitted only to the extent of the scope of the particular consent provided. If consent is withdrawn prior to completing review of information on an electronic device, the agent will retain only the data reviewed up to the time that consent was withdrawn.

EXHIBIT 43



Homeland Security Investigations

Search and Seizure Handbook

HSI HB 12-04 / September 14, 2012



U.S. Immigration
and Customs
Enforcement

6.3 The Fourth Amendment

The constitutional limitations on SAs' authority to conduct searches and seizures are found in the Fourth Amendment, which states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment protects against unreasonable searches and seizures and extends this protection to people and their property. It applies to all persons in the United States, whether citizen or noncitizen, and whether they are legally or illegally in the United States.

The Fourth Amendment also provides that all warrants shall be based on probable cause. The Fourth Amendment does not mandate a warrant for all searches or seizures, and the courts have recognized several exceptions under which a warrantless search is reasonable. (These exceptions, including border search authority, are discussed in subsequent chapters.)

The courts have overwhelmingly expressed a preference for searches and seizures with a warrant. As a result, it is always recommended that SAs obtain a warrant if time permits, if one of the specific exceptions to the warrant requirement does not apply, and especially if SAs have any doubt concerning whether or not a particular search or seizure requires a warrant.

6.4 Concept of Level of Suspicion

Ultimately, when an SA's conduct is challenged, a court will decide whether the SA acted in a reasonable manner. When determining whether the SA's actions were reasonable under the Fourth Amendment, the courts will compare the SA's conduct during the search or seizure to the level of suspicion that the SA had at the time the search or seizure was conducted. The level of suspicion is a label used to describe how certain the SA is that there was a violation of law. Generally, as a seizure or search grows broader in scope or becomes more intrusive, the required level of suspicion increases.

6.5 Articulate Facts

To establish a level of suspicion, the SA combines articulable facts – pieces of information that can be observed and put into words. The SA may use any reliable information to establish a level of suspicion, including, but not limited to:

- A. The SA's own observations of people and physical evidence.
- B. Information gathered from other SAs or other law enforcement officers. (Statements from law enforcement officers are generally presumed to be reliable.)

7.11.3 Proportionality and the Eighth Amendment

Seizures of property for forfeiture purposes should not only be “reasonable” within the meaning of the Fourth Amendment, but also be proportionate in terms of the Eighth Amendment, which states: “Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.” Defendants often attempt to avoid forfeiture by arguing that it is “excessive.” In considering a defendant’s arguments, the court will weigh the extent of the criminal activity against the value of the forfeited property. For example, if a defendant’s house is to be forfeited as a narcotics stash house, the court will consider the quantity of drugs stored in the house and how frequently the house was used for this purpose. SAs should be mindful of this potential defense against forfeiture and should document as much evidence as possible of criminal misuse, particularly in the case of facilitating properties.

7.11.4 Seizure Warrants

As with seizures of property for evidence, seizures of property for forfeiture may or may not require a warrant. If SAs have probable cause that an item is forfeitable as proceeds or for facilitation and if the SAs have lawful access to the property, SAs may make some seizures without a warrant. For example, SAs may conduct a warrantless seizure of a vehicle used to smuggle drugs if the vehicle is located on the public street. Likewise, if SAs are executing a search warrant at a house and observe money or other high value items that they have probable cause to believe are proceeds of the crime, they may seize the items for forfeiture without obtaining a seizure warrant.

However, if time allows, it is always recommended that the SAs obtain a seizure warrant. The use of a warrant, even if one is not required, will help to prevent legal challenges to the SAs’ conduct later in the forfeiture proceedings.

With the assistance of the USAO, SAs may obtain a seizure warrant for any seizure, whether the intended forfeiture proceedings will be administrative, civil, or criminal. When applying for a seizure warrant, an SA should prepare an affidavit establishing probable cause, which should contain the following:

- A. A section identifying the SA and describing the SA’s training and experience;
- B. A section specifically identifying the property to be seized;
- C. A section explaining the legal basis for seizure and forfeiture and citing the applicable laws;
- D. A section providing the background of the investigation leading up to the discovery of probable cause for the seizure of the property; and
- E. A section that establishes the SA’s probable cause for the seizure.

The SA will submit the seizure warrant, the supporting affidavit, and any sealing or other orders to a federal magistrate or district judge, swearing before the judge to the veracity of the affidavit. When issued, the warrant will command the SA or any authorized officer to execute the seizure within a 10-day period. Once executed, the SA must leave a copy of the warrant with the owner of the property or at the location where the property was seized. The SA must then return the warrant to the issuing judge or magistrate in a timely manner, specifying what property, if any, was located and seized pursuant to the warrant.

7.11.5 Asset Identification and Removal Groups

AIRGs are located in the SAC offices to assist criminal case agents with seizures of property for forfeiture. If SAs need additional expertise or assistance with forfeiture questions that arise during an investigation, they may contact the local AIRG. If an investigation holds the potential for significant seizures and forfeitures of property, the SAs should enlist the aid of the local AIRG as early in the investigation as possible.

Forfeitures of real property or businesses involve additional pre-seizure planning and forfeiture considerations. Only SAs assigned to an AIRG may seize real property. If a case holds the potential for forfeiture of real property or a business entity, the criminal case agent must request assistance from the local AIRG. The criminal case agent also should contact the local AIRG if the investigation involves any asset valued at more than \$100,000. (*See* the Asset Forfeiture Handbook (HSI HB 10-04), dated June 30, 2010, or as updated.)

7.12 Electronic Tracing System

When acting in the capacity of seizing officer during any enforcement action or investigative process resulting in firearms seizures, or when encountering firearms during the course of an enforcement action or investigation, SAs should use the Bureau of Alcohol, Tobacco, Firearms, and Explosives' (ATF's) Electronic Tracing System (eTrace).

eTrace is a firearms trace request submission system and interactive trace analysis module that facilitates firearms tracing. eTrace provides the electronic exchange of gun crime incident data in a Web-based environment with a portal to ATF's Firearms Tracing System (FTS) database. The system provides real-time capabilities that allow ICE HSI SAs to submit electronic firearms trace requests, monitor the progress of traces, retrieve completed trace results, and query firearms trace-related data in the FTS database. Firearms tracing is the systematic tracking of the movement of a firearm from its creation by the manufacturer or its introduction into the U.S. commerce by the importer, through the distribution chain, to the first retail purchase.

eTrace also provides HSI SAs with the ability to initiate a search on virtually any data field or combination of data elements such as firearms serial numbers, an individual's name, type of crime, date of recovery, or other identifiers. Additionally, HSI SAs can generate statistical reports on the number of traces submitted, the top firearms traced, the average time-to-crime rates, and other variables.

has approved the affidavit and prepared the appropriate accompanying documents, the SA will present the affidavit to a federal magistrate or judge, affirm its contents under oath, and sign the affidavit in the presence of the judge or magistrate.

8.2 Contents of a Search Warrant Affidavit

While the precise format may vary depending on the nature of the property or item to be searched and the district in which the SA is operating, an SA's search warrant affidavit should include the following:

- A. An introductory section identifying the SA and describing the SA's background, training, and experience.
- B. A section describing the purpose of the affidavit, including the specific statutory violations and legal authorities for requesting the warrant.
- C. An identification of the property or item to be searched. This should consist of as complete a description of the property or item as possible, including not only an overall description of the property or item, but also any identifying marks or numbers (e.g., addresses, license plate numbers, vehicle identification numbers, serial numbers, etc.). The description of the property or item to be searched is often incorporated into an attachment to the affidavit.
- D. A detailed description of the evidence sought and the items to be seized. This also may be included as an attachment to the affidavit. The list should be as detailed and inclusive as possible.

(Note: If SAs have probable cause to search for evidence that may be stored in electronic form, they should enlist the aid of their local computer forensics group. Likewise, if they have probable cause to search for and seize financial documents, SAs should consult their local AIRG or financial investigative group. These subject matter experts can assist in providing the appropriate language to be included in this section of the affidavit.)

- E. A section providing background information about the investigation. This may include an overview of the investigation leading up to the discovery of probable cause for the search warrant. For investigations dealing with complex violations or technical issues, this section may also provide definitions or explanations necessary for an understanding of the probable cause.
- F. A statement of probable cause. It is not necessary to relate every fact of the investigation to the judge or magistrate, but it is important to be thorough and include enough detailed information for the judge to make a finding of probable cause based solely on the affidavit. Information establishing probable cause should be timely, i.e., it should be recent enough to convince the judge that the evidence and items to be seized are still located in the place to be searched.

Probable cause may be established by means of any of the articulable facts described in Section 6.5. It may include both the SA's firsthand observations and hearsay. If the SA uses hearsay from non-law enforcement third parties, such as informants, the SA should include the reasons why he or she believes that the information is reliable. If the SA used his or her training and experience to add value to certain facts in the investigation, this should be stated and explained in the affidavit.

- G. In applicable cases, the SA will include a statement justifying nighttime execution or a "no knock" entry. Primarily, justification for a "no knock" entry or nighttime execution are based on either officer safety or preventing the destruction of evidence. The list of factors that could fall under these general categories are numerous and should be articulated to the judge or magistrate in the affidavit when a "no knock" entry or nighttime execution is sought.
- H. A search warrant may include additional attachments that provide documentary evidence for some of the assertions made in the statement of probable cause. Most search warrants will not include such attachments, but they are useful in cases where references to documentary evidence are so frequent that it is easier and clearer to attach the document itself.

8.3 Issuance of a Search Warrant

Upon a finding of probable cause, the judge or magistrate will issue a search warrant to be served within 10 calendar days from issuance. If, for some reason, SAs are unable to execute the warrant within the 10-day period, the warrant will become invalid and the SAs must apply for a new warrant based on whatever probable cause may still be timely.

Although a specific SA may be named as the affiant to a search warrant affidavit, it is recommended that the search warrant itself be directed to "any Special Agent of the U.S. Immigration and Customs Enforcement." If the affiant becomes unavailable, or if multiple warrants are to be served simultaneously at different locations, this wording will allow another SA to execute the search warrant.

8.4 Telephonic Search Warrants

In some critical circumstances, a federal judge or magistrate may issue a search warrant based on sworn testimony communicated by an SA from a remote location. In the past, these warrants were obtained by reading a warrant and probable cause statement over the telephone. Rule 41 of the FRCrP was modified to allow for the submission of search warrants by facsimile or other "reliable electronic means."

When seeking a telephonic warrant, the SAs should be prepared to show that: 1) they could not reach the magistrate in his or her office during regular business hours; 2) the SAs seeking to make the search are at a significant distance from the magistrate; 3) because of the particular factual situation, it would be unreasonable for a substitute SA who is near the magistrate to prepare a written affidavit and appear before the magistrate in person; and 4) the need for a

If SAs working in a border environment believe that an individual may be armed, they may conduct an immediate patdown of the individual. It may be conducted when there is reasonable suspicion that the person is armed. An immediate patdown is not a border search for merchandise, but rather a search conducted for the safety of the SAs and others. SAs should limit the immediate patdown to areas where they believe a weapon may be concealed.

Any border search beyond the scope of a routine personal search or an immediate patdown for weapons should be conducted by an SA of the same sex as the individual being searched. SAs should take care to conduct these more intensive personal searches in a private area away from the eyes of the public.

With some or mere suspicion, SAs may move a person to a private area and conduct a patdown search of an individual. As opposed to an immediate patdown for weapons, a patdown search is a search for merchandise and requires no suspicion. It may consist of one or more of the following actions:

- A. Patting the hands over the person's body.
- B. Removing the person's shoes.
- C. Lifting the pant leg or hem of a skirt a few inches.
- D. Removing a belt.
- E. Examining or reaching into pockets.
- F. Rolling up shirt sleeves.
- G. Removing a wig or hairpiece.

If, during the course of the patdown search, SAs develop reasonable suspicion that the person has merchandise concealed beneath the clothing, the SAs may conduct a partial body search. A partial body search is the removal of some of the clothing to recover an item hidden underneath. The removal of clothing should be limited to the area where the SAs believe the merchandise is hidden. The SAs should conduct a partial body search in a private area out of the public view. Unless the person refuses to cooperate, SAs should conduct the search by directing the person to remove his or her own clothing.

Any personal search related to the suspected concealment of merchandise within a person's body, i.e., x-ray or body cavity search, must be conducted by medical personnel and requires reasonable suspicion that the individual is concealing material evidence inside his or her body. In the absence of consent for an x-ray, monitored bowel movements may be conducted. All decisions regarding appropriate medical procedures for a patient are to be made by medical personnel only. CBP officers and HSI SAs neither suggest nor concur in any medical procedure.

Chapter 11. IMMIGRATION BORDER AUTHORITY

The INA grants SAs the statutory authority to conduct certain types of border searches and seizures. While the purpose of a customs border search is to look for merchandise, the purpose of a border search under the INA is to examine aliens regarding their admissibility, search for aliens who are being transported into the United States, and search for documentary or other evidence of the alienage and admissibility of persons seeking entry into the United States.

11.1 Questioning and Routine Searches at the Functional Equivalent of the Border

Persons seeking admission to the United States must present themselves to an immigration officer at a U.S. POE. POEs are defined as FEBs, as discussed in Section 10.5, and may be land POEs, seaport POEs, or airport POEs. While inspections at POEs to determine admissibility are generally carried out by CBP officers, the INA also grants this authority to ICE HSI SAs.

An applicant for admission who claims to be a U.S. citizen must establish that fact to the SA's satisfaction. If U.S. citizenship is established, the person is not subject to any further examination under the INA and must be allowed to proceed (although he or she may still be detained and searched for merchandise under the SAs' customs border authority). If U.S. citizenship is not established, the person may be detained and examined as an alien. For additional guidance on claims of U.S. citizenship, refer to ICE Memorandum 16001.1, "Superseding Guidance on Reporting and Investigating Claims to United States Citizenship," dated November 19, 2009, or as updated.

An alien applicant for admission must answer any questions posed by SAs regarding whether or not the applicant is admissible, his or her purpose for seeking admission, the intended length of stay, and whether or not the applicant intends to establish permanent residence or become a U.S. citizen. The applicant must also present any documentation required to establish, to the SA's satisfaction, that the individual is entitled to enter the United States and is not subject to exclusion under the provisions of the INA.

In addition to the authority to detain and question, the INA grants SAs the authority to conduct routine searches at the FEB. The purpose of these searches is to look for documents or other evidence which might substantiate grounds for denial of admission. With mere suspicion that a person is inadmissible, an SA may search the person's outer clothing, luggage, and other personal effects. At the FEB, SAs may also search, with mere suspicion, any conveyance suspected of containing aliens or of containing documents relating to a person's admissibility.

To conduct a more intensive personal search – a partial body search or a destructive search of a vehicle, for example – SAs must have reasonable suspicion that the search will reveal evidence of a person's inadmissibility.

11.2 Access to Lands Within 25 Miles of the Border

Under Section 287(a)(3) of the INA [8 U.S.C. §1357(a)(3)], SAs are authorized to enter private lands located within 25 miles of the border for the purpose of patrolling the border to prevent the

EXHIBIT 44

MEMORANDUM OF UNDERSTANDING

between

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
HOMELAND SECURITY INVESTIGATIONS**

and

U.S. POSTAL INSPECTION SERVICE

regarding

EXTENDED BORDER SEARCH AUTHORITY (EBSA)

1. PARTICIPANTS.

The Participants to this Memorandum of Understanding (MOU) are U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), an agency of the Government of the United States of America, and U.S. Postal Service (USPS), Postal Inspection Service (USPIS), an agency of the Government of the United States of America.

Nothing in this MOU alters the historic, statutory, or regulatory mission, duties, or responsibilities of ICE-HSI and is only to clarify the role of each Participant relative to the enforcement of U.S. laws that combat illicit trade. In addition, this MOU does not alter ICE-HSI's or USPIS obligations pursuant to statute or regulation. While both Participants have described in this MOU the way they intend to collaborate with each other, nothing in this MOU will be interpreted as imposing binding obligations (or liabilities) on any of the Participants in contravention of their respective obligations under the applicable laws and regulations.

2. AUTHORITY.

This MOU is authorized under HSI's general enforcement authority as customs officers under 19 U.S.C. § 1589a and entered into pursuant to the provisions of DHS Management Directive 0450.1, which allows for DHS organizational elements to enter into MOUs for describing concepts of mutual understanding, goals and plans shared by the parties to the agreement.

This MOU shall supersede and replace the prior MOU entered into by the U.S. Postal Service and U.S. Customs Service on March 22, 1978.

3. PURPOSE.

The Participants enter into this MOU in order to clarify the roles, responsibilities, and authorities of the Participants as they relate to the customs inspection of mail matter originating outside of

For Official Use Only / Law Enforcement Sensitive

the customs territory of the United States or destined for delivery outside of the Customs Territory of the United States (CTUS).

4. RESPONSIBILITIES.

ICE-HSI intends to:

- A. Inbound Mail - Without a search warrant, Customs officers, authorized by law or designated by the Secretary of Homeland Security to enforce the customs laws of the United States (hereinafter "customs officers"), may open or inspect the contents of mail (including APO and FPO mail) that originated outside the CTUS and is addressed for delivery either inside the CTUS or inside the customs district of the Virgin Islands, under the following conditions:
1. Inspection of Unsealed Mail - Customs officers may search inbound international mail that is not sealed against inspection under the postal laws and regulations of the United States, inbound international mail which bears a customs declaration, and inbound international mail with respect to which the sender or addressee has consented in writing to search.
 2. Inspection of Sealed Mail - Customs officers may, without a search warrant, search inbound international mail that is sealed against inspection if a customs officer has a reasonable suspicion that the mail contains merchandise or contraband. No one acting under the authority of this section shall read or authorize any other person to read any correspondence contained in mail sealed against inspection without a search warrant, issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure or the written consent of the sender or addressee.
 3. Inbound international mail that is sealed against inspection and appears to only contain correspondence may not be searched by customs officers without a search warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure or the written consent of the sender or addressee.
 4. Search Warrant Required for Domestic and Certain International Mail - No customs officers may, without a search warrant, issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure or the written consent of the sender or addressee, open, inspect, read, or seize any mail in postal custody (including APO and FPO mail) that has diplomatic or consular immunity from Customs inspection or has not originated outside the CTUS.
- B. Outbound Mail - Without a search warrant, customs officers may open or inspect the contents of mail (including APO and FPO mail) that originated inside the CTUS and is addressed for delivery either outside the CTUS or outside the customs district of the Virgin Islands, under the following conditions:

For Official Use Only / Law Enforcement Sensitive

1. Inspection of Unsealed Mail - Customs officers may search outbound international mail that is not sealed against inspection under the postal laws and regulations of the United States, outbound international mail which bears a customs declaration, and outbound international mail with respect to which the sender or addressee has consented in writing to search.
2. Inspection of Sealed Mail - Customs officers may, without a search warrant, search outbound international mail that weighs more than 16 ounces and is sealed against inspection if there is reasonable cause to suspect that the mail contains one or more of the items listed in 19 U.S.C. § 1583(c)(1). No one acting under the authority of this section shall read or authorize any other person to read any correspondence contained in mail sealed against inspection without a search warrant, issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, or the written consent of the sender or addressee.
3. Outbound international mail that weighs less than 16 ounces and is sealed against inspection may not be searched by customs officers without a search warrant, issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, or the written consent of the sender or addressee.
4. Search Warrant Required for Domestic and Certain International Mail - No customs officers may, without a search warrant, issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure or the written consent of the sender or addressee, open, inspect, read, or seize any mail in postal custody (including APO and FPO mail) that is not destined for delivery outside the CTUS, or that has diplomatic or consular immunity from Customs inspection.
5. International Transit Mail - Customs officers may, without a search warrant, screen international transit mail to detect materials that pose a physical threat to persons or property, such as explosives, flammables, and other dangerous materials. Such screening must be done by non-intrusive means such as canines trained to detect explosives, radiation detection equipment, x-rays, explosive swabs, or other characteristics of the mail that can be sensed from the examination of the mail, including seeing or feeling exposed wires or leaking fluids, hearing ticking sounds, or smelling black powder. Such screening shall be subject to the conditions enumerated below.

USPIS intends to:

- A. Screening of international transit mail may not disrupt the processing of that mail. ICE personnel will be provided a reasonable opportunity to perform screening of specifically identified mail, but may not prevent the Postal Service from forwarding the mail without delay by the quickest means it uses for United States mail unless the mail has been screened and the screening has detected, or appears to have detected, materials that pose a physical threat to persons or property including explosives, flammables, or other dangerous materials. International transit mail that has been screened and found to be free

For Official Use Only / Law Enforcement Sensitive

EXHIBIT 45

1300 Pennsylvania Avenue NW
Washington, DC 20229

APR 28 2015



**U.S. Customs and
Border Protection**

MEMORANDUM FOR: DIRECTORS, FIELD OPERATIONS
DIRECTOR, PRECLEARANCE OPERATIONS

FROM: Todd C. Owen
Assistant Commissioner
Office of Field Operations

SUBJECT: [REDACTED]

The Office of Field Operations (OFO) conducts border searches of electronic devices containing information in furtherance of border security. Going forward, and for uniformity and consistency with the vocabulary used by our law enforcement partners at other government agencies, OFO will replace the [REDACTED]

In addition, to address evolving threats, the use of [REDACTED] equipment is [REDACTED]

The use [REDACTED] equipment will now be authorized on all inbound and outbound passengers [REDACTED]

[REDACTED]

Please be reminded that all border searches of electronic devices must be performed in accordance with CBP Directive 3340-049, "Border Search of Electronic Devices Containing Information" dated August 20, 2009.

THE INFORMATION BELOW ONLY APPLIES TO THE NINTH (9th) CIRCUIT

In the jurisdiction of the Ninth Circuit – California, Arizona, Nevada, Montana, Idaho, Oregon, Washington, Alaska, Hawaii, Guam, and the Northern Mariana Islands – the 2013 [REDACTED]

Operational Guidance Update applies. Under that guidance, in the Ninth Circuit, CBP, by policy, limits [REDACTED] to perform a border search of a [REDACTED] or a [REDACTED]. Such searches require – prior to the search – establishing that reasonable suspicion of activity in violation of the laws enforced and administered by CBP exists.

[REDACTED]

[REDACTED]

[REDACTED] However, for comprehensive forensic border searches within the Ninth Circuit, reasonable suspicion should be established using factor(s) independent of [REDACTED]

These enhancements reflect the necessary evolution of [REDACTED] to meet the emerging transnational threat posed by terrorists, drug traffickers and other organized crime.

If we can be of further assistance, please contact me at (202) 344-[REDACTED] or have a member of your staff contact the Director of the Tactical Operations Division, at (202) 344-[REDACTED]

Attachment

EXHIBIT 46

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS**

GHASSAN ALASAAD, NADIA
ALASAAD, SUHAIB ALLABABIDI, SIDD
BIKKANNAVAR, JÉRÉMIE DUPIN,
AARON GACH, ISMAIL ABDEL-RASOUL
AKA ISMA'IL KUSHKUSH, DIANE
MAYE, ZAINAB MERCHANT,
MOHAMMED AKRAM SHIBLY, AND
MATTHEW WRIGHT,

Plaintiffs,

v.

KIRSTJEN NIELSEN, SECRETARY OF
THE U.S. DEPARTMENT OF HOMELAND
SECURITY, IN HER OFFICIAL
CAPACITY; KEVIN MCALEENAN,
COMMISSIONER OF U.S. CUSTOMS
AND BORDER PROTECTION, IN HIS
OFFICIAL CAPACITY; AND RONALD
VITIELLO, ACTING DIRECTOR OF U.S.
IMMIGRATION AND CUSTOMS
ENFORCEMENT, IN HIS OFFICIAL
CAPACITY,

Defendants.

Civil Action No. 17-cv-11730-DJC

Hon. Denise J. Casper

JOINT STATEMENT OF STIPULATED FACTS

Counsel for the parties have conferred and submit the following stipulated facts:

1. U.S. Customs and Border Protection (“CBP”) Directive No. 3340-049A (issued January 4, 2018) defines an ‘advanced’ search as any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to a device, but to review, copy and/or analyze its contents. The same directive defines a ‘basic’ search as a search of an electronic device that does not qualify as an advanced search. U.S. Immigration and Customs Enforcement (“ICE”) uses the same definitions of a basic and an advanced search as CBP.
2. When conducting a basic search, as defined in CBP’s policy, officials conducting border searches are able to search content from allocated space physically resident on an

electronic device that is accessible using the native operating system of the device, including but not limited to its native graphical user interface and/or touchscreen.

3. When conducting a basic search, as defined in CBP's policy, officials are able to use the native search functions in the native operating system of the device, such as a keyword search tool, if there is one.
4. Basic searches of electronic devices, as defined in CBP's policy, can extend to any allocated file or information that is resident on the device and accessible using the device's native operating system.
5. Separate from the primary content stored on them, some electronic devices may also store data related to that content—such as the date and time associated with the content, usage history, sender and receiver information, or location data. That content may be revealed during a basic search, as defined in CBP's policy, depending on the type of device, the operating system, the relevant settings, and the applications used to create and/or maintain the data being searched.
6. Depending on the equipment, procedures, and techniques used, advanced searches of electronic devices, as defined in CBP's policy, are generally capable of revealing everything a basic search may reveal.
7. Depending on the type of device, the operating system, the relevant settings, and the applications used to create and/or maintain the data being searched, advanced searches, as defined in CBP's policy, may reveal data related to content stored on an electronic device, such as the date and time associated with the content, usage history, sender and receiver information, or location data.
8. An advanced search of an electronic device, as defined in CBP's policy, depending on the equipment, procedures, and techniques used, may be capable of revealing deleted or other data in unallocated storage space and password-protected or encrypted data.
9. Digital data can be posted, shared, or transmitted via the Internet, and stored on electronic devices.
10. To the extent consistent with the applicable system of records notice, ICE and CBP can retain information from a device in any of their record keeping systems when an electronic device search reveals information relevant to immigration, customs, or other laws enforced by the Department of Homeland Security.
11. To the extent consistent with the applicable system of records notice, CBP and ICE officials can maintain written notes or reports or document impressions relating to a border encounter. CBP documents relevant information regarding border inspections, including both basic and advanced searches of electronic devices, in its primary law enforcement system, TECS. CBP officers document border searches of electronic devices in the 'Electronic Media Report' module of TECS. These TECS records may

include notes on information collected from electronic devices pursuant to a border search, consistent with CBP Directive No. 3340-049A.

12. Officials conducting an advanced search, as defined in CBP policy, may be able to copy all information physically resident on the device or may be limited to only certain files, depending on the search equipment, procedures, and techniques used.
13. CBP conducted the following number of border searches of electronic devices in each of the identified fiscal years:
 - FY 2018 – 33,295
 - FY 2017 – 30,524
 - FY 2016 – 19,051
 - FY 2015 – 8,503
 - FY 2014 – 6,029
 - FY 2013 – 5,709
 - FY 2012 – 5,085

In FY 2017, approximately 0.007% of arriving international travelers processed by CBP officers had their electronic devices searched. In FY 2017, CBP processed more than 397 million arriving international travelers and searched the devices of more than 29,200 of them.

14. ICE conducts both basic and advanced searches of electronic devices, as defined in CBP's policy. ICE does not maintain records of the number of basic searches it conducts.
15. ICE records all instances in which its Computer Forensics Agents or Analysts (CFA) conduct advanced searches, as defined in CBP policy. ICE conducted the following number of advanced searches of electronic devices in each of the identified fiscal years:
 - FY 2018 – 483
 - FY 2017 – 681
 - FY 2016 – 726
 - FY 2015 – 888
 - FY 2014 – 850
 - FY 2013 – 789
 - FY 2012 – 825

For plaintiffs:

Sophia Cope

Dated: March 1, 2019

ADAM SCHWARTZ
SOPHIA COPE
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333 (phone)
(415) 436-9993 (fax)
adam@eff.org
sophia@eff.org

ESHA BHANDARI
HUGH HANDEYSIDE
NATHAN FREED WESSLER
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

MATTHEW R. SEGAL
JESSIE J. ROSSMAN
American Civil Liberties Union Foundation
of Massachusetts
211 Congress Street
Boston, MA 02110
(617) 482-3170 (phone)
(617) 451-0009 (fax)
jrossman@aclum.org

Attorneys for Plaintiffs

For defendants:

Marsha Edney

Dated: March 4, 2019

U.S. DEPARTMENT OF JUSTICE

JOSEPH H. HUNT
Assistant Attorney General

JOHN R. GRIFFITHS
Director, Federal Programs Branch

DIANE KELLEHER
Assistant Director, Federal Programs Branch

Marsha Stelson Edney
Senior Trial Counsel
Michael Drezner
Trial Attorney
U.S. DEPARTMENT OF JUSTICE
Civil Division/Federal Programs
Mail: P.O. Box 883
Washington, DC 20530
Street: 20 Massachusetts Avenue, N.W.,
Rm. 7146
Washington, DC 20001
T: (202) 514-4505
Email: Michael.Drezner@usdoj.gov

Attorneys for Defendants