EXHIBIT 15

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.	)	Civil Action No. 17-cv-11730-DJC
KIRSTJEN NIELSEN,[1] 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 THOMAS HOMAN, ACTING DIRECTOR OF U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, IN HIS OFFICIAL CAPACITY,	)	
Defendants.	)	

ANSWER

Defendants Kirstjen Nielsen, Secretary of the U.S. Department of Homeland Security ("DHS"); Kevin McAleenan, Commissioner, U.S. Customs and Border Protection ("CBP"); and Thomas Homan, Deputy Director and Senior Official Performing the Duties of the Director, U.S. Immigration and Customs Enforcement ("ICE") (collectively "Defendants"), hereby respond to each numbered paragraph of the Amended Complaint (ECF No. 7) as follows:

[1] Pursuant to Federal Rule of Civil Procedure 25(d), Secretary Kirstjen Nielsen is automatically substituted as a Defendant.

41. The first two sentences of this paragraph consist of argument, statements of law, or legal conclusions to which no response is required. To the extent a response is deemed required, denied. The third sentence consists of Plaintiffs' characterization of *Riley v. California*, 134 S. Ct. 2473 (2014). Defendants respectfully refer the Court to that decision for a full and accurate statement of its contents.

42. Defendants deny the allegations contained in this paragraph; Defendants further state that CBP and ICE border searches include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Defendants further state that CBP and ICE officials do not intentionally use the device to access information that is solely stored remotely and not otherwise present on the device.

43. With respect to the allegations contained in this paragraph, Defendants state that the use of the word "forensic" is ambiguous in this context, but admits that CBP and ICE officials can conduct basic, advanced, or both basic and advanced searches on an electronic device at the border consistent with their Directives. Defendants admit that in an advanced search, a CBP or ICE officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents. Defendants further admit that CBP and ICE officials can use particularized software tools to conduct advanced searches of electronic devices at the border, and that there are different types of searches that may constitute an advanced search.

44. With respect to the first sentence contained in this paragraph, Defendants admit that CBP and ICE officials use particularized software tools to conduct advanced searches of electronic devices at the border. With respect to the second sentence, Defendants deny that the

use of "algorithms" to search the contents of an electronic devices indicates the use of any "forensic tools," and further state that the terms "algorithms" and "forensic tools" are ambiguous in this context; Defendants deny the remaining allegations in the second sentence. With respect to the third sentence, admitted.

45. This paragraph contains argument, statements of law, or conclusions of law, to which no response is required. To the extent a response is deemed required, denied.

46. The first and fourth sentences of this paragraph contain conclusions of law, to which no response is required. To the extent a response is deemed required, denied. Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations in the second and third sentences, except that Defendants admit that officials searched Mr. Dupin's phone on two occasions in the context of a border search, and officials searched Mr. Kushkush's phones on at least one occasion in the context of a border search.

47. This paragraph consists of Plaintiffs' arguments, statements of law, or legal conclusions, to which no response is required. To the extent a response is deemed required, denied, except Defendants admit that CBP law enforcement officials wear uniforms and are armed. Defendants further admit that all individuals who cross the border are obligated to present themselves and their effects to CBP. Defendants further admit that while in many instances inspection at the port of entry is brief, given the high volume of travelers and CBP's efforts to facilitate travel efficiently, any traveler whose inspection is expected to last more than a couple of minutes will be generally be referred for additional scrutiny, sometimes referred to as "secondary inspection," which is merely a continuation of a border inspection initiated during primary processing.

61. This paragraph, and sub-paragraphs, consist of Plaintiffs' characterization of the different types of electronic device searches that may be performed pursuant to Defendants' policies. The Court is respectfully referred to those policies for a full and accurate statement of their contents. Defendants admit that CBP and ICE policies authorize border searches of electronic devices for a reasonable time without a warrant. Defendants further admit that CBP and ICE policies authorize searches of electronic devices without individualized suspicion in certain circumstances. Defendants further admit that the travelers' consent is not required to conduct a border search. The allegations in this paragraph that Defendants engage in "confiscations" of electronic devices consist of argument, statements of law, or legal conclusions, to which no response is required. To the extent a response is required, denied.

62. Defendants admit that on July 12, 2017, Plaintiffs Ghassan and Nadia Alasaad entered the United States through the Highgate Springs Port of Entry. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

63. Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations in this paragraph.

64. Defendants admit that that the Alasaads stated that their daughter was ill and had a fever. Defendants admit that the Alasaads were referred for a continuation of their border inspection, commonly known as "secondary inspection". Defendants admit that the secondary inspection of Mr. Alasaad was conducted in a private interview room at the Port of Entry.

65. With respect to the first sentence of this paragraph, Defendants lack knowledge or information sufficient to form a belief as to the allegation about what the Alasaads observed. Defendants admit the remaining allegations contained in this paragraph.

Plaintiffs' arguments, statements of law, or legal conclusions, to which no response is required. To the extent a response is deemed required, denied.

71. Denied.

72. With respect to the first sentence in this paragraph, denied; Defendants state that the two phones referenced in this paragraph were returned to the Alasaads via UPS delivery 12 days from the date of the border inspection. With respect to the second sentence in this paragraph, Defendants deny that CBP's search of the phones damaged the content of the phones. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph. The allegation that Defendants engage in "seizures" of electronic devices consists of argument, statements of law, or legal conclusions, to which no response is required. To the extent a response is required, denied.

73. With respect to the first sentence in this paragraph, Defendants admit that on August 28, 2017, Plaintiff Alasaad arrived at JFK International Airport, Terminal 4 aboard flight AT 202 from Morocco, with her two children and sister. Defendants lack knowledge and information sufficient to form a belief as to the truth of the remaining allegations in the first sentence. With respect to the second sentence in this paragraph, Defendants lack knowledge and information sufficient to form a belief as to the truth of this allegation. With respect to the third sentence in this paragraph, Defendants admit that the smartphone found in Nadia Alasaad's handbag was locked. Defendants lack knowledge and information sufficient to form a belief as to the truth of the remaining allegations in the third sentence.

74. Defendants admit the allegations in the first and third sentences contained in this paragraph. With respect to the second sentence, Defendants admit that a CBP officer asked if Ms. Alasaad had a phone in her possession, but deny the remaining allegations in the sentence to

the extent inconsistent with the foregoing. With respect to the third sentence in this paragraph, Defendants admit that a CBP Officer found a phone in Plaintiff's handbag. Defendants deny knowledge and information sufficient to form a belief as to the truth of the remaining allegations in the third sentence. Defendants admit the allegations contained in the fourth sentence in this paragraph.

75. Defendants deny the allegation in the first sentence of this paragraph. With respect to the second sentence in this paragraph, Defendants admit this allegation. With respect to the third sentence in this paragraph, Defendants admit that a CBP officer obtained the password on a piece of paper, but lack knowledge and information sufficient to form a belief as to the truth of the remaining allegations in this sentence. With respect to the fourth sentence in this paragraph, Defendants lack knowledge and information sufficient to form a belief as to the truth of this allegation, though the statement that the environment was "coercive" consists of argument, statements of law, or legal conclusions, to which no response is required. To the extent a response is necessary, denied. In regards to the fifth sentence, Defendants deny this allegation.

76. Defendants admit that CBP officials searched the phone during this inspection.

77. Defendants admit that Plaintiff Allababidi was inspected by CBP at Dallas/Fort Worth International Airport on January 24, 2017, and that he had two phones in his possession when he presented himself for inspection and that at least one of the phones was locked. Defendants otherwise lack knowledge or sufficient information to form a belief as to the truth of the allegations in this paragraph.

78. With respect to the first sentence of this paragraph, Defendants admit this allegation. Defendants further admit CBP conducted a baggage exam of Plaintiff Allababidi's

luggage. With respect to the allegations contained in the third and fourth sentences in this paragraph, Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations. The allegation that Defendants "seize" electronic devices consists of argument, statements of law, or legal conclusions, to which no response is required. To the extent a response is required, denied.

79. With respect to the first sentence in this paragraph, Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations. With respect to the second sentence, Defendants admit that Plaintiff Allababidi failed to unlock one of his phones for purposes of conducting an inspection, but lack knowledge or sufficient information as to the truth of the remaining allegations in this sentence. With respect to the third sentence, Defendants admit that Plaintiff Allababidi's two phones were detained for further examination; the statement that CBP responded by "confiscating" the phones consists of argument, statements of law, or legal conclusions to which no response is required. To the extent a response is required, denied.

80. With respect to the first sentence in this paragraph, Defendants admit that officials detained Plaintiff Allababidi's two phones in the context of a border inspection, and returned his iPhone on April 5, 2017 and another on December 13, 2017. Otherwise, denied.

81. Defendants admit that on January 31, 2017, Plaintiff Bikkannavar arrived at the Houston International Airport from Santiago, Chile and that he had a phone in his possession when he presented himself for inspection. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations contained in this paragraph.

82. With regard to the first sentence, Defendants admit that Plaintiff Bikkannavar was referred for a continuation of his border inspection, commonly known as secondary inspection. The second sentence in this paragraph consists of argument, statements of law, or legal

extent a response is deemed required, denied. With respect to sub-paragraph (b), Defendants admit that Plaintiff Dupin was referred for a continuation of his border inspection, commonly known as secondary inspection, with CBP officials; Defendants lack knowledge or information sufficient to form a belief as to the remaining allegations of sub-paragraph (b). Defendants deny the remaining allegations contained in paragraph.

90. Defendants admit that a CBP Officer conducted a basic search of Plaintiff Dupin's phone, that the search occurred in a different room, and that the search lasted approximately fifteen minutes. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

91. Defendants admit that the CBP officials returned Plaintiff Dupin's phone to him and that he departed following the inspection. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

92. Defendants admit that Plaintiff Dupin arrived at the Champlain, New York Port of Entry via bus with his daughter, on December 23, 2016. Defendants admit Plaintiff had a smartphone in his possession. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

93. Defendants admit that Plaintiff Dupin was referred for a continuation of his border inspection, commonly known as secondary inspection, with CBP officials at approximately 11:00 p.m. and was questioned by CBP officials. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

94. With respect to the first sentence of this paragraph, the allegation that Defendants "seized" an electronic devices consists of argument, statements of law, or legal conclusions, to

which no response is required. To the extent a response is required, denied. Defendants admit that CBP conducted a border search of Plaintiff Dupin's phone for purposes of a border search inspection, and admit that Mr. Dupin provided the password to his phone. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in the first sentence of this paragraph. The remainder of this paragraph consists of Plaintiffs' arguments, statements of law, or legal conclusions, to which no response is required. To the extent a response is deemed required, denied.

95. The first sentence and sub-paragraph (a) of this paragraph consists of Plaintiffs' arguments, statements of law, or legal conclusions, to which no response is required. To the extent a response is required, denied. With respect to sub-paragraph (b), Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations. With respect to sub-paragraphs (c) and (d), Defendants admit that Plaintiff Dupin was referred for secondary inspection at approximately 11:00 p.m., that he was traveling with his daughter, that he and his daughter arrived at the port of entry by bus, and that they departed the port of entry following his inspection on the next available bus. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

96. Defendants admit that Plaintiff Dupin's phone was searched and that Plaintiff Dupin provided information to the CBP Officers about some of the photos that were identified on his device while it was being inspected. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

97. Defendants admit that CBP records indicate that the border inspection of Plaintiff Dupin began at approximately 11:00 p.m. on December 23, 2016, and was completed at approximately 3:55 a.m. on December 24, 2016, that CBP officials returned Plaintiff Dupin's

Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations contained in these sub-paragraphs.

102. Defendants admit CBP inspected Plaintiff Gach's phone for a brief period. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

103. Defendants admit CBP inspected Plaintiff Gach's phone during this time for a brief period.

104. Admit.

105. Defendants admit that on January 9, 2016, Plaintiff Kushkush arrived at JFK International Airport, Terminal 1 from Arlanda Airport in Stockholm, Sweden via London, England. Defendants lack knowledge and information sufficient to form a belief as to the truth of the remaining allegations in this paragraph.

106. Defendants admit that Plaintiff Kushkush was referred for a continuation of his border inspection, commonly known as secondary inspection; Plaintiff Kushkush was brought into the secondary inspection area, and a search was conducted of one checked bag and one messenger bag, including one or more notebooks contained therein. Defendants lack knowledge and information sufficient to form a belief as to the truth of the remaining allegations contained in this paragraph.

107. Defendants deny the allegations contained in the first two sentences in this paragraph. With respect to the third sentence, Defendants admit that Plaintiff Kushkush was permitted to leave the secondary inspection area approximately three hours after he arrived at the secondary inspection area. Defendants deny the remaining allegations in this sentence.

Defendants admit that Plaintiff Kushkush stated that he did not consent to the search of his phone and that he was advised that the phone could be seized. Defendants deny the remaining allegations contained in the first, second sentences and third of this paragraph. The fourth sentence in this paragraph consists of argument, statements of law, and legal conclusions, to which no response is required; to the extent a response is required, denied.

116. The first sentence and sub-paragraph (a) in this paragraph consist of argument, statements of law, and legal conclusions, to which no response is required; to the extent a response is required, denied. With respect to sub-paragraph (b), Defendants deny the allegations in this sub-paragraph.

117. Denied, except that Defendants admit that a CBP officer noted the password to Plaintiff's Kushkush's phone when Plaintiff Kushkush provided it to the officer. Defendants further admit that a manual search of Plaintiff Kushkush's phone was conducted, and that the manual search of the phone lasted at least one hour.

118. Denied.

119. Admitted.

120. Defendants admit that Plaintiff Maye arrived at Miami International Airport on June 25, 2017 from Oslo, Norway, and that she had a phone in her possession when she presented herself for inspection. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

121. With respect to the first sentence, the allegation that Defendants had "seized" an electronic device consists of argument, statements of law, or legal conclusions, to which no response is required. To the extent a response is required, denied. Defendants admit that CBP conducted a manual search of Plaintiff Maye's cellphone and that Ms. Maye provided the

password to the cellphone. Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations concerning any other devices. The second sentence consists of Plaintiffs' arguments, statements of law, or legal conclusions, to which no response is required. To the extent a response is deemed required, denied.

122. The first sentence and sub-paragraph (a) in this paragraph consist of argument, statements of law, and legal conclusions, to which no response is required; to the extent a response is required, denied. Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations in this paragraph and sub-paragraph (a)-(d), but admit that Plaintiff Maye was referred to a continuation of her border inspection, commonly referred to as "secondary inspection," that CBP officials were present there, and that Plaintiff Maye provided the password to her phone for purposes of conducting an inspection.

123. Defendants lack knowledge or sufficient information to form a belief as to what Plaintiff Maye observed.

124. With respect to the first sentence, the allegation that Defendants "seized" an electronic device consists of argument, statements of law, or legal conclusions, to which no response is required. To the extent a response is required, denied. Defendants admit that CBP detained Ms. Maye's phone and conducted a border inspection of the device and that CBP records indicate that the inspection of her phone lasted approximately 45 minutes. Defendants deny the remaining allegations in this paragraph to the extent inconsistent with the foregoing.

125. Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations in this paragraph.

126. Defendants admit that on March 5, 2017, Plaintiff Merchant arrived at the Toronto, Canada airport for a flight to the United States, and that she had a phone in her

134. Defendants admit that Plaintiff Merchant's electronic device was returned to her on March 5, 2017, and that she was permitted to leave the CBP preclearance area. Defendants deny that Plaintiff Merchant's inspection lasted approximately two hours. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

135. Defendants admit that Plaintiff Merchant's phone was inspected during the March 5, 2017 search, but deny the allegations that her electronic device was out of her sight for approximately one and a half hours. The allegation that Defendants engage in "seizures" of electronic devices consists of argument, statements of law, or legal conclusions, to which no response is required. To the extent a response is required, denied. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

136. Defendants admit that on January 1, 2017, Plaintiff Shibly presented himself for inspection at the Lewiston Bridge Port of Entry in New York and that he was travelling with a cellular phone. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

137. Defendants admit that Plaintiff Shibly was referred for a continuation of his border inspection, commonly referred to as secondary inspection. Defendants admit that, during the course of the border inspection, Plaintiff Shibly declined to write down the password to his cellular phone, but he later unlocked the phone for purposes of an inspection. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

138. Defendants admit that, during the course of the border inspection, Plaintiff Shibly declined to write down the password to his cellular phone, but he later unlocked the phone for purposes of an inspection. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph. In addition, the remaining allegations contained in paragraph consist of arguments, statements of law, or legal conclusions, to which no response is required; to the extent a response is required, denied.

139. The first sentence and sub-paragraph (a) in this paragraph consist of argument, statements of law, and legal conclusions, to which no response is required; to the extent a response is required, denied. With respect to sub-paragraphs (b) and (c), Defendants lack knowledge or sufficient information to form a belief as to the truth of the allegations.

140. Defendants admit that CBP conducted a border search of Plaintiff Shibly's cellular phone, and that he unlocked it for purposes of inspection. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

141. The first sentence in this paragraph consists of argument, statements of law, and legal conclusions, to which no response is required; to the extent a response is required, denied. Defendants deny the allegations contained in the second sentence of this paragraph.

142. Admit.

143. Defendants admit that on January 4, 2017, Plaintiff Shibly presented himself for inspection at the Lewiston Bridge port of entry in New York and that he was travelling with a cellular phone. Defendants lack knowledge or sufficient information to form a belief as to the truth of the remaining allegations in this paragraph.

153. This paragraph characterizes certain records disclosed pursuant to a FOIA request, and the Court is respectfully referred to those records for a full and accurate statement of their contents.

154. Admit that the detained items were returned to Plaintiff Wright on June 14, 2016. The allegation in this paragraph that Defendants "confiscated" electronic devices consists of argument, statements of law, or legal conclusions, to which no response is required. To the extent a response is required, denied.

155. With respect to this paragraph, Defendants state that "retained" as used in this context, is vague and ambiguous. Defendants admit that CBP extracted and obtained information from Plaintiff Wright's devices. Sub-paragraphs (a) and (c) characterize certain records disclosed pursuant to a FOIA request, and the Court is respectfully referred to those records for a full and accurate statement of their contents. Sub-paragraph (b) characterizes a CBP policy related to border searches of electronic devices. Defendants respectfully refer the Court to that policy for a full and accurate statement of its contents.

156. The first sentence of this paragraph constitutes argument, statements of law, or legal conclusions, for which no response is necessary. To the extent a response is deemed required, denied. With respect to sub-paragraph (a), Defendants admit that they adopted the following policies: CBP Directive 3340-049A, Border Search of Electronic Devices (January 4, 2018), and ICE Directive 7-6.1, Border Searches of Electronic Devices (August 18, 2009), which govern the search of electronic devices in the context of border inspections. The remaining allegations of sub-paragraph (a) contains Plaintiffs' characterization of public reports reflecting the number and type of searches of electronic devices conducted by CBP and ICE at the border, to which no response is required. To the extent a response is deemed required, the Court is

EXHIBIT 16

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. Elaine Duke, Acting 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.	COMPLAINT FOR INJUNCTIVE AND DECLARATORY RELIEF (Violation of First and Fourth Amendment rights) No. 1:17-cv-11730-DJC

AMENDED COMPLAINT

PRELIMINARY STATEMENT

1. This lawsuit challenges searches and seizures of smartphones, laptops, and other electronic devices at the U.S. border in violation of the First and Fourth Amendments to the U.S. Constitution. U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE") search travelers' mobile electronic devices pursuant to policies that do not require a warrant, probable cause, or even reasonable suspicion that the device contains contraband or evidence of a violation of immigration or customs laws. Today's electronic devices contain troves of data and personal information that can be used to assemble detailed, comprehensive pictures of

extraordinarily invasive of travelers' privacy. With little effort, an officer without specialized training or equipment can conduct thorough manual searches, including by opening and perusing various stored files, programs, and apps, or by using a device's built-in keyword-search function. The device searches at issue in *Riley*, which the Supreme Court held were unlawful without a search warrant based on probable cause, were manual searches.

42. The accessibility of cloud-based content on smartphones and other electronic devices—including email, social media, financial records, or health services—further expands the amount of private information officers could view during a manual search.

43. In a forensic search, border officials use sophisticated tools, such as software programs or specialized equipment, to evaluate information contained on a device. Although there are different types of forensic searches, many of them begin with agents making a copy of some or all data contained on a device. Forensic tools can capture all active files, deleted files, files in allocated and unallocated storage space, metadata related to activities or transactions, password-protected or encrypted data, and log-in credentials and keys for cloud accounts. They also are able to capture the same kinds of information that can be viewed in a manual search. Officials then can analyze the data they have copied using powerful programs that read and sort the device's data even more efficiently than through manual searches.

44. CBP and ICE use various sophisticated tools to conduct forensic searches. For example, a CBP officer told Mr. Bikkannavar that "algorithms" were used to search the contents of his phone, indicating the use of one or more forensic tools. Likewise, an

ICE agent attempted to image Mr. Wright's laptop with MacQuisition software, and a CBP forensic scientist extracted data from the SIM card in Mr. Wright's phone and from his camera.

45. Searches of electronic devices by CBP and ICE, regardless of the method used, are extraordinarily invasive of travelers' privacy, given the volume and detail of highly sensitive information that the devices contain.

46. Searches of electronic devices also impinge on constitutionally protected speech and associational rights, including the right to speak anonymously, the right to private association, the right to gather and receive information, and the right to engage in newsgathering. For example, CBP officers twice searched the contents of Mr. Dupin's phone, which contained his confidential journalistic work product, including reporting notes and images, source contact and identifying information, and communications with editors. Similarly, on three separate occasions, officers searched the contents of Mr. Kushkush's phones, which he used for his work as a journalist, and which contained his work product, work-related photos, and lists of contacts. Such warrantless searches of travelers' electronic devices unconstitutionally chill the exercise of speech and associational rights protected by the First Amendment.

47. Border searches of electronic devices typically occur in the "secondary inspection" or "secondary screening" area of a port of entry. The secondary inspection environment is inherently coercive. Officers wear government uniforms and carry weapons, and they command travelers to enter and remain in the secondary inspection areas. Travelers are not free to exit those areas until officers permit them to leave. The areas are unfamiliar to travelers and closed off from the public areas of the airports or

period of ICE confiscation is 30 days, ICE supervisors may extend this period under undefined "circumstances . . . that warrant more time." ¶ 8.3.1.

BORDER SEARCHES AND CONFISCATIONS OF PLAINTIFFS' ELECTRONIC DEVICES

Ghassan Alasaad and Nadia Alasaad

Search 1

62. On July 7, 2017, Plaintiffs Ghassan and Nadia Alasaad drove with their daughters and other family members from Revere, Massachusetts, to Quebec for a family vacation. During their return trip on July 12, 2017, they entered the United States at the border crossing near Highgate Springs, Vermont. Ghassan Alasaad had an unlocked smartphone, and Nadia Alasaad had a locked smartphone.

63. The Alasaads' 11-year-old daughter was ill and had a high fever.

64. CBP officers directed them to secondary inspection. Mr. Alasaad explained that his daughter was ill and needed care. Nevertheless, a CBP officer took Mr. Alasaad into a small room for questioning.

65. The Alasaads observed a CBP officer in the waiting room manually searching Mr. Alasaad's unlocked phone, which CBP officers had retrieved from the Alasaads' car.

66. The Alasaads told a CBP supervisor that their daughter's fever had worsened. The supervisor responded that they would have to continue waiting. Mr. Alasaad asked why the family was being detained and searched. The supervisor responded that he had simply felt like ordering a secondary inspection.

were told, the Alasaads understood that they would need to wait several hours for their phones to be searched. Exhausted and desperate to attend to their daughter's health, the Alasaads departed without their phones. CBP officers coerced them into leaving their phones at the border, with the threat of several more hours of detention.

71. The family departed after approximately six hours of detention.

72. Approximately fifteen days later, CBP returned the two phones to the Alasaads. On information and belief, CBP's search and seizure of Mr. Alasaad's phone damaged its functionality. Soon after CBP returned the phone to him, he attempted to access certain media files in his WhatsApp application, including videos of his daughter's graduation. The phone displayed the message, "Sorry, this media file doesn't exist on your internal storage." This problem did not occur prior to CBP's search and seizure of the phone.

Search 2

73. On August 28, 2017, Ms. Alasaad and her 11-year-old daughter arrived from Morocco, where they had been visiting family, in New York's John F. Kennedy International Airport. Ms. Alasaad was not carrying her smartphone with her because she had lost it while traveling. Her daughter was traveling with a locked smartphone.

74. CBP officers directed Ms. Alasaad and her daughter to a secondary inspection area. While questioning Ms. Alasaad, officers asked her to produce her phone. Ms. Alasaad informed the officers that she had lost it. Officers then searched Ms. Alasaad's handbag and found the smartphone her daughter was using. The phone was locked.

75. CBP officers directed Ms. Alasaad to unlock the phone. Ms. Alasaad informed the officers that she did not know the password. The officers then directed Ms. Alasaad's daughter to write down the password on a piece of paper. She did so, because the environment was coercive, and because she was an 11-year old obeying an instruction from an adult. A CBP officer took the phone to another room for approximately 15 minutes.

76. On information and belief, one or more CBP officers searched this phone during this time. They had the means to do so (Ms. Alasaad's daughter had provided the password to unlock it), and they had no reason to order her to unlock it other than to search it.

Suhaib Allababidi

77. On January 21, 2017, Mr. Allababidi returned from a business trip on a flight from Dubai, United Arab Emirates, to Dallas, Texas. He carried with him a locked smartphone that he used regularly for both personal and business matters inside the United States. He also carried an unlocked smartphone that he had brought on the trip because it enabled him to communicate easily while overseas.

78. At the passport control area in the Dallas-Fort Worth airport, a CBP officer directed Mr. Allababidi to a secondary inspection area. There, as CBP officers searched his belongings, Mr. Allababidi observed a CBP officer seize and manually search his unlocked phone for at least 20 minutes. The officer then returned the phone to Mr. Allababidi.

79. The officer then ordered Mr. Allababidi to unlock his other phone. Concerned about officers accessing private information on his phone, Mr. Allababidi

declined to do so. CBP officers responded by confiscating both phones, including the unlocked phone that the officer had already searched and returned to him.

80. The government returned the unlocked phone to Mr. Allababidi more than two months later. After more than seven months, CBP still has not returned the locked phone to him.

Sidd Bikkannavar

81. On January 31, 2017, Mr. Bikkannavar flew into Houston, Texas, from Santiago, Chile, where he had been on vacation. He traveled with a locked smartphone that is the property of his employer, NASA's Jet Propulsion Laboratory ("JPL"). Consistent with his employer's policies, Mr. Bikkannavar used the phone for both work and personal matters.

82. At the passport control area of the Houston airport, CBP officers escorted Mr. Bikkannavar to a secondary inspection area. A CBP officer seized Mr. Bikkannavar's phone. The officer coerced Mr. Bikkannavar into disclosing his phone's password. Specifically:

a. The secondary inspection setting is inherently coercive. *Supra* ¶¶ 47–48.

b. A CPB officer had handed Mr. Bikkannavar a CBP form titled "Inspection of Electronic Devices."[8] It stated in relevant part: "All persons, baggage, and merchandise . . . are subject to inspection, search and detention. . . . [Y]our electronic device(s) has been detained for further examination, which may include copying. . . . CBP may retain documents or information . . . . Consequences of failure to provide

[8] https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf.

c. When Mr. Dupin had told a CBP officer that he was frustrated by the delay in his processing, the officer responded by putting his hand on the holster of his gun and ordering Mr. Dupin to sit down and wait.

90. A CBP officer searched Mr. Dupin's phone for about two hours. During some of this time, Mr. Dupin observed the officer manually searching his phone. At other times, the officer took Mr. Dupin's phone into another room and returned periodically to ask Mr. Dupin questions about the contents of the phone, including his photos, emails, and contacts.

91. After Mr. Dupin had spent about two hours in the smaller room, the officers returned Mr. Dupin's phone to him and told him he could leave.

Search 2

92. On December 23, 2016, Mr. Dupin traveled by bus with his seven-year-old daughter from Montreal to New York City. Mr. Dupin carried the same locked smartphone with him.

93. Mr. Dupin and his daughter arrived at the customs checkpoint at the U.S. border near midnight. A CBP officer directed Mr. Dupin and his daughter to a secondary inspection area, where they waited and tried to sleep. CBP officers arrived and asked Mr. Dupin some of the same questions officers had asked him in Miami.

94. During the questioning, the officers seized Mr. Dupin's phone and ordered him to provide the password to the phone. As on the day before, Mr. Dupin had no meaningful choice and provided the password.

95. The officers coerced Mr. Dupin into unlocking his phone. Specifically:

a. The secondary inspection setting is inherently coercive. *Supra* ¶¶ 47–48.

b. Mr. Dupin again understood, based on the CBP officers' tone and demeanor, that they were commanding him to disclose his password.

c. It was the middle of the night, and the bus on which Mr. Dupin and his daughter had been traveling had already departed. Mr. Dupin did not know how or when he would be able to catch another bus to New York City.

d. Mr. Dupin was traveling with his young daughter. When the officers ordered Mr. Dupin to unlock his phone, his exhausted daughter was trying to sleep in his lap. Mr. Dupin feared that if he refused to unlock his phone, the officers would escalate the encounter, which would upset and frighten his daughter.

96. A CBP officer took Mr. Dupin's phone into another room for about four hours. During this time, one or more CBP officers searched the phone. An officer periodically returned to ask Mr. Dupin questions about the contents of the phone, including specific photos and emails.

97. After approximately seven hours of detention on the morning of Christmas Eve, officers returned the phone to Mr. Dupin and told him that he and his daughter could catch another bus to New York City.

Aaron Gach

98. On February 23, 2017, Mr. Gach arrived at San Francisco International Airport on a flight from Belgium, where he had participated in an art exhibition displaying works that could be considered critical of the government. He traveled with a locked smartphone.

99. A CBP officer directed Mr. Gach to a secondary inspection area, where two CBP officers asked him detailed questions about his work as an artist and the exhibition in Belgium and told him they needed to search his phone. Mr. Gach responded that he did not want the officers to search his phone, and he asked what specific information the officers were seeking. They refused to identify any information in response.

100. The CBP officers asked Mr. Gach why he did not want to submit his phone for a search. Mr. Gach responded that he believes strongly in the U.S. Constitution and in his right to privacy. The officers told Mr. Gach that his phone would be held for an indeterminate amount of time if he did not disclose his password. The CBP officers continued to demand that Mr. Gach submit to a phone search. Because he had no meaningful choice, Mr. Gach entered his password and handed over his unlocked phone.

101. The officers coerced Mr. Gach into unlocking his phone. Specifically:

a. The secondary inspection setting is inherently coercive. *Supra* ¶¶ 47–48.

b. The officers repeatedly demanded that Mr. Gach produce his phone for a search.

c. The CBP officers told Mr. Gach that they would keep his phone for an indeterminate amount of time if he did not unlock his phone for a search.

102. The officers refused to conduct a search of the phone in Mr. Gach's presence. Instead, they took it behind a dividing wall for approximately 10 minutes.

103. On information and belief, one or more CBP officers searched Mr. Gach's phone during this time. They had the means to do so (Mr. Gach had unlocked it), and they had no reason to order him to unlock it other than to search it.

104. The CBP officers then returned Mr. Gach's phone and permitted him to leave the secondary inspection area.

Isma'il Kushkush

Search 1

105. On January 9, 2016, Mr. Kushkush traveled to New York City from Stockholm, Sweden, where he had been conducting research for his master's thesis on refugees for Columbia Journalism School. He had a locked laptop computer and two unlocked cell phones, one being a smartphone, with him. He uses his laptop and phones for his work as a journalist.

106. Upon Mr. Kushkush's arrival at New York's John F. Kennedy International Airport, CBP officers took him to a secondary inspection area, where they questioned him and searched his belongings. The officers searched his notebooks, which contained information related to his work as a journalist, and asked him about the contents of the notebooks.

107. The CBP officers took Mr. Kushkush's laptop and two phones out of his sight for approximately 20 minutes. On information and belief, one or more CBP officers searched Mr. Kushkush's two phones during this time, either manually or forensically. The officers returned the devices to Mr. Kushkush and permitted him to leave after he had spent approximately three hours in the secondary inspection area.

information and belief, one or more CBP officers searched Mr. Kushkush's unlocked devices during that time, either manually or forensically.

113. The officers returned the devices to Mr. Kushkush and permitted him to leave after he had spent about one and a half hours in the secondary inspection area.

Search 3

114. On July 30, 2017, Mr. Kushkush traveled by bus from Middlebury, Vermont, where he was attending a language program at Middlebury College, to Montreal, Quebec, along with other students in the program. They returned the following day, on July 31, 2017, and entered the United States at Highgate Springs, Vermont. Mr. Kushkush carried a locked smartphone with him.

115. A CBP officer directed Mr. Kushkush to secondary inspection, where he waited for approximately one hour. An officer then demanded Mr. Kushkush's phone and the password to unlock it. The officer stated that he could seize the phone if Mr. Kushkush did not cooperate. Because he had no meaningful choice, Mr. Kushkush unlocked his phone and stated that he was doing so against his will.

116. Mr. Kushkush was coerced into unlocking his phone. Specifically:

a. The secondary inspection setting is inherently coercive. *Supra* ¶¶ 47–48.

b. The CBP officer told Mr. Kushkush that he would keep his phone for an indeterminate amount of time if Mr. Kushkush did not unlock his phone for a search.

117. The CBP officer wrote down the password to Mr. Kushkush's phone as he unlocked it and took the phone out of Mr. Kushkush's sight for at least one hour. On

information and belief, one or more CBP officers then searched the phone, either manually or forensically: they had the means to do so (Mr. Kushkush had unlocked it), and they had no reason to order him to unlock the phone other than to search it.

118. After nearly three hours, two CBP officers directed Mr. Kushkush to a separate room, where they questioned him about his work as a journalist.

119. The officers permitted Mr. Kushkush to leave after he had spent approximately three and a half hours in the customs inspection building. He was given his phone to take with him.

Diane Maye

120. On June 25, 2017, Ms. Maye flew from Oslo, Norway, to Miami, Florida. She was on her way home after a vacation in Europe. She was traveling with a locked laptop computer and a locked smartphone.

121. Upon landing, a CBP officer seized Ms. Maye's computer and phone and ordered her to unlock the devices. Because she had no meaningful choice, Ms. Maye unlocked both devices.

122. An officer coerced Ms. Maye into unlocking her computer and phone. Specifically:

a. The secondary inspection setting is inherently coercive. *Supra* ¶¶ 47–48.

b. She was confined alone with two CBP officers in a small room that felt to her like a police station. An officer had ordered her to enter the room.

c. Ms. Maye understood, based on the CBP officers' tone and demeanor, that they were commanding her to unlock her devices.

d. Ms. Maye was exhausted after 24 hours of continuous travel, and she needed to communicate with her husband, who was waiting for her.

123. Ms. Maye observed a CBP officer manually search her unlocked laptop.

124. A CBP officer seized Ms. Maye's unlocked phone for approximately two hours. On information and belief, one or more CBP officers searched Ms. Maye's phone during this time: they had the means to do so (Ms. Maye had unlocked it), and they had no reason to order her to unlock it other than to search it.

Zainab Merchant

125. Zainab Merchant is the founder and editor of *Zainab Rights*, a media organization that publishes multimedia content on the Internet on current affairs, politics, and culture, and she is a graduate student at Harvard University.

126. In March 2017, Ms. Merchant traveled from her home in Orlando, Florida to Toronto, Ontario to visit her uncle. On March 5, 2017, she went to the Toronto airport for her flight home to Orlando. She carried with her a locked laptop and a locked smartphone.

127. At a U.S. customs preclearance station at the Toronto airport, she was directed to a secondary inspection area.

128. CBP officers took Ms. Merchant's laptop out of her sight.

129. CBP officers told her to turn over her smartphone. Ms. Merchant, who wears a headscarf in public in accordance with her religious beliefs, did not want to turn over the phone because it contained pictures of her without her headscarf that she did not want officers to see. It also contained information and communications related to her blog site. She told the CBP officers she would turn over the phone, but would not unlock it. A

135. Ms. Merchant's laptop and phone were out of her sight for approximately one and a half hours. On information and belief, one or more CBP officers searched her laptop and phone during this time: they had the means to do so (they had the passwords), and they had no reason to seize the laptop and phone other than to search them. When the CBP officers returned the phone to Ms. Merchant and she unlocked it, the Facebook application was open to the "friends" page. It had not been open to that page when she had given up the phone.

Akram Shibly

Search 1

136. Akram Shibly drove from his home in Buffalo, New York, to Toronto, Ontario, in late December 2016 for his job as a professional filmmaker. He returned on January 1, 2017, and sought to enter the United States at the Lewiston-Queenston Bridge in New York. He was traveling with a locked smartphone.

137. At the customs checkpoint, a CBP officer directed Mr. Shibly to a secondary inspection area, where officers told Mr. Shibly to fill out a form with information that included, among other things, his phone's password. Mr. Shibly left that line of the form blank. A CBP officer examined the completed form and ordered Mr. Shibly to provide his password. Mr. Shibly told the officer that he did not feel comfortable doing so. In an accusatory manner, the officer told Mr. Shibly that if he had nothing to hide, then he should unlock his phone.

138. Because he had no meaningful choice, Mr. Shibly disengaged the lock screen of his phone, which the officer then took from him.

139. The officer coerced Mr. Shibly into unlocking his phone. Specifically:

a. The secondary inspection setting is inherently coercive. *Supra* ¶¶ 47–48.

b. Mr. Shibly understood, based on the CBP officer's tone and demeanor, that the officer was commanding him to disclose his password.

c. Mr. Shibly feared that if he refused to unlock his phone, the officer would assume he had done something wrong and treat him accordingly. Among other things, Mr. Shibly feared that if he refused to unlock his phone, the officer would detain him for the rest of the day.

140. The CBP officer took Mr. Shibly's phone out of his sight for at least one hour. On information and belief, one or more CBP officers searched Mr. Shibly's phone during this time: they had the means to do so (Mr. Shibly had unlocked it), and they had no reason to order him to unlock it other than to search it.

141. A CBP officer also coerced Mr. Shibly into disclosing his social media identifiers. On information and belief, CBP officers used this information to facilitate their search of Mr. Shibly's phone as a portal to search his cloud-based apps and content.

142. A CBP officer returned Mr. Shibly's phone and permitted him to leave the customs inspection building.

Search 2

143. On January 4, 2017, Mr. Shibly again drove from Buffalo to the Toronto area for a social outing. He returned later that day and again sought to enter the United States at the Lewiston-Queenston Bridge in New York. He was traveling with the same smartphone, but this time it was not locked, because he had not restored the lock screen that he had disengaged during the prior border crossing.

149. The CBP officers confiscated Mr. Wright's devices on instructions from ICE's Homeland Security Investigations ("HSI"), which sought "further forensic review," according to CBP documents disclosed to Mr. Wright under the Freedom of Information Act and Privacy Act ("FOIA/PA").

150. An officer informed Mr. Wright that it might take CBP as long as a year to return his devices to him.

151. Soon after leaving the airport, Mr. Wright spent $2,419.97 for a new laptop and phone. He is a computer programmer, and his livelihood depends on these tools.

152. CBP records show that HSI "attempted to image" Mr. Wright's laptop with MacQuisition software. Also, a CBP forensic scientist extracted data from the SIM card in Mr. Wright's phone and from his camera, stored the data on three thumb drives, and sent those thumb drives to other CBP officers.

153. CBP did not find any "derogatory" information about Mr. Wright, in his devices or otherwise, according to a CBP document disclosed to Mr. Wright under the FOIA/PA.

154. Mr. Wright received his devices 56 days after CBP had confiscated them.

155. On information and belief, CBP retained the information it extracted from Mr. Wright's devices:

a. CBP extracted data from Mr. Wright's devices. *Supra* ¶ 152.

b. The 2009 CBP Policy provides that if a CBP officer destroys the information extracted from a traveler's device, then the agent must document the destruction. ¶ 5.3.1.2.

c. CBP's documentation of its search and seizure of Mr. Wright's devices, disclosed to Mr. Wright under the FOIA/PA, does not reflect such destruction.

FACTS RELEVANT TO ALL PLAINTIFFS

156. All Plaintiffs face a likelihood of future injury caused by the challenged policies and practices:

a. Defendants adopted the policies and practices discussed above related to searching and seizing electronic devices at the border. The frequency with which border officials enforce these policies and practices against travelers is rapidly growing. *Supra* ¶ 38.

b. All Plaintiffs have traveled across the U.S. border with their electronic devices multiple times. All Plaintiffs will continue to do so in the future.

c. When Plaintiffs cross the U.S. border, they will be subject to CBP's and ICE's policies and practices. Thus, all Plaintiffs are at great risk of constitutional harm, namely, search and seizure of their devices absent a warrant, probable cause or reasonable suspicion that their electronic devices contain contraband or evidence of a violation of immigration or customs laws. There is nothing that Plaintiffs can do to avoid this harm, except to forego international travel or to travel without any electronic devices, which would cause great hardship.

157. On information and belief, Plaintiffs are suffering the ongoing harm of CBP and ICE retaining (a) content copied from their devices or records reflecting content observed during searches of their devices, (b) content copied from their cloud-based accounts accessed through their devices or records reflecting content from their cloud-

EXHIBIT 17

No 579936

1. Held for other agency? Yes ☐ No ☐
Name of Agency
2. Certified Mail No.
3. Investigative Case No.
4. General Order No.
5. Exodus Command Center Notified?
☐ Yes ☐ No
Date: Time:

DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

Detention Notice and Custody Receipt for Detained Property
Handbook 5200-09

6. Port Code	7. Date of Detention (mm/dd/yyyy)	8. Time (Use 24 Hours)	9. Entry Number
5501	01/24/2017	1600	

10. Detained from:

11. Seal or Other ID No.

Name: ALLABABIDI, SUHAIB

12. Misc. Nos.

Address: [redacted]

13. Remarks

Telephone No.: [redacted]

14. FPF No. (For CBPLab Use Only) ☐☐☐☐☐☐☐☐☐☐☐☐☐☐-☐☐

15. Point of Contact Information - Send all correspondence to: [redacted]

16. Additional Information/Action Request from Importer/Exporter/Subject

Telephone No. [redacted] Fax No. ( )

17. Reason for Detention: BORDER SEARCH OF ELECTRONIC MEDIA

18. Tests or Inquiries to be Conducted: EXAMINATION

19. **PROPERTY** (By Line Item) Attach CBP 58 if conveyance

a. Line Item No.	b. Description	c. Packages Number	c. Packages Type	d. Measurement Qty.	d. Measurement UM	e. Est. Dom. Value	f. Samples Sent to the CBP Lab Yes or No	Date
001	Apple I-phone			1		$	Yes ☐ No ☐	/ /
002	SAMSUNG CELLPHONE			1		$	Yes ☐ No ☐	/ /
						$	Yes ☐ No ☐	/ /
						$	Yes ☐ No ☐	/ /

20. Detaining Officer Name
Special Agent Charles Plosser 01/24/2017
Print Signature Date

21. **ACCEPTANCE/CHAIN OF CUSTODY**

a. Line Item No.	b. Description	c. Print Name/Title/Organization	d. Signature	e. Date
001/002	Apple I Phone / SAMSUNG CELLPHONE	CHARLES PLOSSER / SA/HSI		01-24-2017

Shipments may be detained for up to 30 days, unless statutory authority or interagency agreement mandates that a longer period of time is required, or the importer/exporter/subject requests a longer detention period through the Port Director.

CBP 6051A Continuation Sheet Attached? Yes ☐ No ☑

CBP Form 6051D (08/03)

PID0062

EXHIBIT 18

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.

In evaluating and updating its policies, CBP carefully evaluated its operational posture to ensure that CBP was fulfilling its operational responsibilities while protecting civil rights and civil liberties. In striking this balance, CBP imposed certain requirements above what is currently required by law. Notably, CBP distinguished between *types* of border searches based on their level of intrusiveness. Creating a categorical exception to CBP's authority to search items crossing the border would pose a dangerous threat to national security. With that in mind, basic searches continue to require no level of suspicion. This is crucial – any other rule would allow those who seek to harm U.S. interests to bring something across the border that completely evades inspection. Notably, the vast majority of CBP border searches of electronic devices are basic searches designed to evaluate what is crossing the border. On the other hand, for an advanced search – which involves connection to external equipment not merely to gain access to the device, but to review, copy, and/or analyze its contents – CBP requires the search is done in situations in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern.

Additional Request for CBP:

Q. What factors determine if and when a traveler will be referred to secondary screening?
A. Secondary inspection is used as a queuing management technique for people who need additional time to complete the inspectional process so that an officer can make a determination about compliance with the laws CBP enforces.

Q. Does an individual have to be referred to secondary screening to have a basic or advanced search of their electronic devices conducted?
A. Secondary inspection is merely a continuation of the inspection initiated at primary for travelers who require a more extensive examination to ensure compliance with the laws CBP enforces. As a general matter, an officer may examine an electronic device and may review and analyze information encountered at the border in basic searches of electronic devices. Advanced searches of electronic devices occur when an officer connects the electronic device to external equipment no review, copy and/or analyze its content.

Q. Does a referral to secondary screening mean you have a "reasonable suspicion" based upon a traveler's behavior, advance intelligence or information, etc.?
A. No. Individuals are referred for additional scrutiny for a number of reasons, including at random. Each secondary inspection is different; depending on the circumstances, secondary inspection can last anywhere from a few minutes to several hours.

Q. What impact would raising the standard to "probable cause" have on CBP officers' ability to perform their duties?
A. In the criminal context, reasonable suspicion generally requires "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *United States v. Cortez*, 449 U.S. 411, 417–18 (1981). Probable cause is an even more exacting standard and generally requires the officer determine there is a fair probability that seizable evidence will be found in a particular place or on a particular person or that a particular person committed a crime. *See Florida v. Harris*, 568 U.S. 237, 243-44 (2013). These standards' focus on a *particularized* information relating to *criminal activity* are not readily translatable to the border

EXHIBIT 19

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049A

DATE: January 4, 2018
ORIGINATING OFFICE: FO:TO
SUPERSEDES: Directive 3340-049
REVIEW DATE: January 2021

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES

1 **PURPOSE.** To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. They can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws.

2 POLICY

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

2.3 This Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of this Directive, this excludes actions taken to determine if a device functions (e.g., turning a device on and off); or actions taken to determine if physical contraband is concealed within the device itself; or the review of information voluntarily provided by an individual in an electronic format (e.g., when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). This Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., an importation of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the functional equivalent of the border (FEB), or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

3 DEFINITIONS

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Special Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. 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, music and other media players.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

4 AUTHORITY/REFERENCES. 6 U.S.C. §§ 122, 202, 211; 8 U.S.C. §§ 1225, 1357, and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

The plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty. "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that 'searches made at the border, pursuant to the longstanding 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.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). "Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Additionally, the authority to conduct border searches extends not only to persons and merchandise entering the United States, but applies equally to those departing the country. *See, e.g.*, *United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Odutayo*, 406 F.3d 386, 391-92 (5th Cir. 2005); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995); *United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991); *United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983).

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. *See Flores-Montano*, 541 U.S. at 154 (noting that "the expectation of privacy is less at the border than it is in the interior"). Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign. *See Boumelhem*, 339 F.3d at 423.

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, such as electronic devices. *See, e.g.*, 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a; *see also* 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of

the United States from places outside thereof are liable to inspection and search by a Customs officer."). These authorities support CBP's enforcement and administration of federal law at the border and facilitate the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department. This includes, among other things, the responsibility 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 the illegal entry of terrorists, terrorist weapons, persons, and contraband"; and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons." 6 U.S.C. § 211.

CBP must conduct border searches of electronic devices in accordance with statutory and regulatory authorities and applicable judicial precedent. CBP's broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

5 PROCEDURES

5.1 Border Searches

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. § 507).

5.1.2 Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

5.1.3 Basic Search. Any border search of an electronic device that is not an advanced search, as described below, may be referred to as a basic search. In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.4 Advanced Search. An advanced search is 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 the device, but to review, copy, and/or analyze its contents. In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device. Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.

5.1.5 Searches of electronic devices will be documented in appropriate CBP systems, and advanced searches should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire advanced search, or where supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.6 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to remain present during a search does not necessarily mean that the individual shall observe the search itself. If permitting an individual to observe the search could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material

5.2.1 Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.

5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP Associate/Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

5.2.1.3 At the completion of the CBP review, unless any materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained in coordination with the CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel office, and this consultation shall be noted in appropriate CBP systems.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel office or the CBP Privacy Officer, as appropriate.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect appropriately such information, and such information will only be shared in accordance with this Directive.

5.3 Review and Handling of Passcode-Protected or Encrypted Information

5.3.1 Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents. Passcodes or other means of access may be requested and retained as needed to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on the device that is being inspected or has been detained, seized, or retained in accordance with this Directive.

5.3.2 Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

5.3.3 If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.

5.3.4 Nothing in this Directive limits CBP's ability, with respect to any device presented in a manner that is not readily accessible for inspection, to seek technical assistance, or to use external equipment or take other reasonable measures, or in consultation with the CBP Associate/Assistant Chief Counsel office to pursue available legal remedies, to render a device in a condition that allows for inspection of the device and its contents.

5.4 Detention and Review in Continuation of Border Search of Information

5.4.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days. Devices must be presented in a manner that allows CBP to inspect their contents. Any device not presented in such a manner may be subject to exclusion, detention, seizure, or other appropriate action or disposition.

5.4.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems.

5.4.1.2 Destruction. Except as noted in section 5.5 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.4, there is no probable cause to seize the device or the information contained therein, any copies of the information held by CBP must be destroyed, and any electronic device must be returned. Upon this determination, the copy of the information will be destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system and which must be no later than twenty-one (21) days after such determination. The destruction shall be noted in appropriate CBP systems.

5.4.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, the individual subject to search will be notified of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. If the Officer or other appropriate CBP official determines that the fact of conducting this search cannot be disclosed to the individual transporting the device without

impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld.

5.4.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.4.2 Assistance

Officers may request assistance that may be needed to access and search an electronic device and the information stored therein. Except with respect to assistance sought within CBP or from ICE, the following subsections of 5.4.2 govern requests for assistance.

5.4.2.1 Technical Assistance. Officers may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection. For example, Officers may encounter a device or information that is not readily accessible for inspection due to encryption or password protection. Officers may also require translation assistance to inspect information that is in a foreign language. In such situations, Officers may convey electronic devices or copies of information contained therein to seek technical assistance.

5.4.2.2 Subject Matter Assistance – With Reasonable Suspicion or National Security Concern. Officers may encounter information that requires referral to subject matter experts to determine the meaning, context, or value of information contained therein as it relates to the laws enforced or administered by CBP. Therefore, Officers may convey electronic devices or copies of information contained therein for the purpose of obtaining subject matter assistance when there is a national security concern or they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP.

5.4.2.3 Approvals for Seeking Assistance. Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.4.2.4 Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of data from the device should be conveyed in lieu of the device in accordance with this Directive.

5.4.2.5 When an electronic device or information contained therein is conveyed for assistance, the individual subject to search will be notified of the conveyance unless the Officer or other appropriate CBP official determines, in consultation with the receiving agency or other entity as appropriate, that notification would impair national security, law enforcement, officer safety, or other operational interests. If CBP seeks assistance for counterterrorism purposes, if a relevant national security-related lookout applies, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the conveyance, the existence of a relevant national security-related lookout, or his or her presence on a watch list.

When notification is made to the individual, the Officer will annotate the notification in CBP systems and on the Form 6051D.

5.4.3 Responses and Time for Assistance

5.4.3.1 Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are expected to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced or administered by CBP.

5.4.3.2 Time for Assistance. Responses from assisting agencies or entities are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager, responses should be received within fifteen (15) days. If the assisting agency or entity is unable to respond in that period of time, the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager may permit extensions in increments of seven (7) days.

5.4.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency or entity to return to CBP all electronic devices provided, and any copies thereof, as expeditiously as possible, except as noted in 5.5.2.3. Any such revocation shall be documented in appropriate CBP systems. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency or entity pursuant to the procedures outlined in this Directive.

5.4.3.4 Destruction. Except as noted in section 5.5.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the device or the information from the device does not exist, CBP will retain no copies of the information.

5.5 Retention and Sharing of Information Found in Border Searches

5.5.1 Retention and Sharing of Information Found in Border Searches

5.5.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer.

5.5.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice. For example, information

collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or E3 or other systems as may be appropriate and consistent with the policies governing such systems.

5.5.1.3 Sharing Generally. Nothing in this Directive limits the authority of CBP to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

5.5.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is authorized by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. § 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with entities of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the entity receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.5.1.5 Safeguarding Data During Storage and Conveyance. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during conveyance. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during conveyance such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the CBP Office of Professional Responsibility and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

5.5.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.5.2 Retention by Agencies or Entities Providing Technical or Subject Matter Assistance

5.5.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting agency or entity may be retained for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.5.2.3 below.

5.5.2.2 Return or Destruction. CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible, and that the assisting agency or entity advise CBP in accordance with section 5.4.3 above. In addition, the assisting agency or entity should destroy all copies of the information conveyed unless section 5.5.2.3 below applies. In the event that any electronic devices are conveyed, they must not be destroyed;

they are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.2.3.

5.5.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency assumes responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.6 Reporting Requirements

5.6.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.6.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.4.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.6.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.7 Management Requirements

5.7.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.7.2 The appropriate CBP second-line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.7.3 The appropriate CBP second-line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another agency or entity.

5.7.4 The Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of

information contained therein in order to ensure compliance with the procedures outlined in this Directive.

5.7.5 Officers will ensure, in coordination with field management as appropriate, that upon receipt of any subpoena or other request for testimony or information regarding the border search of an electronic device in any litigation or proceeding, notification is made to the appropriate CBP Associate/Assistant Chief Counsel office.

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 REVIEW. This Directive shall be reviewed and updated, as necessary, at least every three years.

10 DISCLOSURE. This Directive may be shared with the public.

11 SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008), to the extent they pertain to electronic devices; CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).

Acting Commissioner

EXHIBIT 20

From: [redacted]
Sent: Friday, May 11, 2018 5:19 PM
To: [redacted]
[redacted]
Subject: (0476-18) Broadcast- Legal Update- Border Search of Electronic Devices

HSI HOMELAND SECURITY INVESTIGATIONS
Message from the AD of Domestic Operations

Legal Update Border Search of Electronic Devices

On May 9, 2018, in *United States v. Kolsuz*, the U.S. Court of Appeals for the Fourth Circuit held that the "forensic" examination of a cell phone is a nonroutine border search, requiring some measure of individualized suspicion. --- F.3d ---, 2018 WL 2122085 (4th Cir. 2018). The court, however, determined that it need not resolve whether the proper standard should be reasonable suspicion or probable cause and a warrant.

Although the Office of the Principal Legal Advisor (OPLA) advises Homeland Security Investigations (HSI) nationwide that it should have reasonable suspicion before performing an advanced search of an electronic device (any border search of an electronic device in which external equipment, through a wired or wireless connection, is connected to an electronic device not merely to gain access to the device or its contents but to review, copy, and/or analyze its contents), **this decision creates binding precedent in the jurisdiction of the U.S. Court of Appeals for the Fourth Circuit that at least some level of individualized suspicion is required for such searches;** the only other circuit to have required this standard is the Ninth Circuit Court of Appeals. *See U.S. v. Cotterman*, 709 F.3d 952 (9th Cir. 2013 (en banc).

Formal policy guidance with regard to border searches of electronic devices is forthcoming. In the interim, in order to limit litigation risk, HSI Special Agents and others authorized by HSI to perform border searches, even outside of the Fourth and Ninth Circuits, should no longer perform advanced border searches of electronic

devices without reasonable suspicion. All factors supporting such a standard should be documented in reports of investigation.

If you have any questions on this matter, please contact OPLA imbed counsel.

Limitation on the Applicability of this Guidance. This message is intended to provide internal guidance to the operational components of U.S. Immigration and Customs Enforcement. It does not, is not intended to, shall not be construed to, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any person in any matter, civil or criminal.

[redacted]

Thanks,

Tatum King
Assistant Director, Domestic Operations
Homeland Security Investigations

HSI Domestic Operations / MW
500 12th Street SW, 6th Floor
Washington, D.C. 20536
Email – [redacted]

EXHIBIT 21

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
ICE Policy System

DISTRIBUTION:	**ICE**
DIRECTIVE NO.:	**7-6.1**
ISSUE DATE:	**August 18, 2009**
EFFECTIVE DATE:	**August 18, 2009**
REVIEW DATE:	**August 18, 2012**
SUPERSEDES:	**See Section 3 Below.**

DIRECTIVE TITLE: BORDER SEARCHES OF ELECTRONIC DEVICES

1. PURPOSE and SCOPE.

1.1. This Directive provides legal guidance and establishes policy and procedures within U.S. Immigration and Customs Enforcement (ICE) with regard to border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border to ensure compliance with customs, immigration, and other laws enforced by ICE. This Directive applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise.

1.2. This Directive applies to border search authority only. Nothing in this Directive limits the authority of ICE Special Agents to act pursuant to other authorities such as a warrant, a search incident to arrest, or a routine inspection of an applicant for admission.

2. AUTHORITIES/REFERENCES. 8 U.S.C. § 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; and the December 12, 2008, ICE Office of Investigations (OI) guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices."

3. SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES. ICE Directive No. 7-6.0 entitled "Border Searches of Documents and Electronic Media" is hereby superseded as it relates to electronic devices. Additionally, all other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded as they relate to searches of electronic devices, with the exception of the March 5, 2007, OI guidance entitled "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry" and the December 12, 2008, OI guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media."

4. BACKGROUND. ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, Special Agents may review and analyze computers, disks, hard drives, and other electronic or digital storage devices. These searches are part of ICE's long-standing practice and are essential to enforcing the law at the United States border. Searches of electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

5. DEFINITIONS. The following definitions are provided for the purposes of this Directive:

5.1. Assistance. The use of third party analytic resources such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in electronic devices or in determining the meaning, context, or value of information contained therein.

5.2. Electronic Devices. Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices.

6. POLICY.

6.1. ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth herein. Assistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate.

6.2. When U.S. Customs and Border Protection (CBP) detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.

6.3. Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems.

7. RESPONSIBILITIES.

7.1. The Directors of OI, the Office of Professional Responsibility (OPR), and the Office of International Affairs (OIA) have oversight over the implementation of the provisions of this Directive.

7.2. Special Agents in Charge (SACs) and Attachés are responsible for:

1) Implementing the provisions of this Directive and ensuring that Special Agents in their area of responsibility (AOR) receive a copy of this Directive and are familiar with its contents;

2) Ensuring that Special Agents in their AOR have completed any training programs relevant to border searches of electronic devices, including constitutional, privacy, civil rights, and civil liberties training related to such searches, as may be required by ICE Headquarters; and

3) Maintaining appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this Directive. (See "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices" memo dated December 12, 2008.)

7.3. Attachés are responsible for ensuring coordination with their host countries, as appropriate, before conducting any such border search outside of the United States.

7.4. When ICE receives electronic devices, or copies of information therefrom, from CBP for analysis and investigation, ICE Special Agents are responsible for advising CBP of the status of any such analysis within 10 calendar days, and periodically thereafter, so that CBP records may be updated as appropriate. For example, "search ongoing"; "completed with negative results"; "returned to traveler"; or "seized as evidence of a crime."

7.5. Special Agents are responsible for complying with the provisions of this Directive, knowing the limits of ICE authority, using this authority judiciously, and ensuring comprehension and completion of any training programs relevant to border searches of electronic devices as may be required by ICE.

8. PROCEDURES.

8.1. Border Searches by ICE Special Agents.

1) Authorization to Conduct Border Search. Border searches of electronic devices must be performed by an ICE Special Agent who meets the definition of "customs officer" under 19 U.S.C. § 1401(i), or another properly authorized officer with border search authority, such as a CBP Officer or Border Patrol Agent, persons cross designated by ICE as customs officers, and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.

2) Knowledge and Presence of the Traveler. To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler. When not practicable due to law enforcement, national security, or other operational concerns, such circumstances are to be noted by the Special Agent in appropriate ICE systems. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement

techniques or potentially compromise other operational concerns, the individual will not be permitted to observe the search.

3) Consent Not Needed. At no point during a border search of electronic devices is it necessary to ask the traveler for consent to search.

4) Continuation of the Border Search. At any point during a border search, electronic devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location, including a location associated with a demand for assistance from an outside agency or entity (see Section 8.4).

5) Originals. In the event electronic devices are detained, the Special Agent should consider whether it is appropriate to copy the information therefrom and return the device. When appropriate, given the facts and circumstances of the matter, any such device should be returned to the traveler as soon as practicable. Consultation with the Office of the Chief Counsel is recommended when determining whether to retain a device in an administrative immigration proceeding. Devices will be returned to the traveler as expeditiously as possible at the conclusion of a negative border search.

8.2. Chain of Custody.

1) Detentions of electronic devices. Whenever ICE detains electronic devices, or copies of information therefrom, the Special Agent will initiate the correct chain of custody form or other appropriate documentation.

2) Seizures of electronic devices for criminal purposes. Whenever ICE seizes electronic devices, or copies of information therefrom, the Special Agent is to enter the seizure into the appropriate ICE systems. Additionally, the seizing agent must complete the correct chain of custody form or other appropriate documentation.

3) Retention of electronic devices for administrative immigration purposes. Whenever ICE retains electronic devices, or copies of information therefrom, or portions thereof, for administrative immigration purposes pursuant to 8 U.S.C. § 1357, the Special Agent is to record such retention in appropriate ICE systems and is to include the location of the retained files, a summary thereof, and the purpose for retention.

4) Notice to traveler. Whenever ICE detains, seizes, or retains original electronic devices, the Special Agent is to provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation.

8.3. Duration of Border Search.

1) Special Agents are to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search. Searches are generally to be completed within 30 calendar days of

the date of detention, unless circumstances exist that warrant more time. Such circumstances must be documented in the appropriate ICE systems. Any detention exceeding 30 calendar days must be approved by a Group Supervisor or equivalent, and approved again every 15 calendar days thereafter, and the specific justification for additional time documented in the appropriate ICE systems.

2) Special Agents seeking assistance from other Federal agencies or non-Federal entities are responsible for ensuring that the results of the assistance are received in a reasonable time (see Section 8.4(5)).

3) In determining "reasonable time," courts have reviewed the elapsed time between the detention and the completion of the border search, taking into account any additional facts and circumstances unique to the case. As such, ICE Special Agents are to document the progress of their searches, for devices and copies of information therefrom, and should consider the following factors:

   a) The amount of information needing review;

   b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;

   c) Whether assistance was sought and the type of such assistance;

   d) Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;

   e) Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and

   f) Any unanticipated exigency that may arise.

8.4. Assistance by Other Federal Agencies and Non-Federal Entities.

1) Translation, Decryption, and Other Technical Assistance.

   a) During a border search, Special Agents may encounter information in electronic devices that presents technical difficulties, is in a foreign language, and/or encrypted. To assist ICE in conducting a border search or in determining the meaning of such information, Special Agents may demand translation, decryption, and/or technical assistance from other Federal agencies or non-Federal entities.

   b) Special Agents may demand such assistance absent individualized suspicion.

   c) Special Agents shall document such demands in appropriate ICE systems.

2) Subject Matter Assistance.

   a) During a border search, Special Agents may encounter information in electronic devices that are not in a foreign language or encrypted, or that do not require other technical assistance, in accordance with Section 8.4(1), but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by ICE. For the purpose of obtaining such subject matter expertise, Special Agents may create and transmit a copy of such information to other Federal agencies or non-Federal entities.

   b) Special Agents may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by ICE.

   c) Special Agents shall document such demands in appropriate ICE systems.

3) Demand Letter. Unless otherwise governed by a Memorandum of Understanding or similar mechanism, each demand for assistance is to be in writing (e.g., letter or email), approved by a supervisor, and documented in the appropriate ICE systems. Demands are to detail the context of the search requested, ICE's legal parameters regarding the search, retention, and sharing of any information found during the assistance, and relevant timeframes, including those described in this Directive.

4) Originals. For the purpose of obtaining subject matter assistance, Special Agents may create and transmit copies of information to other Federal agencies or non-Federal entities. Original electronic devices should be transmitted only when necessary to render the demanded assistance.

5) Time for Assistance and Responses Required.

   a) Assistance is to be accomplished within a reasonable period of time in order to preserve the status of the electronic devices and the integrity of the border search.

   b) It is the responsibility of the Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities and to act in accord with section 8.3 of this Directive. In addition, Special Agents shall:

      i) Inform assisting agencies or entities that they are to provide results of assistance as expeditiously as possible;

      ii) Ensure that assisting agencies and entities are aware that responses to ICE must include any findings, observations, and conclusions drawn from their review that may relate to the laws enforced by ICE;

iii) Contact the assisting agency or entity to get a status report on the demand within the first 30 calendar days;

iv) Remain in communication with the assisting agency or entity until results are received;

v) Document all communications and actions in appropriate ICE systems; and

vi) Consult with a supervisor to determine appropriate action if the timeliness of results is a concern. If a demand for assistance is revoked, the Special Agent is to ensure all electronic devices are returned to ICE as expeditiously as possible.

8.5. Retention, Sharing, Safeguarding, And Destruction.

1) By ICE

a) Seizure and Retention with Probable Cause. When Special Agents determine there is probable cause of unlawful activity—based on a review of information in electronic devices or on other facts and circumstances—they may seize and retain the electronic device or copies of information therefrom, or relevant portions thereof, as authorized by law.

b) Retention of Information in ICE Systems. To the extent authorized by law, ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained. For example, information entered into TECS during the course of an investigation will be retained consistent with the policies governing TECS.

c) Sharing. Copies of information from electronic devices, or portions thereof, which are retained in accordance with this section, may be shared by ICE with Federal, state, local, and foreign law enforcement agencies in accordance with applicable law and policy. Sharing must be in compliance with the Privacy Act and applicable ICE privacy policies, such as the ICE Search, Arrest, and Seizure System of Records Notice.

d) Safeguarding Data During Storage and Transmission. ICE will appropriately safeguard information detained, copied, retained, or seized under this directive while in ICE custody and during transmission to an outside entity. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking originals and copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic data or physical protections (e.g., locked containers). Any suspected loss or compromise of information that contains personal data detained, copied, or seized under this directive must be reported immediately to the ICE Service Desk.

e) Destruction. Copies of information from electronic devices, or portions thereof, determined to be of no relevance to ICE will be destroyed in accordance with ICE policy governing the particular form of information. Such destruction must be accomplished by the responsible Special Agent within seven business days after conclusion of the border search unless circumstances require additional time, which must be approved by a supervisor and documented in appropriate ICE systems. All destructions must be accomplished no later than 21 calendar days after conclusion of the border search.

2) By Assisting Agencies

a) Retention during Assistance. All electronic devices, whether originals or copies of information therefrom, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to ICE.

b) Return or Destruction. At the conclusion of the requested assistance, all electronic devices and data must be returned to ICE as expeditiously as possible. In the alternative, the assisting Federal agency may certify to ICE that any copies in its possession have been destroyed or it may advise ICE in accordance with Section 8.5(2)(c). In the event that any original electronic devices were transmitted, they must not be destroyed; they are to be returned to ICE.

c) Retention with Independent Authority. Copies may be retained by an assisting Federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information is of national security or intelligence value. In such cases, the retaining agency must advise ICE of its decision to retain certain information on its own authority. In the event that any original electronic devices were transmitted, the assisting Federal agency may make a copy of information therefrom for its retention; however, any originals must be returned to ICE.

3) By Non-Federal Entities

a) ICE may provide copies of information from electronic devices to an assisting non-Federal entity, such as a private language translation or data decryption service, only for the period of time needed by that entity to render the requested assistance.

b) Upon the completion of assistance, all copies of the information in the possession of the entity must be returned to ICE as expeditiously as possible. Any latent copies of the electronic data on the systems of the non-Federal entity must also be destroyed so that recovery of the data is impractical.

8.6. Review, Handling, and Sharing of Certain Types of Information.

1) Border Search. All electronic devices crossing U.S. borders are subject to border search; a claim of privilege or personal information does not prevent the search of a traveler's information at the border. However, the nature of certain types of information are subject to special handling by Special Agents, whether through policy or laws such as the Privacy Act and the Trade Secrets Act.

2) Types of Information

a) Business or Commercial Information. If, in the course of a border search, Special Agents encounter business or commercial information, such information is to be treated as business confidential information. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may specifically govern or restrict handling of the information, including criminal penalties for unauthorized disclosure.

b) Legal Information. Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.

c) Other Sensitive Information. Other possibly sensitive information, such as medical records and work-related information carried by journalists shall be handled in accordance with all applicable federal law and ICE policy. Although there is no Federal legal privilege pertaining to the doctor-patient relationship, the inherent nature of medical information warrants special care for such records. Questions regarding the review of these materials shall be directed to the ICE Office of the Chief Counsel and this consultation shall be noted in appropriate ICE systems.

3) Sharing. Information that is determined to be protected by law as privileged or sensitive is to be handled consistent with the laws and policies governing such information.

8.7 Measurement. ICE Headquarters will develop appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from ICE systems using data elements entered by Special Agents pursuant to this Directive.

8.8 **Audit**. ICE Headquarters will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

9. **ATTACHMENTS.** None.

10. **NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees; or any other person.

Approved 

John Morton
Assistant Secretary
U.S. Immigration and Customs Enforcement

EXHIBIT 22

Privacy Impact Assessment Update for

CBP Border Searches of Electronic Devices

DHS/CBP/PIA-008(a)

January 4, 2018

Contact Point
John Wagner
Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-1610

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

CBP's border authorities permit the inspection, examination, and search of vehicles, persons, baggage, and merchandise to ensure compliance with any law or regulation enforced or administered by CBP. All travelers entering the United States are required to undergo customs and immigration inspection to ensure they are legally eligible to enter and that their belongings are not being introduced contrary to law. CBP's authorities to conduct searches of travelers and their merchandise entering or leaving the United States will be referred to in this PIA as "border search authority." CBP may search electronic devices, as with any other belongings, pursuant to border search authority.

CBP's border search authority applies at the physical border, the functional equivalent of the border (for example, international airports in the interior), or the extended border, as those terms are defined under applicable law. The border search authority applies to both inbound and outbound travelers and merchandise, including electronic devices.

If Selected for a Search of Your Electronic Device

CBP searches only a fraction of international travelers' electronic devices.[7] Travelers arriving at a port of entry must present themselves and their effects for inspection. During the border inspection, a CBP Officer checks the traveler's documentation and reviews relevant information (including relevant law enforcement information and "lookouts"[8]). The Officer may verbally request additional information from the traveler and may perform a basic search (defined further below) of the traveler's electronic device with or without suspicion. If the CBP Officer determines that the traveler warrants further examination, he or she will refer the traveler for additional scrutiny, known as "secondary inspection," which may include a basic or advanced search of the traveler's electronic devices. CBP documents relevant information regarding border inspections, including inspections of both basic and advanced searches, in its primary law enforcement system, TECS.[9]

CBP Officers document searches of electronic devices in the "Electronic Media Report" module of TECS, which provides information on why the traveler was selected for an examination. Furthermore, at every stage after the traveler is referred to "secondary inspection," CBP maintains records of the examination, detention, retention, or seizure of a traveler's property, including any electronic devices. Additionally, signage is posted throughout the port areas informing travelers

[7] In FY17, CBP conducted 30,200 border searches, both inbound and outbound, of electronic devices. CBP searched the electronic devices of more than 29,200 arriving international travelers, affecting 0.007 percent of the approximately 397 million travelers arriving to the United States. Of the more than 390 million arriving international travelers that CBP processed in FY16, 0.005 percent of such travelers (more than 18,400) had their electronic devices searched.

[8] As part of processing individuals at the border, DHS/CBP conducts pre-arrival or pre-departure TECS queries, which include checks against lookouts, such as "wants and warrants," watchlist matches, etc.

[9] For a complete overview of TECS, its functions, and the associated privacy risks, *see* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (December 22, 2010) and DHS/CBP/PIA-021 TECS System: Platform (August 2016), *available at* www.dhs.gov/privacy.

within one year of publication of this PIA. The Privacy Evaluation will be shared with the DHS Privacy Office.

If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may detain the device pending a determination as to its admissibility, exclusion, or other disposition.

2. Storage of Information Extracted from an Electronic Device in the Automated Targeting System

The 2009 Directive provided for the retention of information relating 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. Since that time, CBP published a Privacy Impact Assessment Update regarding CBP's use of the Automated Targeting System (ATS)[24] to store information copied and stored from a traveler's electronic device. To further CBP's border security mission, CBP may use ATS to further review, analyze, and assess the information physically resident on the electronic devices, or copies thereof, that CBP collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns. CBP may retain information from the physical device and the report containing the analytical results, which are relevant to immigration, customs, and/or other enforcement matters, in the ATS-Targeting Framework (TF) for purposes of CBP's border security mission, including identifying individuals who and cargo that need additional scrutiny. CBP may use ATS-TF to vet the information collected from the electronic devices of individuals of concern against CBP holdings and create a report which includes data that may be linked to illicit activity or actors. Information from electronic devices uploaded into ATS will be normalized[25] and flagged as originating from an electronic device.

Section 5.5.1.2 of the 2018 CBP directive, *Border Searches of Electronic Devices*, provides for retention of information in CBP Privacy Act-Compliant Systems and states that without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and/or 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.

ATS may be used to conduct an analytic review of the information and will transfer results of that review to ATS-TF. ATS-TF may retain the analytic review, which includes the information that may be linked to illicit activity or illicit actors and the underlying information relating to immigration, customs, and/or other enforcement matters for the purposes of ensuring compliance with laws CBP is authorized to enforce and to further CBP's border security mission,

[24] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.
[25] Normalization is the process of organizing data in a database to reduce redundancy and ensure that related items are stored together.

detention and search. CBP has created a tear-sheet[27] to provide travelers who have questions or concerns regarding the search of their electronic device. CBP has also published its previous, and newly updated, policies regarding border searches of electronic devices, and is publishing this PIA in tandem. CBP has also posted information on its website regarding the issue of border searches of electronic devices.[28]

In addition, at the time of the search, as a matter of policy, CBP will notify the individual subject to search of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. If the Officer or other appropriate CBP official determines that the fact of conducting this search cannot be disclosed to the individual transporting the device without impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld.[29]

As in 2009, CBP may retain information obtained from searches of electronic devices in a Privacy Act compliance system of records, consistent with the purpose of the collection. CBP has provided additional notice to the public by publishing system of records notices regarding these collections. Some of the SORNs that may be applicable to information obtained from a border search of electronic devices are:

- DHS/CBP-006 Automated Targeting System[30] covers information that is extracted from an advanced search of a device and stored in the ATS-Targeting Framework.
- DHS/CBP-011 U.S. Customs and Border Protection TECS[31] covers among other things, any records of any inspections conducted at the border by CBP, including inspections of electronic devices, including factors on the initiation of the search as described in the TECS Electronic Media Report module.
- DHS/CBP-013 Seized Assets and Case Tracking System (SEACATS)[32] provides notice regarding any seizures, fines, penalties, or forfeitures associated with the seizure of electronic devices.

These SORNs provide overall notice and descriptions of how CBP functions in these circumstances, the categories of individuals, the types of records maintained, the purposes of the examinations, detentions, and seizures, and the reasons for sharing such information. Any third party information that is retained from an electronic device and maintained in a CBP system of records will be secured and protected in the same manner as all other information in that system.

---

[27] *See* https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf.
[28] *See* CBP Search Authority, *available at* https://www.cbp.gov/travel/cbp-search-authority.
[29] CBP Directive at 5.4.1.3.
[30] DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297.
[31] DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.
[32] DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008, 73 FR 77764.

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel.[39] Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign.[40]

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, such as electronic devices.[41] These authorities support CBP's enforcement and administration of federal law at the border and facilitate the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department.[42]

Because CBP enforces federal law at the border, information may be detained or retained from a traveler's electronic device for a wide variety of purposes. CBP may use data contained on electronic devices to make admissibility determinations or to identify evidence of violations of law, including importing obscene material, drug smuggling, other customs violations, or terrorism, among others. The information may be shared with other agencies that are charged with the enforcement of a law or rule if the information is evidence of a violation of such law or rule. In appropriate circumstances, CBP may also convey electronic device or information obtained from the device with third parties for the purpose of obtaining technical assistance to render a device or its contents in a condition that allows for inspection. Consistent with applicable laws and SORNs, information lawfully obtained by CBP may be shared with other state, local, federal, and foreign law enforcement agencies in furtherance of enforcement of their laws.

Privacy Risk: There is no privacy risk to purpose specification. The legal precedent is clear, and all information is maintained, stored, and disseminated consistent with published systems of records notices.

Ezeiruaku, 936 F.2d 136, 143 (3d Cir. 1991) *United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983).

[39] *See Flores-Montano*, 541 U.S. at 154 (noting that "the expectation of privacy is less at the border than it is in the interior").

[40] *See Boumelhem*, 339 F.3d at 423.

[41] *See, e.g.*, 8 U.S.C. §§ 1225; 1357; 19 U.S.C. §§ 482; 507; 1461; 1496; 1581; 1582; 1589a; 1595a; *see also* 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer.").

[42] This includes, among other things, the responsibility 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 the illegal entry of terrorists, terrorist weapons, persons, and contraband;" and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons." 6 U.S.C. § 211.

EXHIBIT 23

Privacy Impact Assessment Update
for the
Automated Targeting System

DHS/CBP/PIA-006(e)

January 13, 2017

Contact Point
Mario Medina
National Targeting Center
U.S. Customs and Border Protection
(202) 325-1251

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS). ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. CBP is updating this Privacy Impact Assessment (PIA) to notify the public about ATS user interface enhancements for passenger vetting (known as Unified Passenger or UPAX), the use of ATS for vetting new populations, vetting of master crew member list and master non-crew member list data collected under 19 CFR. 122.49c, and several new information sharing initiatives, including between the Transportation Security Administration (TSA) and CBP to enhance the identification of possible threats and to assist in securing the border and transportation security.

Overview

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS) to facilitate legitimate trade and travel while managing the shared threat to the homeland posed by individuals and cargo that may require additional scrutiny prior to entering or exiting the United States. ATS supports CBP in identifying individuals and cargo that may require additional scrutiny across various transportation networks using the following functionalities:[1]

- Comparison: ATS compares information about travelers and conveyances arriving in, transiting through, or exiting the country against law enforcement and intelligence databases. For example, ATS compares information about individuals (identified as passengers, travelers, crewmembers, or persons appearing on documents supporting the movement of cargo) against the Terrorist Screening Database (TSDB)[2] as well as data concerning outstanding wants and warrants.
- Rules: ATS compares existing information about individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP Officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence.
- Federated Query: ATS allows users to search data across many different databases and systems to provide a consolidated view of data about a person or entity.

[1] For a complete overview of ATS, its modules, and the associated privacy risks, see DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update (June 1, 2012), *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update.

[2] ATS ingests the TSDB via the DHS Watchlisting Service (WLS). Please see DHS/ALL/PIA-027 Watchlist Service and subsequent updates for a full description of WLS, *available at* https://www.dhs.gov/publication/dhs-all-pia-027c-watchlist-service-update.

In order to execute the above three functionalities, ATS uses data from many different source systems. In some instances ATS is the official record for the information, while in other instances ATS ingests and maintains the information as a copy or provides a pointer to the information in the underlying system. Below is a summary; see Appendix A for referenced SORN citations.

- Official Record: ATS maintains the official record for Passenger Name Records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d; for Importer Security Filing (10+2 documentation) and express consignment manifest information, which provides advanced information about cargo and related persons and entities for risk assessment and targeting purposes; for results of Cargo Enforcement Exams; for the combination of license plate, Department of Motor Vehicle (DMV) registration data, and biographical data associated with a border crossing; for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information; and for certain information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department.
- Ingestion of Data: ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems, including, but not limited to: CBP's Automated Commercial Environment (ACE), Automated Commercial System (ACS), Overstay Leads from Arrival and Departure Information System (ADIS), Automated Export System (AES), Advance Passenger Information System (APIS), Border Crossing Information (BCI), Electronic System for Travel Authorization (ESTA), Electronic Visa Update System (EVUS), Global Enrollment System (GES), I-94 data, Non-Immigrant Information System (NIIS), Seized Asset and Case Tracking System (SEACATS), and TECS; the U.S. Citizenship and Immigration Services' (USCIS) Central Index System (CIS) data received through TECS, and special protected classes[3] data; the U.S. Immigration and Customs Enforcement's (ICE) Student Exchange and Visitor Information System (SEVIS) and Enforcement Integrated Database (EID), which includes Criminal Arrest Records and Immigration Enforcement Records (CARIER); Secure Flight Passenger Data (SFPD) and Master Crew List/Master Non-Crew List data from Transportation Security Administration (TSA); the Department of Justice's (DOJ) National Crime Information Center (NCIC) and Federal Bureau of Investigation (FBI) Interstate Identification Index (III) hits for manifested travelers; Electronic Questionnaires for Investigations Processing (e-QIP); historical National Security Entry-Exit Registration System (NSEERS); Flight Schedules and Flight Status OAG data; Social Security Administration (SSA) Death Master File; TSDB (Terrorist

[3] Special protected classes of individuals include nonimmigrant status for victims of human trafficking, nonimmigrant status for victims of crimes, and relief for domestic violence victims.

Screening Database), which ATS ingests from the WLS (Watchlist Service); and Non-immigrant and Immigrant Visa data from Department of State (DOS) Consular Consolidated Database (CCD), Refused Visa data from CCD, and the Consular Electronic Application Center (CEAC).

- Pointer System: ATS accesses and uses additional databases without ingesting the data, including: CBP's ADIS, Border Patrol Enforcement Tracking System (BPETS), Enterprise Geospatial Information Services (eGIS), e3 Biometrics System, and U.S. and Non-U.S. Passport Service through TECS; ICE's Enforcement Integrated Database (EID); DHS Automated Biometric Identification System (IDENT); USCIS's Person Centric Query System (PCQS); DOS CCD; commercial data aggregators; Nlets (not an acronym), DOJ's NCIC and the results of queries in the FBI's III; Interpol; the National Insurance Crime Bureau's (NICB's) private database of stolen vehicles.
- Data Manually Processed: ATS is used to manually process certain datasets to identify national security and public safety concerns and correlate records. Currently, DHS conducts this process for those records in ADIS that have been identified as individuals who may have overstayed their permitted time in the United States.

Reason for the PIA Update

ATS support for CBP's mission is directed into five general areas: 1) export of cargo; 2) import of cargo; 3) land borders; 4) air/sea borders; and 5) cross cutting view of risks across the four previous areas. To support these mission areas, ATS is divided into sub-systems or modules to support CBP Officers in determining whether or not a particular individual or cargo is higher risk than other individuals or cargo. Each sub-system uses slightly different data to conduct its risk assessment, but the basic purposes as described above remain the same. Previously issued PIAs for ATS discuss each module in detail and continue to apply unless otherwise specified in this document.[4]

Previously issued PIAs for ATS also discuss the scope of the targeting rules used by ATS. This process has not changed.[5] ATS continues to build risk-based assessments for cargo and conveyances based on criteria and rules developed by CBP. ATS maintains the assessment results from rules together with a record of which rules were used to develop the assessment results. With regard to travelers, ATS identifies persons whose information matches criteria comprising a targeting rule. This initial match and any subsequent matches are reviewed by CBP Officers to confirm continued official interest in the identified person. It is worth clarifying, however, that only the ATS components pertaining to cargo or conveyances rely on rules-based targeting to build

[4] For a complete overview of ATS, its modules, and the associated privacy risks, see https://www.dhs.gov/publication/automated-targeting-system-ats-update.
[5] For a complete assessment of the rules process and procedures within ATS, please see the 2012 PIA for ATS: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update (June 1, 2012), *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update.

a score for the cargo or conveyance to subsequently identify cargo or conveyances of interest. Persons associated with cargo shipments are screened against TECS lookouts and prior law enforcement actions to permit any identified violations to be considered as part of the overall score. Travelers identified by risk-based targeting scenarios are not assigned scores.

ATS rules and assessment results from rules are designed to signal to CBP Officers that further inspection of a person, shipment, or conveyance may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise be noted as a person of concern to law enforcement. ATS-Targeting Framework (TF) is a workflow and reporting function that separately allows users to track assessment results from rules and create various reports permitting a more comprehensive analysis of CBP's enforcement efforts.

ATS risk assessments are always based on predicated and contextual information. As noted above, unlike in the cargo and conveyance environments, ATS traveler risk assessments do not use a score to determine an individual's risk level; instead, they compare personally identifiable information (PII) from the databases listed above against lookouts and patterns of suspicious activity identified through past investigations and intelligence. This analysis is done in advance of a traveler's arrival in or departure from the United States and becomes one tool available to DHS officers in identifying illegal activity.

ATS modules support CBP's mission with the functionality summarized below, and described in more detail in previously published PIAs.

- Export Data: ATS evaluates export information, which includes information filed electronically with CBP. The export data is sorted, compared to rules, and scored so that CBP Officers can identify exports with transportation safety and security risks, such as Office of Foreign Assets Control (OFAC) violations, smuggled currency, illegal narcotics, and other contraband. ATS screens both commodity information on export documents and individuals identified on those documents. Officers can input findings from outbound exams of exports, generate multiple reports, and internally track shipments through custom rule criteria, review marking, and watched entity list.
- Inbound Cargo Screening: ATS evaluates all cargo to identify high risk inbound cargo for examinations. ATS uses rule and weight sets to analyze information from manifest, importer security filing, and entry data, to prioritize shipments for review and generate targets by scoring each shipment. In some places, ATS automatically places shipments on hold when they score above a specified risk threshold. ATS screens commodity information on the manifest, importer security filing, and entry data, and also screens individuals identified on these data sources against lookouts and prior violations.
- Vehicle and Traveler Targeting: ATS evaluates historical crossing records against internal and external data sources for targeting of vehicles and individuals at the border, as well as for the identification of potential terrorists, transnational criminals, and in some cases, other persons who pose a higher risk of violating U.S. law. ATS is used within CBP by Passenger

ATS PIA Update Addendum 1:

Automated Targeting System-Passenger (ATS-P) – Module Updates

Last updated January 13, 2017 *(back to top)*

Automated Targeting System-Passenger (ATS-P) is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals, and, in some cases, other persons who pose a higher risk of violating U.S. law. ATS-P capabilities are used at ports of entry to augment the CBP Officer's decision-making about whether a passenger or crew member should receive additional scrutiny.

ATS-P is also used within CBP by Passenger Analytical Units (PAU) at ports of entry, the National Targeting Center (NTC), Border Patrol Agents, CBP headquarters intelligence analysts, and within DHS by DHS agents, analysts, and officers in the Office of Intelligence and Analysis (I&A), ICE, U.S. Coast Guard, and TSA. ATS-P provides a hierarchical system that allows DHS personnel to focus efforts on potentially high-risk passengers by eliminating labor-intensive manual reviews of traveler information or interviews with every traveler. The assessment process is based on a set of uniform and user-defined rules based on specific operational, tactical, intelligence, or local enforcement efforts.

ATS-P is used to augment visa overstay leads received from Arrival and Departure Information Systems (ADIS) based on supporting data available in ATS (e.g., border crossing information, I-94 information, and Student and Exchange Visitor Information System (SEVIS) information). In addition to augmenting the list of overstay leads, ATS also develops priorities based on associated risk patterns. This prioritized list of overstay leads is then passed on to the LeadTrac case management system[6] for ICE to generate case leads.

By logging into ATS-P, authorized CBP and DHS personnel can access information from the various source systems on passengers who have arrived in and/or departed from the United States. ATS-P allows users to query other available Federal Government systems as well as publicly available information on the Internet through the user interface. In addition, ATS-P maintains a copy of information from the following systems: Advance Passenger Information System (APIS), I-94, Non-Immigrant Information System (NIIS), Electronic System for Travel Authorization (ESTA), Border Crossing Information (BCI), TECS secondary processing, and seizure and enforcement data, as well as Suspect and Violator Indices (SAVI), Central Index System (CIS), Electronic Visa Update System (EVUS), Global Enrollment Systems (GES), Terrorist Screening Database (TSDB) via the Watchlist Service, and the Department of State's (DOS) Consular Consolidated Database (CCD) Visa and Consular Electronic Application Center

[6] *See* DHS/ICE/PIA-044 LeadTrac System (July 22, 2016), *available at* https://www.dhs.gov/publication/dhsicepia-044-leadtrac-system.

or other operational considerations that make it inappropriate to permit the individual to remain present.

Section 5.4.1.2 of the CBP directive, *Border Search of Electronic Devices Containing Information*, provides for retention of information in CBP Privacy Act-Compliant Systems and states that without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and/or 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. CBP's collection of information from electronic devices is discussed in detail in other privacy compliance documentation.[46] Searches of electronic devices will be documented.

To further CBP's border security mission, CBP may use ATS to further review, analyze, and assess the information physically resident on the electronic devices, or copies thereof, that CBP collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns. CBP may retain information from the physical device and the report containing the analytical results, which are relevant to immigration, customs, and/or other enforcement matters, in ATS-TF for purposes of CBP's border security mission, including identifying individuals who and cargo that need additional scrutiny. CBP may use ATS-TF to vet the information collected from the electronic devices of individuals of concern against CBP holdings and create a report which includes data that may be linked to illicit activity or actors. Information from electronic devices uploaded into ATS will be normalized[47] and flagged as originating from an electronic device.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

CBP's authorities to search and retain information obtained from travelers, including from electronic devices, derives from the following: 8 U.S.C. § 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1595a; 31 U.S.C. § 5317; 22 U.S.C. § 401.

[46] *See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* https://www.dhs.gov/topic/privacy.

[47] Normalization is the process of organizing data in a database to reduce redundancy and ensure that related items are stored together.

CBP retains copies of information from electronic devices and the report containing the analytical results in ATS, only when it relates to customs, immigration, or other enforcement matters, in accordance with the CBP directive, *Border Search of Electronic Devices Containing Information*, and the National Archives and Records Administration (NARA) approved retention schedule as reflected in the Automated Targeting System (ATS) System of Records Notice.[48]

Characterization of the Information

CBP conducts searches of electronic devices at the border, both inbound and outbound, to ensure compliance with customs, immigration, and other laws enforced by CBP. These searches are part of CBP's long-standing practice and are essential to enforcing the law at the U.S. border, and to protecting border security, including to assist in detecting evidence relating to terrorism and other national security matters, narcotics, human and bulk cash smuggling, and export violations, and are often integral to a determination of admissibility under the immigration laws. CBP only copies information from electronic devices and retains that information in ATS relating to customs, immigration, or other enforcement matters, including for example, terrorism or narcotics.

Privacy Risk: There are privacy risks associated with the volume and breadth of information from electronic devices stored in ATS.

Mitigation: This risk is partially mitigated. CBP may use ATS to further review, analyze, and assess electronic information collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns, consistent with CBP's border security mission. In addition, CBP follows all of the reporting, handling, and other requirements in the CBP Directive, *Border Search of Electronic Devices Containing Information*, including the requirements outlined in the review and handling of privileged or other sensitive material section.

Privacy Risk: There is a risk that information from electronic devices in ATS is inaccurate.

Mitigation: This risk is not mitigated. CBP is obtaining this information directly from the electronic device, but it remains possible that data on the device may not be accurate. CBP will use this information to match against CBP holdings and will take action on information obtained from an electronic device if, based on information available to CBP, the information is assessed to be accurate and reliable. The information will be used to facilitate additional lines of inquiries, to corroborate existing information, and to identify those travelers and cargo that needs additional scrutiny.

Uses of the Information

ATS may be used to conduct an analytic review of the information and will transfer results of that review to ATS-TF. ATS-TF may retain the analytic review, which includes the information that may be linked to illicit activity or illicit actors and the underlying information relating to immigration, customs, and/or other enforcement matters for the purposes of ensuring compliance

[48] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).

electronic devices. Because CBP does not provide specific notice at the time of collection, however, some risk remains. This is a similar risk posed by other law enforcement information collections, since the nature of law enforcement activities and operations does not always enable specific, on-time notice.

Data Retention by the project

The information in ATS will be retained consistent with the established NARA schedule, as reflected in the ATS SORN. The retention period for the official records maintained in ATS will not exceed 15 years, after which time the records will be deleted, except information maintained only in ATS that is "linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related."

Privacy Risk: There is a risk CBP will retain in ATS sensitive information obtained from electronic devices that is unrelated to any law enforcement matter.

Mitigation: This risk is partially mitigated. CBP conducts its activities involving the border search of electronic devices containing information consistent with the CBP Directive, *Border Search of Electronic Devices Containing Information.* Pursuant to the CBP Directive, without probable cause to seize an electronic device or copy of information contained therein, CBP may retain only information relating to immigration, customs, and/or 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. Consistent with the CBP Directive and the ATS SORN, CBP may use ATS to further review, analyze, and assess the copy of the electronic information collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns. CBP may retain the information from the electronic device and the report containing the analytical results, which are relevant to immigration, customs, and/or other enforcement matters, in ATS for CBP's border security mission, including identifying individuals and cargo needing additional scrutiny.

Information Sharing

Absent any legal prohibitions, CBP may share information from ATS with other DHS Component personnel who have an authorized purpose for accessing the information in performance of their duties, possess the requisite security clearance, and assure adequate safeguarding and protection of the information. In addition, CBP may share information with external agencies consistent with the routine uses published in the ATS SORN.[49] Specifically, CBP may share information from ATS:

[49] For a complete list of routine uses, *see* DHS/CBP-006 Automated Targeting System, System of Records, 77 FR 30297 (May 22, 2012).

EXHIBIT 24

From: Edney, Marsha (CIV)
To: Hugh Handeyside; Drezner, Michael L. (CIV); Balakrishna, Annapurna (USAMA)
Cc: Esha Bhandari; Nathan Wessler; Adam Schwartz; Sophia Cope; Aaron Mackey; Jessie Rossman
Subject: RE: Alasaad v. Nielsen: update re allegation of breach of privilege
Date: Thursday, September 20, 2018 5:43:56 PM

Counsel –

I am writing to update you on what I have learned about the search of Ms. Merchant's phone on September 9 in the Toronto airport pre-clearance area. As I previously indicated, an attorney not involved with the *Alasaad* litigation was tasked to determine whether attorney-client information was reviewed and/or retained by CBP in connection to the inspection of Ms. Merchant's cell phone. That attorney has completed his review, and as a result, we can confirm that CBP conducted a basic search of Ms. Merchant's cell phone (as that term is used in CBP's Guidance). During the secondary inspection, no information from the phone was copied nor were any notes taken regarding the contents of the phone. Ms. Merchant's cell phone was never taken from her line of sight, and the actual search of the phone lasted approximately 10 minutes. The records documenting the inspection of the phone were also reviewed by the attorney, and none of those records referred to any content on Ms. Merchant's phone. Additionally, both customs officers involved in the inspection confirmed that they have no recollection of reviewing any emails or texts that contain information about a lawsuit. A reminder has been provided to the appropriate management in Toronto regarding the applicable agency policies and protocols to follow if the attorney client or attorney work product privileges are asserted during an inspection.

Given that no potentially privileged information was included in CBP records, we do not believe any further steps are necessary and we plan to advise the attorneys working on the *Alasaad* litigation that they can resume normal practices.

Marsha Stelson Edney
Senior Trial Counsel
202-514-4520

From: Hugh Handeyside [mailto:hhandeyside@aclu.org]
Sent: Thursday, September 13, 2018 10:50 AM
To: Edney, Marsha (CIV) <MEdney@CIV.USDOJ.GOV>; Drezner, Michael L. (CIV) <midrezne@CIV.USDOJ.GOV>; Balakrishna, Annapurna (USAMA) <Annapurna.Balakrishna@usdoj.gov>
Cc: Esha Bhandari <ebhandari@aclu.org>; Nathan Wessler <nwessler@aclu.org>; Adam Schwartz <adam@eff.org>; Sophia Cope <sophia@eff.org>; Aaron Mackey <amackey@eff.org>; Jessie Rossman <JRossman@aclum.org>
Subject: Re: Alasaad v. Nielsen: Letter re breach of privilege

Marsha,

Thank you for your update. We will await further information about the government's investigation and remedial measures.

From: Edney, Marsha (CIV)
To: Nathan Wessler; Drezner, Michael L. (CIV)
Cc: Michael Rosenbloom (michael.rosenbloom@eff.org); Esha Bhandari; Hugh Handeyside; Adam Schwartz (adam@eff.org); Sophia Cope; Jessie Rossman; Balakrishna, Annapurna (USAMA)
Subject: RE: Alasaad: Conferring re 30(b)(6) depositions
Date: Wednesday, November 21, 2018 11:55:46 AM
Attachments: 909.pdf

Counsel --

Thanks for your email re the 30(b)(6) depositions – we were also starting to think about noticing the individual plaintiffs' depositions and it may make sense for us to have a call after the holiday weekend to discuss timing and location for those depositions.

As for the 30(b)(6) depositions, we are still waiting for the agencies to get back to us with the schedules of the possible deponents and that will not happen until next week sometime. I can tell you that there is no way for us to prepare such high level witnesses on all the proposed topics for an early December deposition. I see you mentioned extending the discovery deadline and I was wondering if that was in order to give the parties more time to complete these depositions? Given the holiday season it does seem likely to us that depositions will need to bleed beyond the Dec 30 cut-off date.

We also wanted to mention that we should discuss the topics you have listed for the 30(b)(6) as they seem duplicative of both the written discovery and the stipulations the parties have agreed upon and we wonder if plaintiffs would consider narrowing the topics. Additionally, as you can imagine there will likely be some objections to the deposition questions based on the law enforcement sensitive nature of the information and it may be helpful for us to agree how the parties will handle those privileges at the depositions.

As for your question regarding the initial disclosures, we did not designate witnesses as fact witnesses given the narrow focus of the current discovery i.e, not going into facts of past searches; rather we listed these individuals because they have knowledge of the agency's operations and policies and expect that they could be 30(b)(6) witnesses if necessary.

Also just want to let you know that we intend to get you responses to your new RFPS 18 and 19 as well as Interrogatories 10 and 11 by Nov. 30th. We should also have the draft stipulation regarding the redacted narrative information on or before then.

Finally, attached to this email is a document that we previously withheld in full, marked as Privilege ID No. 4, now Bates 909, and are now providing to you with redactions. The document is a log of items received by a law enforcement laboratory, and includes a notation of receipt of thumb drives relating to the inspection of Plaintiff Wright's electronic devices. The remaining redactions are applied for the same reasons previously identified on our privilege log as the basis for withholding the document in full.

Have a nice Thanksgiving!

EXHIBIT 25

U.S. Customs and Border Protection
U.S. Department of Homeland Security
(b) 7(E)

(b) 7(E) Generated By: (b) (6) Page 1 of 3

REPORT NUMBER: 20163307172451 REPORT STATUS: CLOSED

Summary Information		
Reason For Search		Port Code
(b) 7(E)		3307-DENVER
Incident Date		NTC#
04/21/2016		
Last Name	First Name	Middle Initial
WRIGHT	MATTHEW	
Date of birth	Gender	Race
[redacted]	M - Male	W - WHITE
Country Of Birth		Nationality
USA - UNITED STATES		USA - UNITED STATES
I/O		Notified Of Search
I - Inbound		Y - Yes
Tear Sheet Provided		
Yes		
Officer/Agent		
(b)(6) (b)(7)(C) [CBP OFFICER]		
Supervisor		
(b) (6)		

Item 01 Details			
Item Type		Make	Model
CEL-CELLPHONE/ALL COMM DEVICES		APPLE	IPHONE A 1549
ID1		Number	
I-International Mobile Station Equipment Identity (IMEI) Number		[redacted]	
ID2		Number	
Inspection Start Date	Time	Inspection End Date	Time
04/21/2016	13:11		

Actions			
Action	Date	Action Status	Additional Information
Manual Examination and Returned to Traveler	06/14/2016	N/A	Passenger Consented: N
Detained - TOT HSI	04/21/2016	Approved	6051D#: 0154762,HSI Agent Name: (b) (6)
Detained - at CBP	04/21/2016	Canceled	6051D#: 0154762,Supervisor (b) (6)
Detained - TOT HSI	04/21/2016	Canceled	6051D#: 0154762,HSI Agent Name: (b) (6)
Detained - TOT HSI	04/21/2016	Canceled	6051D#: 0154762,HSI Agent Name: (b) (6)

U.S. Customs and Border Protection
U.S. Department of Homeland Security
(b) 7(E)

(b) (7)(E) Generated By: (b) (6) Page 2 of 3

REPORT NUMBER: 20163307172451 REPORT STATUS: CLOSED

Detained - TOT HSI	04/21/2016	Canceled	6051D#: 0154762,HSI Agent Name: (b) (6)
Detained - TOT HSI	05/19/2016	Canceled	6051D#: 0154762,HSI Agent Name: (b) (6)
Detained - TOT HSI	05/19/2016	Canceled	6051D#: 0154762,HSI Agent Name: (b) (6)
Detained - at CBP	05/19/2016	Canceled	6051D#: (b) (6)

Item 01 Details

Item Type		Make	Model
CMP-COMPUTER/LAPTOP		APPLE	MACBOOK PRO 81502
ID1		Number	
S-Serial Number		[redacted]	
ID2		Number	
Inspection Start Date	Time	Inspection End Date	Time
04/21/2016	13:11		

Actions

Action	Date	Action Status	Additional Information
Manual Examination and Returned to Traveler	06/14/2016	N/A	Passenger Consented: N
Detained - TOT HSI	04/21/2016	Approved	6051D#: 0154762,HSI Agent Name: (b) (6)
Detained - at CBP	04/21/2016	Canceled	6051D#: (b) (6)
Detained - TOT HSI	04/21/2016	Canceled	6051D#: 0154762,HSI Agent Name: (b) (6)
Detained - TOT HSI	05/19/2016	Canceled	6051D#: 0154762,HSI Agent Name: (b) (6)
Detained - at CBP	05/19/2016	Canceled	6051D#: (b) (6)

Item 01 Details

Item Type	Make	Model
DII-DIGITAL CAMERA/VIDEO CAMERA	GOPRO	HERO 3

U.S. Customs and Border Protection
U.S. Department of Homeland Security
(b) (7)(E)

(b) 7(E) Generated By: (b)(6) (b)(7)(C) Page 3 of 3

REPORT NUMBER: 20163307172451 REPORT STATUS: CLOSED

ID1		Number	
S-Serial Number		[redacted]	
ID2		Number	
Inspection Start Date	Time	Inspection End Date	Time
04/21/2016	13:11		

Actions

Action	Date	Action Status	Additional Information
Manual Examination and Returned to Traveler	06/14/2016	N/A	Passenger Consented: N
Detained - TOT HSI	04/21/2016	Approved	6051D#: 0154762,HSI Agent Name: (b)(6) (b)(7)(C)
Detained - at CBP	05/19/2016	Canceled	6051D#: (b)(6) (b)(7)(C)

REMARKS

LETICIA MARTINEZ 06/29/2016 00:09
All items were returned to subject WRIGHT via FEDEX #871760367935 and delivered on 06/16/2016. No derogatory information was discovered from the laboratory examination.

(b)(6) (b)(7)(C) 06/28/2016 15:25
Items detained from passenger WRIGHT, Mathew were returned by HSI on the week of 05/21/2016. Items consequently sent to San Francisco LAB for further examination after failure to extract information from electronics from by HSI. San Francisco LAB on the week of 06/05/2016 returned items after manual examination resulting in 3 thumb drives of information that were turned over to HSI. All items detained (CELL,CMP,DII) returned to passenger WRIGHT, Mathew via FEDEX on 06/14/2016.

(b)(6) (b)(7)(C) 05/19/2016 17:01
REFUSAL TO UNLOCK ELECTRONICS FOR FURTHER INSPECTION. LAPTOP, CELL PHONE AND GOPRO CAMERA DATAINED UNDER 6051D#0154762 FOR FURTHER EXAMINATION OF ELECTRONICS

(b)(6) (b)(7)(C) 05/19/2016 15:41
REFUSAL TO UNLOCK ELECTRONICS FOR FURTHER INSPECTION. LAPTOP, CELL PHONE AND GOPRO CAMERA DATAINED UNDER 6051D#0154762 FOR FURTHER EXAMINATION OF ELECTRONICS.

No. 0154762

U.S. CUSTOMS SERVICE

Detention Notice and Custody Receipt for Detained Property

Handbook 5200-09

1. Held for other agency? Yes ☒ No ☐ Name of Agency: HSI
2. Certified Mail No.
3. Investigative Case No.
4. General Order No.
5. Exodus Command Center Notified? ☐ Yes Date: ☐ No Time:
6. Port Code: 3307
7. Date of Detention (mm/dd/yyyy): 04/21/2016
8. Time (Use 24 Hours): 1311
9. Entry Number: CBP form 7662
10. Detained from:
11. Seal or Other ID No.: L1112009
12. Misc. Nos.

Name: MATTHEW, WRIGHT

Address: [redacted]

Telephone No.: [redacted]

Remarks: Electronics
Flight - UA#138
DOB - 04/15/1979 FIS 3307

14. FPF No. (For Customs Lab Use Only)

15. Point of Contact Information - Send all correspondence to: HSI DENVER

Telephone No. ( ) Fax No. ( )

16. Additional Information/Action Request from Importer/Exporter/Subject

17. Reason for Detention: Refusal to Unlock Electronics for inspection

18. Tests or Inquiries to be Conducted:

19. **PROPERTY** (By Line Item) Attach CF 58 if conveyance

a. Line Item No.	b. Description	c. Packages Number	c. Packages Type	d. Measurement Qty.	d. Measurement UM	e. Est. Dom. Value	f. Samples Sent to the Customs Lab Yes or No	f. Samples Sent to the Customs Lab Date
1	LAPTOP			1	EA	$	Yes ☐ No ☐	/ /
2	CELL PHONE			1	EA	$	Yes ☐ No ☐	/ /
3	GO PRO CAM			1	EA	$	Yes ☐ No ☐	/ /
						$	Yes ☐ No ☐	/ /

20. Detaining Officer Name

CBO [redacted] (b) (6)

Print Signature Date: 04/21/2016

21. **ACCEPTANCE/CHAIN OF CUSTODY**

a. Line Item No.	b. Description	c. Print Name/Title/Organization	d. Signature	e. Date
			20163307172451	

Shipments may be detained for up to 30 days, unless statutory authority or interagency agreement mandates that a longer period of time is required, or the importer/exporter/subject requests a longer detention period through the Port Director.

CF 6051A Continuation Sheet Attached? Yes ☐ No ☒

Customs Form 6051D (11/01)

Contacted subj on 5/19 to explain further Forensics

MW FOIA 011

PID0945

I was able to extract data off of the SIM card (not the phone, it's password protected) and the micro SD card of the GoPro. Who do you want me to send the data to for analysis?

(b) (6)

From: (b) (6)
Sent: Monday, June 06, 2016 9:09 AM
To: (b) (6) @cbp.dhs.gov>
Cc (b) (6) @CBP.DHS.GOV>; (b) (6) @cbp.dhs.gov>
Subject: RE: 6051D - 0154762: MacBook Laptop, iPhone and GoPro

(b) (6)

Please return the laptop to Denver as soon as possible. We will not authorize taking apart the laptop.

If you have any questions please contact me. Thank you.

(b) (6)

Customs and Border Protection

Assistant Port Director – Passenger Operations

Port of Denver

(b) (6)

From: (b) (6)
Sent: Monday, June 06, 2016 9:55 AM
To (b) (6) @CBP.DHS.GOV>
Subject: FW: 6051D - 0154762: MacBook Laptop, iPhone and GoPro

(b) (6)

Assistant Port Director – Trade

Public Affairs Liaison

EXHIBIT 26

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,	)	Civil Action No. 17-cv-11730-DJC
v.	)	Hon. Denise J. Casper
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.	)	

DEFENDANTS' OBJECTIONS AND RESPONSES TO
PLAINTIFFS' FIRST SET OF INTERROGATORIES TO ALL DEFENDANTS

Pursuant to Rules 26 and 33 of the Federal Rules of Civil Procedure and the Local Rules of the United States District Court for the District of Massachusetts, Defendants, by and through undersigned counsel submit their Objections and Responses to Plaintiffs' First Set of Interrogatories To All Defendants.

INTERROGATORIES

INTERROGATORY NO. 1

Identify and describe all of the government interests that are purportedly served by the Defendants' challenged policies and practices on border device searches and confiscations.

Defendants' Response: Defendants object to this interrogatory as vague and overly broad, as it seeks an identification and description of "all of the government interests" that are "purportedly served" by the challenged policies and practices. "Government interests" is not defined here, nor does it have any commonly accepted definition. Similarly, it is unclear what is meant for an interest to be "purportedly served" by a challenged policy or practice. In addition, the term "confiscations" is undefined and has no commonly accepted meaning in this context. Defendants further object to this interrogatory to the extent it calls for a legal conclusion and analysis of the government interests served by the border search exception to the probable cause and warrant requirements of the Fourth Amendment, as recognized in binding legal precedents. Subject to these objections, Defendants respond as follows:

As made clear in CBP Directive 3340-049A and ICE Directive 10044.1, border searches of electronic devices are conducted in furtherance of customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that Defendants are authorized to enforce and administer.

These searches are part of Defendants longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They are a crucial tool for detecting evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. They can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination

of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws.

Pursuant to Fed. R. Civ. P. 33(d), Defendants will also produce documents in response to this interrogatory. Subsequent to the production of those documents, Defendants will identify the Bates numbers which correspond to this response.

INTERROGATORY NO. 2

Identify and describe any and all facts or evidence that show that any of the government interests identified in response to Interrogatory No. 1 are actually served by the challenged policies and practices.

Defendants' Response: Defendants object to this interrogatory as vague and overly broad to the extent it references "any and all" facts or evidence that show that "any" government interests are served by the challenged policies and practices, and because the terms are undefined. Defendants further object to this interrogatory because the burden of providing such information is not proportional to the needs of the case. Read literally, this interrogatory could be interpreted to require information and production of records detailing each instance in which a border search of an electronic device supported DHS's mission to promote border security and to enforce the customs, immigration, and other laws that DHS is authorized to enforce or administer at the border. Defendants further object to this interrogatory to the extent it calls for a legal conclusion and analysis of the government interests served by the border search exception to the probable cause and warrant requirements of the Fourth Amendment, as recognized in binding legal precedents. Defendants further object to this Request to the extent it seeks information protected by the law enforcement privilege. Subject to these objections, Defendants respond as follows:

Pursuant to Fed. R. Civ. P. 33(d), Defendants will produce documents in response to this interrogatory. Subsequent to the production of those documents, Defendants will identify the Bates numbers which correspond to this response.

INTERROGATORY NO. 3

Identify and describe any and all facts or evidence that show the government interests identified in response to Interrogatory No. 1 could still be advanced if border officers 1) were

prevents," and accordingly it is unclear what information is sought by this interrogatory. Defendants further object insofar as this interrogatory suggests that Defendants are not permitted to detain or seize "digital contraband" unless they can guarantee that such items are not available on the Internet from other sources. Subject to these objections, Defendants respond as follows:

Any digital contraband found by Defendants during a border search is appropriately safeguarded pursuant to policies governing border searches, applicable system of records notices and/or chain of custody requirements for evidence preservation. Like any contraband discovered during a border search, the relevant law enforcement agency will retain and/or destroy the contraband as necessary, consistent with applicable laws and policies. Accordingly, by definition, the specific digital contraband discovered during a border search cannot be illicitly transmitted over the internet by a private individual once it has been retained and/or destroyed.

INTERROGATORY NO. 5

Identify and describe any and all facts or evidence that show that digital contraband enters or becomes available in the United States via the Internet or Internet-based communication or other forms of communication.

Defendants' Response: Defendants object to this interrogatory as vague and overly broad, to the extent it seeks "all facts or evidence" and further because it is unclear what is meant by digital contraband "entering" or "becom[ing] available" in the United States via the Internet. Defendants further object to this interrogatory as seeking facts outside of the defendant agencies' knowledge and such facts do not appear to be relevant to the claims and defenses in this case. Defendants further object to this interrogatory because the burden of providing such information is not proportional to the needs of the case. Read literally, this interrogatory would require production of evidence vastly disproportionate to the needs of this case, in violation of Fed. R. Civ. P. 26(b)(1).

Defendants generally use the term 'digital contraband' to refer to electronic information that it is unlawful to possess, to transport, to import into the United States, or to export from the United States.

Defendants further object insofar as this interrogatory suggests that Defendants are not permitted to detain or seize "digital contraband" unless they can guarantee that such items are not available on the Internet or from other sources. Subject to these objections, Defendants state as follows:

Defendants are aware that digital contraband may in certain circumstances be accessible from the United States via the internet.

INTERROGATORY NO. 6

For each of the fiscal years since FY 2012, provide 1) the number of device confiscations by U.S. Customs and Border Protection ("CBP"), 2) the number of basic searches of devices by CBP, 3) the number of advanced searches of devices by CBP, 4) the number of device confiscations by U.S. Immigration and Customs Enforcement.

Defendants' Response: Defendants object to this interrogatory's use of the terms "basic searches" and "advanced searches" to cover information that predates the establishment of definitions for those terms in CBP's January 2018 Directive. In addition, the term "confiscations" is undefined and has no commonly accepted meaning in this context. Prior to CBP's January 2018 Directive, Defendant CBP did not, as a matter of policy, categorize searches of electronic devices as "basic" or "advanced." Subject to these objections, Defendants respond as follows:

Based on available data from CBP records, CBP estimates that it detained the following number of electronic devices after a traveler departed the port of entry or other location of inspection, in each of the identified fiscal years:

- FY 2012 – 8
- FY 2013 – 36
- FY 2014 – 32
- FY 2015 – 21
- FY 2016 – 131

- FY 2017 – 200
- FY 2018 (through 9/15/2018) – 172

Based on available data from CBP records, CBP estimates that it conducted basic searches of electronic devices in the following number of incidents, in each of the identified fiscal years:

- FY 2012 – 3,182
- FY 2013 – 3,561
- FY 2014 – 4,314
- FY 2015 – 6,618
- FY 2016 – 16,914
- FY 2017 – 27,701
- FY 2018 (through 9/15/2018) – 28,429

Based on available data from CBP records, CBP estimates that it conducted advanced searches of electronic devices in the following number of incidents, in each of the identified fiscal years:

- FY 2012 – 2,285
- FY 2013 – 2,444
- FY 2014 – 1,921
- FY 2015 – 2,090
- FY 2016 – 2,394
- FY 2017 – 2,685
- FY 2018 (through 9/15/2018) – 3,485

ICE does not maintain statistics on "device confiscations," but only the number of searches, each of which may involve more than one device, and may not amount to a "confiscation" in any

event.

INTERROGATORY NO. 7

Identify and describe all the types of information about a traveler that a border officer may see or have access to at a port of entry, including at primary and secondary inspection, and including whether or not the traveler has previously been subject to a device search or confiscation.

Defendants' Response: Defendants object to this interrogatory as vague, overly broad, and disproportionate to the needs of the case to the extent it seeks "all" types of information and fails to define "types" of information or "have access to", and further objects to the term "confiscation" as that is not a term used by defendant agencies. In addition, the term "border officer" is not a term used by defendant agencies; therefore Defendants interpret the term to refer to an official employed by Defendants that conducts border searches of electronic devices pursuant to the Defendants' applicable policies. *See* CBP Directive 3340-049A and ICE Directive 10044. Defendants further object to this Request to the extent it seeks information protected by the law enforcement privilege. Subject to these objections, Defendants state as follows:

The type of information about a traveler that is available to the inspecting CBP officer may vary depending on the location and environment in which CBP encounters the traveler. For example, in the air and sea environment, CBP generally obtains certain information about individuals traveling to the U.S. on commercial or private aircraft, as well as commercial vessels, through CBP's Advance Passenger Information System (APIS). Unlike in the air/sea travel environment, CBP does not generally receive advance travel information regarding individuals traveling to the U.S. by foot (pedestrian) or by private vehicle prior to their arrival at a port of entry.

Upon arrival in the United States, individuals are generally required to present themselves to CBP at the port of entry's primary arrival location (known as primary). At primary, the CBP

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,	)	Civil Action No. 17-cv-11730-DJC
v.	)	Hon. Denise J. Casper
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.	)	

DEFENDANTS' OBJECTIONS AND RESPONSES TO
PLAINTIFFS' SECOND SET OF DISCOVERY

Pursuant to Rules 26, 33 and 34 of the Federal Rules of Civil Procedure and the Local Rules of the United States District Court for the District of Massachusetts, Defendants, by and through undersigned counsel submit their Objections and Responses to Plaintiffs' Second Set of Discovery.

INTERROGATORY NO. 10

Identify and describe any and all information or data retained by Defendants from the searches and confiscations of each of the Plaintiffs' electronic devices, including electronic data copied from Plaintiffs' electronic devices (such as copying by means of conducting an advanced search), and narrative descriptions of information or data observed or found during a search of Plaintiffs' electronic devices.

Defendants' Response:

Defendants object to this interrogatory as vague, overly broad and improper because it asks for "any and all information" and further because the term "confiscations" is undefined and has no commonly accepted meaning in this context. Defendants further object to this interrogatory insofar as it characterizes officer impressions and observations as constituting the retention of data from searches or detentions of Plaintiffs' electronic devices. Defendants further object to this interrogatory to the extent it seeks information protected by the law enforcement privilege, the deliberative process privilege, or other applicable privileges or protections from disclosures. Subject to the foregoing objections, Defendants respond as follows:

Pursuant to Fed. R. Civ. P. 33(d), with regard to narrative descriptions of information or data observed or found during a search of Plaintiffs' electronic devices, Defendants refer Plaintiffs to the following documents produced in discovery: Defs. 0098, 0102, 0105, 0106, 0340, 0351, 0355, 0359, 0691, 0711, 0849, 0873, and 0878.

In addition, certain records produced by Defendants in discovery contain redacted information reflecting narrative descriptions of information or data observed or found during a search of the electronic devices of the following Plaintiffs:

- Nadia Alasaad
- Siddarayappa Bikkanavar
- Jeremie Dupin
- Diane Maye
- Zainab Merchant

Additional information regarding whether and to what extent Defendants included information or data copied from or regarding a specific electronic device in their law enforcement records and systems would reveal information protected from disclosure under the law enforcement privilege.

INTERROGATORY NO. 11

Identify and describe the manner in which Defendants calculate the number of border searches of electronic devices conducted in each fiscal year, including whether the number is calculated by relying on particular types of records or reports, such as Electronic Media Reports, in CBP or ICE databases, and whether the number is calculated by using any records or reports not contained in CBP or ICE databases.

Defendants' Response:

Defendants object to this interrogatory's use of the term "in each fiscal year" as vague and ambiguous insofar as it fails to identify the fiscal year(s) at issue. Subject to the foregoing objection, Defendants respond as follows:

ICE calculates the number of searches of electronic devices conducted by ICE from the information entered into the Computer Forensics Program's Field Exam Report (FER) system by the Computer Forensics Agent or Analyst conducting the search. CBP Officers are required by policy to complete an Electronic Media Report (EMR) for each border search of an electronic device. To generate the number of border searches of electronic devices in a given time period, CBP calculates the number of closed or completed EMRs that relate to searches that were initiated during the time period at issue.

DOCUMENT REQUEST 17

Documents reflecting the August 28, 2017 search of the phone being used by Ms. Alasaad's daughter (Lamees Alasaad).

Defendants' Response: Defendants object to this Request to the extent it seeks information protected from disclosure by the attorney-client privilege and/or the work-product doctrine. Subject to the foregoing objections, Defendants respond as follows:

Based on Defendants' search, to the best of their knowledge, there are no responsive documents.

DOCUMENT REQUEST 18

Documents reflecting alleged searches of Plaintiff Kushkush's electronic devices on January 9, 2016, January 10, 2016, or January 4, 2017.

Defendants' Response: Subject to Defendants' Objections and Responses to Requests 11 and 12 in Plaintiffs' First Set of Requests for Production to All Defendants, Defendants respond as follows:

Defendants have produced all responsive documents pertaining to Plaintiff Kushkush and have no additional documents to produce. Based on Defendants' search, to the best of their knowledge, there are no documents reflecting alleged searches of Plaintiff Kushkush's electronic devices on January 9, 2016, January 10, 2016, or January 4, 2017.

DOCUMENT REQUEST 19

Any additional documents used to support the statements in paragraphs 107-113 of Defendants' Answer.

Defendants' Response: Defendants object to this Request to the extent it seeks information protected from disclosure by the law enforcement privilege, attorney-client privilege, and/or the work-product doctrine. Defendants further object to this Request's use of the term "used to support," which is vague and arguably calls for information that is presumptively not subject to

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

DEFENDANTS' OBJECTIONS AND RESPONSES TO PLAINTIFFS' SECOND SET OF REQUESTS FOR PRODUCTION AND PLAINTIFFS' THIRD SET OF INTERROGATORIES

Pursuant to Rules 26, 33, and 34 of the Federal Rules of Civil Procedure and the Local Rules of the United States District Court for the District of Massachusetts, Defendants, by and through undersigned counsel submit their Objections and Responses to Plaintiffs' Second Set of Requests for Production and Third Set of Interrogatories.

DOCUMENT REQUEST NO. 20

All documents, including but not limited to policy and training documents, related to the procedures for obtaining a judicial warrant as outlined in Customs and Border Protection's Personal Search Handbook.[1] *See, e.g.*, pp. 10, 29, 35, and 36

[1] https://www.regulations.gov/document?D=ICEB-2012-0003-000

DOCUMENT REQUEST NO. 23

All documents, including but not limited to policy and training documents, related to Defendants' compliance, during border searches or seizures of electronic devices, with *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), *Riley v. California*, 134 S. Ct. 2473 (2014), or *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018).

RESPONSE:

Defendants object to this Request to the extent it seeks information protected from disclosure by the law enforcement privilege, attorney-client privilege, the work-product doctrine, and/or the deliberative process privilege. Defendants further object to the Request for "all documents . . . related to the procedures for obtaining a judicial warrant[,]" as vague, ambiguous, overly broad and unduly burdensome insofar as it purports to request every document which has any connection to Defendants' compliance with certain court decisions.

Subject to the foregoing objections, in response to this Request, CBP hereby refers Plaintiffs to documents previously produced in discovery: Defs. 0129-132. ICE refers Plaintiffs to documents previously produced in discovery: Defs. 0063-0091 and ICE also produces Bates pages 1266-1267 in response to this Request.

INTERROGATORY NO. 12

For Defendants' produced document Bates 909 regarding Plaintiff Matthew Wright, please explain what "To: EMC" and "Taken: CM" mean.

CBP's Response: In the produced document Bates 909, "To: EMC" refers to the individual to whom the incoming package was addressed. "Taken: CM" refers to the analyst to whom the incoming package was assigned.

INTERROGATORY NO. 13

Of the total number of electronic devices searched by Defendants during Fiscal Years 2012-2018 (per the statistics provided in Stipulations Nos. 13 and 15) pursuant to Defendants' electronic device search policies (CBP Directive Nos. 3340-049 and 3340-049A; ICE Directive No. 7-6.1/ICE Policy 10044.1), provide the number of devices that contained digital contraband for each fiscal year.

Defendants' Response: Defendants object to this interrogatory as vague due to its use of the undefined term "digital contraband," and accordingly it is unclear what information is sought by this interrogatory. Defendants also object to this interrogatory as overly broad and unduly burdensome to the extent it seeks to require Defendants to develop a definition of "digital contraband,"[2] to create mechanisms for compiling information relating thereto, and/or to create new statistics.

Subject to the foregoing objections, Defendants state that neither CBP's nor ICE's recordkeeping systems track or capture any such metrics and therefore they are unable to provide aggregate statistics reflecting the number of devices containing digital contraband.

INTERROGATORY NO. 14

Other than CBP Directive No. 3340-049A Secs. 5.4 and 5.5, and ICE Directive No. 7-6.1 Sec. 8.5, identify and explain the polices, practices, and training that are applicable to the recording and retention of information viewed, searched, or copied during searches of electronic devices seized or obtained from travelers at the border.

Defendant's Response: Defendants object to this interrogatory to the extent it seeks information protected by the law enforcement privilege. Defendants further object to this interrogatory as vague and overly broad to the extent it seeks information relating to policies, practices, and training regarding the processing, handling, and analysis of evidence and merchandise that applies generally, and not specifically to border searches of electronic devices.

Subject to the foregoing objections, Defendants respond as follows:

Pursuant to Fed. R. Civ. P. 33(d), CBP refers Plaintiffs to the following documents previously produced in discovery: Defs. 0113-24, 0125-26, 0127-28, 0133-61, 0162, 0174-218. In addition, CBP refers Plaintiffs to the Privacy Impact Assessment being produced in response to Plaintiffs' Second Set of Requests for Production at Bates Number Defs. 996-1056. The Privacy Impact Assessment addresses policies and practices applicable to the recording and retention of information viewed, searched, or copied during searches of electronic devices seized or obtained

[2] Although not defined by Plaintiffs, and subject to the objections noted above, in this answer Defendants generally use the term 'digital contraband' to refer to electronic information that it is unlawful to possess, to transport, to import into the United States, or to export from the United States.

from travelers at the border.

Pursuant to Pursuant to Fed. R. Civ. P. 33(d), ICE refers Plaintiffs to the documents previously produced discovery: Defs. 0034-0062, and Defs. 0916-0944, and is also producing Bates pages 1184-1224, 1240-1263, and 1264-1265 in response to this Request

In addition, to the extent information viewed, searched, or copied during searches of electronic devices is maintained in a system of records that is subject to the Privacy Act, the applicable System of Records Notice (SORN) sets forth additional policies and requirements related to the retention of such information. Defendants' SORNs are accessible at: https://www.dhs.gov/system-records-notices-sorns.

INTERROGATORY NO. 15

Other than CBP Directive No. 3340-049A Secs. 5.4 and 5.5, and ICE Directive No. 7-6.1 Sec. 8.3, identify and explain the polices, practices, and training that are applicable to the length of time that electronic devices seized or obtained from travelers at the border remain in CBP or ICE custody, in particular, how and why extensions of time are granted.

Defendant's Response: Defendants object to this interrogatory to the extent it seeks information protected by the law enforcement privilege.

Subject to the foregoing objection, Defendants respond as follows:

Pursuant to Fed. R. Civ. P. 33(d), CBP refers Plaintiffs to the following documents previously produced in discovery: Defs 0113-24, and 0174-218. In addition to CBP Directive No. 3340-0489A Secs. 5.4 and 5.5, the Privacy Impact Assessment addresses policies and practices applicable to the recording and retention of information viewed, searched, or copied during searches of electronic devices seized or obtained from travelers at the border.

Pursuant to Pursuant to Fed. R. Civ. P. 33(d), ICE refers Plaintiffs to documents previously produced in discovery: Defs. 0034-0062, 0063-0091, 0916-0944 and also produces Bates pages 1184-1224 in response to this Request.

INTERROGATORY NO. 16

Explain whether ICE (including, but not limited to, Homeland Security Investigations) makes decisions independent of CBP to conduct basic/manual or forensic/advanced searches of electronic devices seized or obtained at the border; and if so, how ICE officers decide to do so,

including what information about travelers is available to ICE officers.

ICE's Response: ICE objects to this Interrogatory as overly broad to the extent that it seeks agency-wide information and is not limited to Homeland Security Investigation, which is the office primarily responsible for investigating crimes at the border. ICE further objects to this Interrogatory to the extent it seeks law enforcement sensitive information.

Subject to the foregoing objections, ICE states that ICE Special Agents make independent decisions on whether and how they will conduct a border search of an electronic device, including whether they will perform a basic/manual and/or advanced/forensic search of that device. Prior to making such a decision, ICE Special Agents have access to numerous law enforcement systems that may contain information about a traveler that would inform a decision to conduct a border search, including any investigative information that ICE may have already developed concerning that traveler. An ICE Special Agent's decision whether and how to conduct any border search of an electronic device will be based upon the potential for that search to further a particular investigation into a suspected crime within the jurisdiction of ICE and will be guided by the policies and practices of ICE with regard border searches of electronic devices.

INTERROGATORY NO. 17

Explain whether and under what circumstances border officers employed by Defendants search or confiscate travelers' electronic devices at the request of any other federal, state, or local government department, agency, or entity. (Note that this interrogatory is not in reference to CBP Directive No. 3340-049A Secs. 5.4.2.1 or 5.5.2.2, or ICE Directive No. 7-6.1 Sec. 8.4, related to situations where CBP/ICE request technical or subject-matter assistance from other agencies or entities.)

Defendant's Response: Defendants object to this Interrogatory as vague and overly broad. Defendants object to the term "border officer" because it is not a term used by defendant agencies; therefore Defendants interpret the term to refer to an official employed by Defendants that conducts border searches of electronic devices pursuant to the Defendants' applicable policies. *See* CBP Directive 3340-049A and ICE Directive 10044. Defendants further object to

this Interrogatory because the term "confiscations" is undefined and has no commonly accepted meaning in this context. Defendants also object to this interrogatory to the extent it seeks information protected by the law enforcement privilege.

Subject to the foregoing objections Defendants respond as follows:

CBP conducts border searches of electronic devices in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer. While CBP decisions to perform border searches of electronic devices benefit from information provided by other law enforcement agencies, the decision for CBP to conduct a border search of an electronic device rests exclusively with CBP and is conducted in accordance with applicable law and policy. A CBP Officer may conduct a basic search, as defined in CBP Directive No. 3340-049A Sec. 5.1.3, with or without suspicion. With appropriate supervisory approval, a CBP Officer may conduct an advanced search, as defined in CBP Directive No. 3340-049A, in instances in which there is reasonable suspicion of activity in violation of the laws enforced and administered by CBP, or in which there is a national security concern.

ICE states that ICE Special Agents make independent determinations on the jurisdiction, justification, and necessity for every border search they undertake. While information provided to ICE by other law enforcement agencies may inform an ICE Special Agent's decision to perform a border search of an electronic device, ICE conducts border searches to further ICE investigations and pursue ICE's law enforcement mission and does not conduct border searches or detain electronic devices at the request of any other agency.

EXHIBIT 27

~~LAW ENFORCEMENT SENSITIVE~~

OFFICE OF INSPECTOR GENERAL

CBP's Searches of Electronic Devices at Ports of Entry - Redacted

~~LAW ENFORCEMENT SENSITIVE WARNING: The information in this document marked LES is the property of the Department of Homeland Security and may be distributed within the Federal Government (and its contractors) to law enforcement, public safety and protection, and intelligence officials and individuals with a need to know. Distribution to other entities without prior Department of Homeland Security authorization is prohibited. Precautions shall be taken to ensure this information is stored and destroyed in a manner that precludes unauthorized access. Information bearing the LES marking may not be used in legal proceedings without prior authorization from the originator. Recipients are prohibited from posting information marked LES on a website or unclassified network.~~

~~LAW ENFORCEMENT SENSITIVE~~

Homeland Security

December 3, 2018

OIG-19-10

Defs. 0972

~~LAW ENFORCEMENT SENSITIVE~~

DHS OIG HIGHLIGHTS

CBP's Searches of Electronic Devices At Ports of Entry

December 3, 2018

Why We Did This Audit

The *Trade Facilitation and Trade Enforcement Act of 2015* (TFTEA) requires U.S. Customs and Border Protection (CBP) to establish standard operating procedures (SOP) for searching, reviewing, retaining, and sharing information in communication, electronic, or digital devices at U.S. ports of entry. The TFTEA also requires the DHS Office of Inspector General to conduct three annual audits to determine to what extent CBP conducted searches of electronic devices in accordance with the SOPs.

What We Recommend

We made five recommendations to improve CBP's oversight of searches of electronic devices at ports of entry.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

Between April 2016 and July 2017, CBP's Office of Field Operations (OFO) did not always conduct searches of electronic devices at U.S. ports of entry according to its SOPs. Specifically, because of inadequate supervision to ensure OFO officers properly documented searches, OFO cannot maintain accurate quantitative data or identify and address performance problems related to these searches. In addition, OFO officers did not consistently disconnect electronic devices, specifically cell phones, from the network before searching them because headquarters provided inconsistent guidance to the ports of entry on disabling data connections on electronic devices.

OFO also did not adequately manage technology to effectively support search operations and ensure the security of data. Finally, OFO has not yet developed performance measures to evaluate the effectiveness of a pilot program, begun in 2007, to conduct advanced searches, including copying electronic data from searched devices to law enforcement databases.

These deficiencies in supervision, guidance, and equipment management, combined with a lack of performance measures, limit OFO's ability to detect and deter illegal activities related to terrorism; national security; human, drug, and bulk cash smuggling; and child pornography.

CBP's Response

CBP concurred with our recommendations. We have included a copy of CBP's response to our draft report at appendix A.

~~LAW ENFORCEMENT SENSITIVE~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

December 3, 2018

MEMORANDUM FOR: Todd Owen
Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

FROM: Sondra F. McCauley
Assistant Inspector General for Audits

SUBJECT: *CBP's Searches of Electronic Devices at Ports of Entry*

Attached for your action is our final report, *CBP's Searches of Electronic Devices at Ports of Entry*. We incorporated the formal comments provided by your office.

The report contains five recommendations aimed at improving the overall effectiveness of CBP's oversight of searches of electronic devices at ports of entry. Your office concurred with all five recommendations. Based on information provided in your response to the draft report, we consider the five recommendations resolved and open. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence showing completion of the agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please call me with any questions, or your staff may contact Donald Bumgardner, Deputy Assistant Inspector General for Audits, at (202) 981-6000.

Background

U.S. Customs and Border Protection (CBP) exercises law enforcement authority when securing the Nation's borders and 328 ports of entry. Electronic devices, such as computers, thumb drives, and mobile phones, are subject to search at U.S. ports of entry to ensure the enforcement of immigration, customs, and other Federal laws.

CBP processed more than 787 million travelers upon arrival at U.S. ports of entry in fiscal years 2016 and 2017, and searched approximately 47,400 electronic devices. In fiscal year 2016, CBP processed more than 390 million travelers arriving at U.S. ports of entry and searched the electronic devices of an estimated 18,400 of those inbound travelers (.005 percent). In FY 2017, CBP processed more than 397 million travelers and searched the electronic devices belonging to more than 29,000 of those inbound travelers (.007 percent).

CBP's Office of Field Operations (OFO) is responsible for determining the admissibility of travelers at U.S. ports of entry. OFO officers conduct primary inspections of all travelers arriving at ports of entry. During a primary inspection, OFO officers review travelers' passports and other documents to decide whether to admit travelers to the United States or refer them for secondary inspection.

During secondary inspection, an OFO officer may search a traveler's electronic device to determine admissibility and identify any violation of laws. For instance, in March 2018, during a search of a traveler's electronic device, officers found images and videos of terrorist-related materials. In another incident, officers found graphic and violent videos, including child pornography. CBP denied both travelers entry into the United States.

A secondary inspection may involve a basic (manual) search, an advanced search, or both. The officer can make a referral for a manual search because of inconsistencies in response, behavioral analysis, or intelligence analysis. A manual search involves the OFO officer manually reviewing the information on a traveler's electronic device.

An advanced search, which OFO started as a pilot program in 2007, involves a specially trained officer connecting external equipment to the traveler's device to copy information. The officer uploads the copied information to CBP's Automated Targeting System (ATS) to be further analyzed against existing ATS information. CBP personnel provide real-time feedback to the OFO officer of any identified derogatory information.

Results of Audit

During our review of a sample of border searches of electronic devices conducted between April 2016 and July 2017, we determined that OFO did not always conduct the searches at U.S. ports of entry according to its SOPs. Specifically, because of inadequate supervision to ensure OFO officers properly documented searches, OFO cannot maintain accurate quantitative data or identify and address performance problems related to these searches. In addition, OFO officers did not consistently disconnect electronic devices, specifically cell phones, from networks before searching them because headquarters provided inconsistent guidance to the ports of entry on disabling data connections on electronic devices. OFO also did not adequately manage technology to effectively support search operations and ensure the security of data. Finally, OFO has not yet developed performance measures to evaluate the effectiveness of a pilot program, begun in 2007, to conduct advanced searches, including copying electronic data from searched devices to law enforcement databases.

These deficiencies in supervision, guidance, and equipment management, combined with a lack of performance measures, limit OFO's ability to detect and deter illegal activities related to terrorism; national security; human, drug, and bulk cash smuggling; and child pornography.

Searches of Electronic Devices Not Always Properly Documented

OFO officers did not always properly document actions and complete the required chain of custody forms when conducting searches of electronic devices. This occurred because supervisors did not always adequately review documentation to ensure officers properly documented searches at the ports of entry.

CBP Directive 3340-049, *Border Search of Electronic Devices Containing Information*, dated August 20, 2009, was in effect at the time of our review. According to the directive, CBP officers are responsible for completing all applicable documentation in the appropriate CBP systems of record when conducting electronic searches. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition, including supervisory approvals and extensions when appropriate. In addition, the duty supervisor is to ensure the officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

We reviewed 194 EMRs and identified 130 (67 percent) that featured one or more problems, which totaled 147 overall. See table 1.

Table 1: Problems Identified in CBP Electronic Media Reports

Insufficient or Inaccurate Information	Number of EMRs
Vague narrative describing border search	62
Inaccurate notes or action details	31
No witnessing supervisor documented	29
Detention and Seizure Chain of Custody Forms	
Missing information on Forms 6051D & 6051S	7
Late Supervisory Review	
Review more than 7 days from incident	18

Source: OIG analysis of EMRs from CBP

Without accurate and complete documentation of border searches of electronic devices, OFO cannot maintain reliable quantitative data, identify and address performance problems, and minimize the risk of electronic devices becoming lost or misplaced.

Data Connections Not Consistently Disabled Prior to Searching Electronic Devices

A border search of an electronic device conducted by an OFO officer should include an examination of only the information that is physically on the device, not information stored on a remote server. To avoid retrieving or accessing information stored remotely, officers should either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode) or, in instances warranted by national security, law enforcement, officer safety, or other operational considerations, officers will disable network connectivity. However, OFO officers did not consistently disconnect electronic devices, specifically cell phones, from the network before searching them. This occurred because headquarters provided inconsistent guidance to the ports of entry on disabling electronic devices' data connections.

Specifically, in April 2017, OFO issued a memo[7] that claimed to reaffirm its existing policy and protocol for disconnecting electronic devices from internet access (i.e., disabling network connections) before a search.[8] Unless each device's network connection is disabled, OFO could potentially retrieve information from external sources, leaving the results of the border search questionable. However, Directive 3340-049, the policy at the time, did not require disabling data connections prior to conducting a search. Of the 194 EMRs we reviewed, 154 were completed prior to the issuance of the April 2017

[7] *Border Search of Electronic Devices Containing Information*, dated April 13, 2017.
[8] Disabling data connections ensures that electronic devices are limited to the data on them.

memo. None of the 154 contained evidence that data connections were disabled on electronic devices searched.

In addition, the April 2017 memo required OFO officers to document in the EMR whether cellular and data connections were disabled prior to conducting a search and further required supervisors to confirm connections were disabled in a statement in the EMR before approving it. Despite these requirements, OFO supervisors did not provide adequate oversight to ensure officers disabled data connections on electronic devices prior to searching them, nor did the supervisors properly review EMRs. We reviewed 40 EMRs completed after the issuance of the April 2017 memo. Even though OFO supervisors reviewed and approved EMRs, more than one-third of the EMRs (14 of 40) lacked a statement confirming that the electronic device's data connection had been disabled.

Since we began the audit, CBP has taken action to improve in this area. In October 2017, CBP completed system enhancements to their EMRs in TECS. Those enhancements include a mandatory data field to allow officers to select, rather than compose, a statement to confirm disabling a device data connection. Additionally, on January 4, 2018, CBP issued Directive 3340-049A, *Border Search of Electronic Devices,* which supersedes Directive 3340-049. Unlike the superseded directive, the newly issued directive expressly states, "Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode); or, where warranted by national security, law enforcement, officer safety, or other operational considerations, officers will themselves disable network connectivity."

External Equipment and Data for Border Searches Not Well Managed

According to the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, Sections 10.03 and 12.01, management is responsible for establishing physical control to secure and safeguard vulnerable assets and implement control activities through policies. However, OFO is not managing the external equipment used to conduct advanced border searches of electronic devices well. Specifically, OFO did not renew software licensing agreements for external equipment expeditiously and maintained information copied on thumb drives that should have been deleted.

OFO Did Not Renew Software Licensing of External Equipment Expeditiously

OFO purchased the [redacted] tool, which is a computer triage tool that enables examination of laptop hard drives, USB[9] drives, and multimedia cards, to prohibit importation of illegal materials. The [redacted] tool requires an annual license renewal that encompasses a warranty, support, maintenance, and software upgrades to maximize security effectiveness. We reviewed software licensing agreements of the [redacted] tool from 2016 and 2017 and found a licensing lapse. Because OFO headquarters did not renew the software licensing of the [redacted] tool expeditiously, licensing agreements were only in effect from January 20, 2016, through January 31, 2017; and from September 13, 2017, through September 12, 2018.

Software licensing agreements were **not** in effect from February 1, 2017, through September 12, 2017.

According to an OFO official, there is no dedicated funding for external equipment such as the [redacted] tool because it is part of the advanced searches of electronic devices pilot program. According to the same official, due to the lack of dedicated funding and the combination of budgetary issues and other funding priorities, the initial vendor estimate he received for the purchase expired. Therefore, he had to obtain another vendor estimate, which caused a delay in promptly submitting the license renewal documentation.

Without a valid software license, OFO officers could not conduct advanced searches of laptop hard drives, USB drives, and multimedia cards at the ports of entry. This deficiency limited OFO's ability to obtain evidence of criminal activity and to detect and deter illegal activities, such as child pornography. Additionally, it hinders OFO's ability to mitigate the risk of criminals entering the United States with unexamined national security or law enforcement-related information on their laptops.

OFO Does Not Always Delete Travelers' Information Copied during Advanced Searches

During advanced searches, OFO officers connect external equipment to electronic devices and copy information onto a thumb drive; the copied information is uploaded via the thumb drive to the CBP's ATS for further analysis. According to two OFO training officials, once an OFO officer completes an ATS upload, he or she should immediately delete all copied information from the thumb drive, but OFO could not provide written policy or procedures related to the training officials' oral requirement.

[9] Universal Serial Bus is a common interface that enables communication between devices and a host controller such as a personal computer.

We physically inspected thumb drives at five ports of entry. At three of the five ports, we found thumb drives that contained information copied from past advanced searches, meaning the information had not been deleted after the searches were completed. Based on our physical inspection, as well as the lack of a written policy, it appears OFO has not universally implemented the requirement to delete copied information, increasing the risk of unauthorized disclosure of travelers' data should thumb drives be lost or stolen.

OFO Has Not Developed Performance Measures for the Advanced Searches of Electronic Devices Pilot Program

According to GAO's *Standards for Internal Control in the Federal Government,* management should establish activities to monitor performance measures and indicators. These may include comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken.

OFO has not developed performance measures to assess the effectiveness of its advanced searches of electronic devices pilot program. In 2007, four ports of entry used external equipment for OFO's advanced searches of electronic devices pilot program; OFO has now expanded the pilot to 67 ports of entry. Although OFO maintains quantitative data on the number and location of advanced searches, it has not developed performance measures. One area to measure is the number of instances in which information collected from searches resulted in a prosecution or conviction, but according to OFO, it does not track this information.

Without performance measures, OFO cannot evaluate the effectiveness of the pilot program. OFO will not be able to determine whether the advanced searches are achieving their intended purpose or whether the use of advanced searches should be expanded to other ports of entry.

Conclusion

In FY 2017, CBP searched electronic devices belonging to more than 29,000 inbound travelers. Given the number of searches, it is important that OFO ensure the searches are properly documented and that OFO officers conducting the searches are adequately overseen. Properly managing the equipment used to conduct advanced searches is also critical to make certain officers are not limited in their ability to detect and deter illegal activities. As the world of information technology evolves, techniques used by OFO must also evolve to identify, investigate, and prosecute individuals who use new technologies to commit crimes. Finally, to demonstrate OFO is meeting its security mission, developing performance measures will be essential to assess the effectiveness of OFO's pilot program of advanced searches, which has been

EXHIBIT 28

Privilege ID No.	Bates-Stamp Number(s)	No. of Pages	Author	Recipient	Date	Location/Origination of Document	Disposition of Document	Privilege and/or Grounds for Withholding	Description of Withheld Information
3	N/A	4	N/A	N/A	Date Withheld	CBP	Withheld in full	Law enforcement privilege	Query results from law enforcement database, containing information subject to the law enforcement privilege: computer system codes and data fields; informaton that would reveal the scope of law-enforcement database queries and the results thereof; information that would reveal communication methods regarding the exchange of law enforcement information pertinent to the exercise of officer discretion; information relating to law enforcement operations, methods, techniques, and procedures (including examination and inspection methods); and information which would reveal the nature, scope, and focus of certain law enforcement processes, techniques, and methods. Disclosure would allow individuals to devise strategies to circumvent law enforcement methods and procedures (including for examination and inspection). Disclosure would further reveal technical capabilities and methods utilized by CBP computer systems and enable an individual to improperly access and navigate the system, to disrupt the exchange of relevant information among law enforcement personnel, and to interfere with enforcement processes or proceedings.
N/A (former 4)	909	1	N/A	N/A	Multiple	Laboratory and Scientific Services, CBP	Produced with redactions	Law enforcement privilege	Log of items received by CBP laboratory, containing information subject to the law enforcement privilege: information which would reveal the nature, scope, and focus of certain law enforcement processes, techniques, and methods; information that would reveal communication and delivery methods regarding the exchange of information and objects relating to law enforcement examinations and inspections. Disclosure would allow individuals to devise strategies to circumvent law enforcement methods and procedures (including for examination and inspection). Disclosure would further reveal technical capabilities and methods utilized by CBP and enable an individual to interfere with enforcement processes or proceedings.

EXHIBIT 29

Privacy Impact Assessment
for the

Border Searches of Electronic Devices

August 25, 2009

Contact Points
Thomas S. Winkowski
Assistant Commissioner, Office of Field Operations
U.S. Customs and Border Protection
(202) 344-1620

Kumar C. Kibble
Acting Director, Office of Investigations
U.S. Immigration and Customs Enforcement
(202) 732-3000

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security
(703) 235-0780

belongings, including electronic devices and the information in such devices.[8] In addition to searches conducted to ensure merchandise is not being introduced into the U.S. contrary to law, the authorities for these searches also allow for the review of information relating to the admissibility of persons into the United States under federal immigration law.

DHS's border search authorities are derived from those exercised, prior to the homeland security reorganization in 2003, by the U.S. Customs Service (USCS) and the Immigration and Naturalization Service (INS). Those agencies were merged into DHS and reorganized into the Customs Service – later renamed CBP, which retained the inspectional and patrol functions of USCS and INS; and ICE, which retained the investigative components of USCS and INS. CBP and ICE continue to hold the border search authorities previously exercised by USCS and INS. CBP, as the interdictory agency, and ICE, as the investigative agency, now work hand-in-hand at the border to set forth a seamless process for the international traveler.

Border Searches in Support of CBP and ICE Law Enforcement Missions

As the Nation's law enforcement agencies at the border, CBP interdicts and ICE investigates a range of illegal activities such as child pornography; human rights violations; smuggling of drugs, weapons, and other contraband; financial and trade-related crimes; violations of intellectual property rights and law (e.g., economic espionage); and violations of immigration law, among many others. CBP and ICE also enforce criminal laws relating to national security, terrorism, and critical infrastructure industries that are vulnerable to sabotage, attack or exploitation.

In the course of their daily practices, CBP Officers and ICE Special Agents may interview travelers undergoing inspection at the border and/or conduct border searches of travelers and their belongings.[9] In some cases, CBP and/or ICE may search a traveler because he is the subject of, or person-of-interest in, an ongoing law enforcement investigation and was flagged by a law enforcement "lookout" in the CBP enforcement system known as TECS.[10] If questions regarding the admissibility of an individual or his or her belongings cannot be resolved at the primary inspection station, CBP may elect to conduct a more in-depth inspection of the traveler (referred to as "secondary inspection"). At any point during the inspection process, CBP may refer the traveler and his belongings to ICE for a search, questioning, and for possible investigation of violations of law. ICE has concurrent border search authority with CBP and may join or independently perform a border search at any time.

In many instances, CBP and ICE conduct border searches of electronic devices with the knowledge of the traveler. However, in some situations it is not practicable for law enforcement reasons to inform the traveler that his electronic device has been searched.

---

[8] *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008), *cert. denied*, 129 S.Ct. 1312 (Feb. 23, 2009); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006); and *United States v. Roberts*, 274 F.3d 1007 (5th Cir. 2001).

[9] Travelers arriving in the United States at a port of entry must go through CBP inspection where CBP has two missions, which are often interdependent: (1) to ensure the traveler is legally admissible to the United States; and (2) to ensure all items accompanying the traveler are permitted legal entry into the United States.

[10] *See* the Privacy Act System of Records Notice, DHS U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008, 73 FR 77778.

specific subject matter expertise that may be necessary to allow CBP or ICE to access or understand the detained information.

Process

Travelers arriving at a port of entry must go through primary inspection, where a CBP Officer checks the traveler's documentation and determines the traveler's admissibility to the United States. During primary inspection, the CBP Officer may determine, through his observations or through an alert indicated on the primary inspection computer screen, that the traveler warrants further examination and thus will refer the traveler to secondary inspection. Travelers are typically referred to secondary inspection to resolve immigration, customs, or other law enforcement matters. At secondary inspection, a CBP Officer or ICE Special Agent may ask the traveler questions and inspect the traveler's possessions to detect violations or evidence of violations of law. This border search may include examination of documents, books, pamphlets, and other printed material, as well as computers, storage disks, hard drives, phones, personal digital assistants (PDAs), cameras, and other electronic devices. Referrals for secondary examination may also be the result of a random compliance measurement selection through a system referred to as COMPEX.[12]

At every stage after the traveler is referred to secondary inspection, CBP and/or ICE maintain records of the examination, detention, retention, or seizure of a traveler's property, including any electronic devices. Additionally, as travelers enter the port area, they are informed through the posting of signage that all vehicles, other conveyances, persons, baggage, packages, or other containers are subject to detention and search. With the publication of this PIA, CBP will work to amend this signage both to state explicitly that electronic devices are subject to detention and search, and to include a Privacy Act Statement providing notice of DHS's authority to collect information from electronic devices. [See Appendix A for the Privacy Act Statement.]

Search

At primary or secondary inspection, a CBP Officer and/or ICE Special Agent may perform a quick, cursory search of the electronic device in front of the passenger. This may be as simple as turning on the device to establish that it is a working device, rather than a shell for concealed contraband, weapons or explosives. CBP or ICE may direct the traveler to turn on the device to establish that it works, or may take the device from the traveler and perform the task itself. A record of the interaction is entered into TECS.[13] Where information found on the electronic device may be relevant to a traveler's admissibility under the Immigration and Naturalization Act (8 U.S.C. § 1101 *et seq.*), a notation may be made in the appropriate CBP or ICE records systems, such as ENFORCE.[14] Where a traveler makes a request and it is operationally feasible to honor such a request, an examination at secondary inspection may take place in a private area, away from other travelers, including traveling companions. If CBP and ICE are satisfied that no further examination is needed, the electronic device is returned to the traveler

[12] For more information about CBP's random examination program, COMPEX, visit: http://www.cbp.gov/xp/cgov/travel/admissibility/random_exams.xml
[13] *See* U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008, 73 FR 77778; U.S. Immigration and Customs Enforcement External Investigations DHS/ICE-009 December 11, 2008, 73 FR 75452..
[14] *See* Enforcement Operational Immigration Records (ENFORCE/IDENT) DHS/ICE-CBP-CIS-001-03, March 20, 2006 71 FR 13987.

entities require all information be returned to ICE upon completion of assistance.[41] The Special Agent is required to contact the assisting agency or entity within the first 30 days to get a status report and to continue contact thereafter until a final response is received.[42]

Seizure

When either CBP or ICE determines probable cause exists to seize the electronic device, the seizing Officer or Special Agent completes a chain of custody form (CF 6051S) to reflect the seizure.[43] A seizure record is also made in the Seized Asset and Case Tracking System (SEACATS) and noted in TECS.[44] If the original device is seized in the presence of the traveler, the traveler is given a copy of the CF 6051S at the time of seizure.[45] If the original device has been detained and referred to ICE, and should ICE find probable cause to seize the device, the chain of custody form for the detention (CF 6051D) is superseded by a seizure form (CF 6051S). The seizure form is mailed to the traveler in accordance with applicable laws and regulations for customs seizures.[46] Any CBP records and notes are turned over to ICE for investigation and prosecution. If CBP or ICE did not detain the original device, but instead detained a copy of the data contained on the device, the first copy made is known as the "gold copy"; the chain of custody form stays with the gold copy.

Destruction

Electronic devices are never destroyed unless they are seized for civil forfeiture or as evidence of criminal activity, and are subsequently forfeited to the Government. Electronic devices that are not seized are returned to the traveler as expeditiously as possible following the conclusion of the border search.[47] Copies of information from electronic devices are not retained by CBP or ICE unless retention is required for a law enforcement purpose and is consistent with the system of records that covers the detained information.[48] Detained electronic information that is destroyed is not merely deleted, but forensically wiped, which entails writing over the information multiple times to ensure it cannot be accessed again.[49] Once the electronic copy is forensically wiped, a record of the destruction is documented in the TECS Report of Investigation (ROI), as appropriate.[50]

As stated above under "Detention," CBP or ICE may detain an electronic device or a copy of information on a device in order to determine if it has investigative or enforcement value. Should CBP or ICE determine there is no value to the information copied from the device, that information is destroyed as expeditiously as possible. For CBP and ICE, the destruction must take place no later than seven

[41] ICE Directive at 8.
[42] ICE Directive at 7.
[43] ICE Directive at 4.
[44] *See* Seized Assets and Case Tracking System DHS/CBP-013 December 19, 2008, 73 FR 77764.
[45] ICE Directive at 4.
[46] *See* 19 C.F.R. Part 162.
[47] CBP Directive at 4.
[48] This means that if CBP retains the information, CBP retention policy for a particular system of records would govern. If ICE ultimately retains the information, ICE retention policy for a particular system of records would govern.
[49] CBP Directive at 2.
[50] CBP Directive at 4; ICE Directive at 8.

and copy) and the electronic devices. (Unless otherwise specified, any reference to ICE Special Agents in this PIA also includes CFAs.) CFAs are also trained in the proper and secure destruction of electronic information.

ICE policies and procedures that safeguard this information are enforced through a variety of oversight mechanisms, including requirements to appropriately document these activities in case files, documentation required for forensic examinations, and random and routine inspections of field offices. Inspections delve into every aspect of the ICE Special Agent's responsibilities, ranging from security of the hardware and facility, to training and recordkeeping. All ICE Special Agents are required to take yearly training courses, available through the ICE Virtual University, including annual Information Assurance Awareness Training, which stresses the importance of good security and privacy practices, and Records Management Training, which stresses agency and individual responsibilities related to record creation, maintenance, use, retention and disposition. Additionally, in the coming months, ICE Special Agents will be required to complete a new training course specifically focusing on ICE's Directive on border searches of electronic devices. This training will focus on ICE policies with respect to searches involving sensitive information (e.g., privileged material) and other procedural requirements and safeguards. The training is intended to reinforce Special Agents' knowledge of the ICE policy and to serve as a reminder to treat such searches with special care. Additionally, CFAs are required to take annual continuing education classes specific to computer and digital forensics, which may include the latest techniques and methods on copying, analyzing, and destroying electronic information.

ICE recognizes electronic devices have the capacity to store sensitive information, however a traveler's claim of privilege or statement to an ICE Special Agent that something is personal or business-related does not preclude the search.[65] ICE policy and certain laws, such as the Privacy Act and the Trade Secrets Act, requires the special handling of some types of sensitive information including attorney-client privileged information, proprietary business information, and medical information.[66] Special Agents violating these laws and policies are subject to administrative discipline and criminal prosecution. Further, when a Special Agent suspects that the content of electronic devices includes attorney-client privileged material that may be relevant to the laws enforced by ICE, ICE policy requires the Special Agents to contact the local ICE Chief Counsel's office or the local U.S. Attorney's Office before continuing a search. [67]

During transmission to other federal agencies and non-federal entities for assistance, ICE takes appropriate measures to safeguard the information, to include, encrypting electronic information where appropriate, storing in locked containers, and hand delivery. In addition to the demand letter that is sent to assisting agencies and entities, the information and devices sent for analysis is accompanied by a chain of custody form.

When ICE determines that electronic devices or information may not be kept by ICE pursuant to its Directive, any copies of information obtained from such devices are destroyed.[68] The destruction technique follows ICE policies with regard to the particular form of information, is coordinated with the

[65] ICE Directive at 9.
[66] ICE Directive at 9.
[67] ICE Directive at 9.
[68] ICE Directive at 8.

EXHIBIT 30

Office of Investigations

U.S. Department of Homeland Security
425 I Street, NW
Washington, DC 20536

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Assistant Directors
All Deputy Assistant Directors
All Special Agents in Charge

MAR 15 2007

FROM: Marcy M. Forman
Director, Office of Investigations

SUBJECT: Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry

This memorandum provides guidance and clarifies responsibilities related to the detention or seizure of electronic media from persons of national security interest at Ports of Entry (POE), and serves as a reminder of current U.S. Immigration and Customs Enforcement (ICE) policies regarding the use of border search authority as it relates to electronic media. ICE's ability to exploit this media represents a unique opportunity to collect, analyze and disseminate valuable information that directly supports the missions of ICE and the Department of Homeland Security (DHS).

BORDER SEARCHES

In accordance with customs border search authorities, pursuant to section 1582 of Title 19, United States Code, ICE may conduct routine stops and searches of merchandise and persons at the U.S. border without any individualized suspicion. Additionally, pursuant to immigration authorities found in sections 1225 and 1357 of Title 8, United States Code, ICE may inspect all aliens who apply for admission; take and consider evidence concerning the privilege of any person to enter, pass through, or reside in the United States that is material or relevant to enforcement of immigration laws; and conduct a search without a warrant of any person and the personal effects in their possession when there is reasonable cause to suspect a basis for denying admission to the United States. The objective of a border search is generally twofold: (1) to inspect for merchandise being imported contrary to law; and (2) to obtain information or evidence relating to an individual's admissibility. ICE may detain or seize anything that may be evidence of a crime or indicates criminal activity. Computers, cellular phones, and other electronic media are considered closed containers with regard to border search authority and are subject to being opened and searched by ICE. Regardless of citizenship, all persons seeking admission to the United States, and their merchandise are subject to border search. There is no requirement that this search be conducted with the knowledge of the person possessing the electronic media.

ICE may review, copy, image, detain or seize, and disseminate electronic media if a violation of law is immediately evident, if further review by ICE is needed to make such a determination, or if technical assistance (e.g., translation services) is deemed necessary. Electronic media detained or seized during a border search shall not be retained by ICE longer than is necessary to determine its relevance to furthering the law enforcement mission of ICE. Any information deemed relevant will be evaluated periodically to determine its continuing significance.

Subsequent to a border search, ICE may share obtained information relating to national security with law enforcement and intelligence agencies. It is important to note that any electronic media obtained through border search authority must be searched by ICE and deemed to be of law enforcement or intelligence interest prior to any sharing with an outside agency. Pursuant to current authorities, law enforcement information may be exchanged between the law enforcement components of DHS and other local, state, Federal, and foreign law enforcement agencies in accordance with specific agreements and other legal authorities. All requests for information [redacted] must be coordinated with the [redacted]

ELECTRONIC MEDIA – PERSONS [redacted]

Pursuant to existing referral agreements between ICE and U.S. Customs and Border Protection (CBP), all CBP interdiction matters related to terrorism or threats to national security are referred to ICE and the [redacted] CBP also notifies the [redacted] and, through that venue, the ICE representative at the [redacted] will notify [redacted] duty agent in the field to respond, as appropriate, per ICE policy. In most cases, the ICE [redacted] duty agent will respond to the POE to interview the subject. An ICE [redacted] duty agent and/or ICE Computer Forensics Agent (CFA) may conduct a cursory search of the subject's electronic media and detain or image the electronic media to conduct a more thorough examination. (NOTE: Electronic media that contains data or images that are obviously contraband should be seized in accordance with established procedures.)

In each case, the CFA [redacted] duty agent if no CFA is available) shall document the search and/or retention of information contained on the electronic media of persons of national security interest by posting [redacted]. When electronic media is physically detained, rather than merely making a forensic image of such media, that detention should be documented in the Seized Asset and Case Tracking System, as per existing ICE policy. The TECS seizure number should be referenced in [redacted].

[redacted] the ICE JTTF duty agent may [redacted]

Questions regarding the search, detention and/or seizure of electronic media from persons of national security interest can be directed to Program Manager [redacted], at (202) [redacted] or via email at [redacted]