

**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, ZAINAB)
MERCHANT, MOHAMMED AKRAM)
SHIBLY, MATTHEW WRIGHT AND)
DIANE MAYE ZORRI,)

Plaintiffs,)

v.)

KEVIN MCALEENAN, Acting Secretary,)
U.S. Department Of Homeland Security, in)
his official capacity; JOHN SANDERS,)
Acting Commissioner, U.S. Customs and)
Border Protection, in his official capacity; and)
MATTHEW T. ALBENCE, Acting Director,)
U.S. Immigration And Customs Enforcement,)
in his official capacity,)

Defendants.)

Civil Action No. 17-cv-11730-DJC

Hon. Denise J. Casper

**DEFENDANTS' STATEMENT OF UNDISPUTED MATERIAL FACTS AND
RESPONSE TO PLAINTIFFS' STATEMENT OF UNDISPUTED MATERIAL FACTS**

Pursuant to Federal Rule of Civil Procedure 56(c) and Local Rule 56.1, Defendants hereby submit their statement of undisputed material facts to which there is no genuine issue to be tried and also respond to Plaintiffs' statement of undisputed material facts. As described more clearly below, although Defendants dispute Plaintiffs' characterizations of evidence and facts, or dispute that the facts are material, Defendants do not contend that there are any disputed issues of material fact that must be tried. Defendants further assert that they are entitled to summary judgment as a matter of law.

DEFENDANTS' STATEMENT OF UNDISPUTED MATERIAL FACTS

FACTS RELATING TO PLAINTIFF' CONSTITUTIONAL CLAIMS

Defendants' Mission Responsibilities:

1. Defendant, Department of Homeland Security (“DHS”), through its components U.S. Customs and Border Protection (“CBP”) and U.S. Immigration and Customs Enforcement (“ICE”), has broad powers to prevent the entry of terrorists, and the instruments of terrorism into the United States and to enforce numerous criminal and civil federal laws at the border. *See* 6 U.S.C. § 202, § 211.
2. CBP’s law enforcement mission is primarily interdictive in nature – identifying and mitigating threats to border security and stopping prohibited and restricted goods and persons from crossing the border, while facilitating and expediting the flow of legitimate travelers and trade. *See* Declaration of Randy J. Howe (“Howe Decl.”) ¶ 7 (Ex. A); 6 U.S.C. § 211.
3. CBP is responsible for enforcing criminal and civil laws and administering comprehensive regulatory schemes relating to immigration, custom, international trade, child pornography, drug smuggling, weapons trafficking, financial crimes as well as national security and terrorism. Howe Decl. ¶ 7. CBP also enforces a host of other laws at the border on behalf of various federal agencies. *Id. See, e.g.*, 31 U.S.C. § 5317; 19 CFR 161.2(a); 19 CFR Part 12.
4. ICE’s Homeland Security Investigations (HSI), is principal investigative arm of DHS and is charged with securing the United States from transnational criminal threats. HSI’s mission is to investigate, disrupt, and dismantle terrorist, transnational, and other criminal organizations that threaten or seek to exploit the customs and immigration laws of the United States. HSI enforces a diverse portfolio of federal laws, including all types of cross-border criminal activity. Declaration of David L. Denton (“Denton Decl.”) ¶ 5 (Ex. B).
5. To accomplish their mission responsibilities. CBP officers and/or ICE Special Agents may conduct an inspection of the traveler and his or her personal belongings, including any electronic

devices. Howe Decl. ¶¶ 7, 17, 21-23; Denton Decl. ¶¶ 6-7, 11; *see generally* PIA dated August 25, 2009 (“2009 PIA”) at Bates 221-22 (Ex. C.).

Defendants’ Policies:

6. In August 2009, CBP and ICE issued policies on their longstanding authority to search and inspect electronic devices at the international border. *See generally* Border Searches of Electronic Devices, ICE Directive 10044.1 (also known as ICE Directive No. 7-6.1) (Aug. 18, 2009) (Ex. D); Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049, (Aug. 20, 2009) (Ex. E);

7. In January, 2018, CBP revised its Directive. *See* Border Search of Electronic Devices, CBP Directive No. 3340-049A, (Jan 4, 2018) (“2018 CBP Directive”) (Ex. F). Specifically, 2018 CBP Directive, among other things, (1) clarified the scope of CBP border searches of electronic devices and explicitly stated that measures would be taken to avoid accessing information only stored remotely (*e.g.*, on the “cloud”); (2) distinguished between different types of searches (basic and advanced); and (3) applied a heightened standard for advanced searches (reasonable suspicion or national security concern). *See id.* ¶ 5.1.

8. The updated CBP Directive defines an “advanced search” as any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy and/or analyze its contents. *Id.* § 5.1.4. A basic search is any border search that is not an advanced search. *Id.* § 5.1.3. The updated Directive further clarified that an advanced search should only be conducted where there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP and ICE or in which there is a national security concern, and requires advance supervisory approval *Id.* § 5.1.4.

9. ICE uses the same definitions of basic and advanced searches and only conducts advanced searches when there is reasonable suspicion. Stipulated Facts ¶¶ 1, 14. (Ex. G); Denton Decl. ¶ 11; HSI Legal Update – Border Search of Electronic Devices, May 11, 2018 at Bates 1266-67.

10. These policies have been carefully crafted to provide the Government, through DHS and its components, with the tools necessary to secure the nation's border, while simultaneously striving to protect personal privacy. *See* PIA, January 4, 2018 at Bates 0174-0195 (Ex. H).

11. These policies permit CBP Officers and ICE Special Agents to search information contained in electronic devices subject to the guidelines set forth in the policy directives and any other applicable laws. *See* ICE Directive ¶ 6.1; CBP Directive ¶¶ 4, 5.

12. The policies recognize that it is not always possible to complete the search of a traveler's electronic device while he or she waits at the border. ICE Directive ¶ 6.1; CBP Directive ¶ 5.4. The policies therefore require the searches of detained devices to be completed, in a reasonable time given the facts and circumstances of the particular search. ICE Directive ¶ 8.3(1); CBP Directive ¶ 5.4.

Border Searches:

13. Border inspections are unique and unlike any other law enforcement activity. CBP's mission to inspect all people and things that cross the border must be balanced with its mission to facilitate the flow of travelers and trade. *Howe Decl.* ¶ 8; 6 U.S.C. § 211.

14. Over one million travelers per day go through U.S. ports of entry, and CBP has limited to no advance information about these travelers. The sheer volume of people and merchandise passing through the border each day means CBP has a limited amount of time to determine the specific law enforcement actions appropriate for each encounter. *Howe Decl.* ¶ 8.

15. CBP officers evaluate the totality of the circumstances for each encounter at the border and will consider every piece of relevant information available to determine if the person and goods are admissible into the United States, if there is a violation of any of the laws CBP enforces, or if there is a threat to border security. *Howe Decl.* ¶¶ 10, 14-16. The ability to engage in these actions and the discretion to determine – based on the totality of the circumstances – which actions are appropriate in

a given inspection is crucial to CBP's ability to secure the border and identify and interdict threats to national security. *Id.* ¶ 16.

16. TECS is CBP's principal law enforcement and anti-terrorism database system used at the border to assist with inspections and determinations regarding admissibility of arriving persons. Howe Decl. ¶ 9. TECS includes law enforcement "lookouts" and other records entered by CBP and other law enforcement agencies regarding persons of interest. *Id.* TECS also includes law enforcement records documenting certain inspections conducted by CBP at the border, including border searches of electronic devices. *Id.*

17. CBP's documentation of its inspections are official government records made by the agency to evidence the decisions made and activities undertaken by CBP during the course of the encounter. Howe Decl. ¶ 9.

18. Upon arrival at a port of entry, at the primary point of inspection, CBP Officers inspect travelers' documentation (e.g., passport, customs declaration), ask questions regarding their travel and search CBP systems for relevant information. Howe Decl. ¶12. At primary, a CBP Officer may conduct limited queries of information maintained in TECS. *Id.* The information available to an officer at primary does not generally include information relating to past border searches of electronic devices. *Id.*

19. If CBP has advance information about travelers or merchandise, CBP compares the advance information against law enforcement and intelligence information and conducts risk assessments to identify travelers or merchandise that warrant additional scrutiny, and a "lookout" can be placed in the TECs system to advise officers to perform additional scrutiny. Howe Decl. ¶ 11.

20. CBP has little to no advance travel information about individuals traveling across land ports of entry. Howe Decl. ¶33.

21. The vast majority of border searches of electronic devices are basic searches that may be as short as a matter of minutes and that may involve briefly scrolling through the device. Howe Decl. ¶

31. In many instances, a brief, basic search is sufficient to alleviate – or heighten – concerns presented during a border inspection. *Id.*

22. Given the volume of travelers that CBP processes, and in order to ensure efficiency, if based on his or her extensive training and experience, a CBP officer determines that additional scrutiny beyond the brief initial encounter is warranted, the traveler will be referred for a continuation of their inspection, often referred to as “secondary” or “secondary inspection.” Howe Decl. ¶ 13. A secondary inspection is a continuation of the border inspection and an officer may refer any traveler to secondary inspection. *Id.*

23. At secondary, the CBP officer may run law enforcement queries through TECS and other CBP systems. Howe Dec. ¶ 13. The information available to officers at secondary includes the same types of information available at primary, but may also include additional records relating to prior encounters between the traveler and CBP. Howe Decl. ¶13.

24. CBP shares its border search authority with ICE whose HSI Special Agents are also designated as customs officers and immigration officers, in addition to being criminal investigators. Where circumstances warrant, CBP Officers may notify ICE HSI of a matter encountered during the course of a border inspection and ICE HSI agents may engage in additional follow-up investigation, particularly where the matter may be a candidate for criminal prosecution Howe Decl. ¶ 18; Denton Decl. ¶ 12.

25. HSI does not undertake border searches to uncover evidence of crimes that lack a nexus to the border. Denton Decl. ¶ 10. However, during a border search HSI Special Agents may encounter evidence of crimes that have no border nexus and may share the information with the agency responsible for enforcing or administering the applicable law or, as federal law enforcement officers generally empowered to enforce federal criminal law, act on it themselves. *Id.*

26. Prior to conducting a border search, HSI Special Agents can review information on a traveler contained in various government systems, including CBP's record systems and in ICE's Investigative Case Management System (ICM). Denton Decl. ¶ 14.

27. ICM is a system that enables ICE personnel to create an electronic case file that organizes and links all records and documents associated with an investigation, so they are easily accessible from a single location and enables personnel to link records to multiple investigations. Denton Decl. ¶ 14.

28. When a border search is conducted, HSI Special Agents must record the occurrence of a search in ICE's Investigation Case Management System (ICM). Denton Decl. ¶ 15. Special Agents can also record in ICM their impressions of the search or notable observations. *Id.*

29. ICM does not contain the forensic copies of the data on any electronic device, which are stored separately. Denton Decl. ¶ 15. ICM only contains the descriptions that a Special Agent may make of what is observed during a search. *Id.* These federal records are maintained in accordance with section 8.5(1)(b) of ICE Directive 10044.1. *Id.*

30. In FY 2017, CBP conducted 30,524 border searches of electronic devices and processed more than 397 million arriving international travelers; only approximately 0.007% of arriving travelers had their devices searched. Less than 3,500 of those searches were advanced searches. *See* Stipulated Facts 13; Response to Interrog. 6. (Ex. I). In that same year, ICE conducted only 681 advanced searches. Stipulated Facts 15.

Warrantless Border Searches of Electronic Devices Support Defendants' Mission

31. All persons, conveyances, cargo, baggage, personal effects and merchandise of every description may be subject to a border inspection, inbound or outbound. Howe Decl. ¶ 21. This may include things as varied as a shipping container, a mobile home, a suitcase, or a purse, along with any items these things might contain. *Id.*

32. As international travelers carry more electronic devices, there is a greater likelihood that information that was previously maintained in hard copy form, and easily accessible to CBP Officers, is now maintained electronically. Howe Decl. ¶ 26.

33. Electronic devices themselves are merchandise and can contain both merchandise and evidence relating to merchandise. There is a myriad of electronic devices, such as computers, phones, tablets, flash drives, and SD Cards, which can all be encountered at the border. Denton Decl. ¶ 7; Howe Decl. ¶¶ 23, 25.

34. Electronic border device searches advance the Defendants interest in stopping contraband because electronic devices can contain illegal goods just as easily as any other container. *See* Howe Decl. ¶¶ 23, 39; Denton Decl. ¶¶ 7-8, 16.

35. Electronic devices can contain many types of “digital contraband” such as child pornography, classified information, and counterfeit media. *See* Howe Decl. ¶ 23.

36. Electronic devices can also contain evidence of contraband, such as child pornography or items that violate intellectual property rights; classified information; export controlled material, drug trafficking, firearm smuggling, and export control violations. Howe Decl. ¶ 23-24, 28, 30; Denton Decl ¶¶ 24-27

37. Defendants’ searches of electronic devices at the border have successfully uncovered threats to national security, information pertaining to terrorism, illegal activities, contraband, and the inadmissibility of people and things. Howe Decl. ¶¶ 27-30; Denton Decl. ¶¶ 16, 24-27.

38. There have been numerous instances where CBP conducted searches without any advance information or suspicion and found evidence that revealed threats to national and/or border security. Howe Decl. ¶ 28.

39. There have been numerous instances where CBP conducted searches without any advance information or suspicion and found evidence that contradicted an individual’s state purpose for travel to the United States. Howe Decl. ¶ 29.

40. There have been numerous instances where CBP conducted searches without any advance information or suspicion and found evidence that could be used to support a criminal prosecution, such as child pornography, narcotics. Howe Decl. ¶ 30.

41. Electronic devices can also contain information that facilitates the execution of the non-criminal aspects of CBP's mission, which includes the enforcement of civil and administrative legal requirements. Howe Decl. ¶ 30.

42. Border search authority is a crucial tool and requiring a warrant for all border searches of electronic devices would significantly impede CBP's and ICE's missions. Howe Decl. ¶¶ 26, 32; Denton Decl. ¶¶ 18, 23-27.

43. Due to the differences between a typical law enforcement encounter and the border, it is highly unlikely that probable cause exists in the border context. First, a border search is generally not a search where the places and things to be searched can be particularly described in advance, as required in a warrant, but is a search of the individual and her belongings as she chooses to present them at the border. Second, the things to be searched at the border are not those identified, described, and targeted by the government, but whatever the traveler chooses to carry with her across the border between nations. Denton Decl ¶ 22; Howe Decl. ¶¶ 33-34.

44. A warrant necessarily requires advance information to support the probable cause determination, requires the time and deliberateness associated with review by a neutral magistrate, and requires the identification of a specific person or thing to be searched and the particular crime that is implicated. In a border environment, such advance information necessary to support probable cause for search is often minimal. Howe Decl. ¶ 34.

45. A warrant requirement is impractical, if not impossible, for the government to obtain because the what, where, how, and when she presents herself and her possessions at the border is generally not knowable to the government in advance. Denton Decl ¶ 22; Howe Decl. ¶¶ 34.

46. Requiring a warrant for electronic devices at the border would have serious consequences for border security by creating a category of, and a container for, merchandise immune from border search. Such an obvious loophole in the ability of the United States to patrol its borders would create a safe-haven for contraband and evidence and inevitably result in exploitation by criminals, terrorists, and transnational criminal organizations to smuggle merchandise, contraband, and evidence of criminal conspiracies into and out of the United States. Denton Decl. ¶¶ 18, 23; Howe Decl. ¶ 32, 35

47. A warrant requirement would obviate the deterrent effect of border searches when it comes to electronic devices and incentivize criminals to store contraband or other evidence of illegal goods on their electronic devices. *See* Howe Decl. ¶¶ 38, 43; Denton Decl. ¶¶ 18, 23.

48. A warrant requirement would impose entirely unknown logistical and resource requirements on Defendants. Howe Decl. ¶¶ 34, 36; Denton Decl. ¶¶ 19-22.

49. A warrant requirement for border searches of electronic devices would likely impede CBP's ability to expeditiously complete certain border inspections; would likely prevent CBP from detecting electronic contraband; and would deprive the federal government of crucial information, including terrorism related information, that informs admissibility determinations relating to both people and goods. Howe Decl. ¶¶ 32, 36- 38.

50. A warrant requirement would threaten the security of this country. Defendants have on numerous occasions interdicted contraband and criminals through use of device border searches, and in most, if not all, of these instances the Government did not have a warrant or probable cause to conduct the search at issue. *See* Howe Decl. ¶ 27-30; Denton Decl. ¶¶ 24-27.

FACTS RELATING TO INDIVIDUAL PLAINTIFFS:

51. Out of the eleven Plaintiffs, seven have had their electronic devices searched at the border only once (Plaintiffs Ghassan Alasaad, Allababidi, Bikkannavar, Gach, Shilby, Wright, and Zorri). *See* Pls. SUMF ¶¶ 120-149. (ECF 90-2)

52. Four have had their electronic devices searched at the border more than once (Plaintiffs Merchant, Nadia Alasaad, Dupin and Kushkush). *See* Pls. SUMF ¶¶ 121, 123, 129, 130, 134, 135, 137, 140, 141, 142 (ECF 90-2).

53. Except for Plaintiff Merchant, none of the Plaintiffs have had their electronic devices searched since August 2017. *See* Pls. SUMF ¶¶ 120-149. (ECF 90-2)

54. Plaintiff Merchant did have her electronic device manually searched in September, 2018 but she has travelled internationally at least five times since her most recent search and has not been searched during any of those trips. *See* Ex. J, Merchant Resp. to Interrogs. 1, 4; Merchant Suppl. Resp. to Interrogs 1, 4, 7.

55. Defendants deleted all copies of Plaintiff Wright’s data. Declaration of Jenny Tsang, (Ex. L).

**DEFENDANTS’ RESPONSE TO PLAINTIFFS’ STATEMENT
OF UNDISPUTED MATERIAL FACTS**

I. Defendants’ Policies and Practices on Border Searches and Confiscations of Travelers’ Electronic Devices

A. CBP Screening

1. U.S. Customs and Border Protection (“CBP”) officers conduct primary inspections of every person who crosses the border into the United States at a port of entry. Exh. 13 (CBP 30(b)(6) depo.) at 85:3–12.

Response: Dispute the characterization as a “primary” inspection here, but admit that CBP officers conduct inspections of every person who crosses the border into the United States at a port of entry. *Id.*

2. During primary inspections, CBP officers must determine whether a traveler seeking entry is admissible to the United States. U.S. citizens are by definition admissible. Lawful permanent residents, with some exceptions, are also by definition admissible. Officers must also determine whether the traveler is carrying goods subject to customs rules, such as prohibited contraband. Exh. 13 (CBP 30(b)(6) depo.) at 35:2–5, 80:4–8, 85:3–12 & errata pages.

Response: Dispute that this determination only occurs during “primary” inspection and also dispute their characterization of the term “lawful permanent resident.” Admit that U.S. citizens are by definition admissible once they establish their identity and citizenship to the satisfaction of the inspecting officer. *Id.* at 35:4-5. Aliens lawfully admitted for permanent residence in the United States are also not regarded as seeking admission for purposes of immigration laws unless certain criteria apply. *See* 8 U.S.C. §1101(a)(13)(C). Further dispute the characterization that Officers are determining “whether the traveler is carrying goods subject to customs rules, such as prohibited contraband;” all goods crossing the border are subject to inspection by customs officers. *See* 19 U.S.C. § 1401(c); *see also* Exh. 13 (CBP 30(b)(6) depo.) at 35:15-36::17

3. If a CBP officer at primary inspection decides that a traveler warrants further screening, the officer will refer the traveler to secondary inspection. Exh. 13 (CBP 30(b)(6) depo.) at 87:6–18.

Response: Dispute that this statement correctly characterizes the cited deposition testimony. Admit that a CBP officer at primary inspection may refer a traveler for additional scrutiny if they require further time for processing.

4. Some travelers are randomly selected for referral to secondary inspection. Exh. 18 (CBP Briefing for Senate Committee) at Bates 282.

Response: No dispute.

5. During secondary inspections, when deciding whether to search a traveler’s device, CBP officers consider past border searches of electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 122:4–13.

Response: Dispute that this statement correctly characterizes the cited deposition testimony which makes clear that a CBP officer considers a number of factors in deciding whether to search a traveler’s device which may include past searches. *Id.* at

122:4-20.

B. The CBP Policy

6. CBP's border searches and confiscations of electronic devices are governed by CBP Directive No. 3340-049A, dated January 4, 2018 (the "CBP Policy"). Exh. 19 (CBP 2018 Directive) at § 11, Bates 124.

Response: Dispute the characterization of the cited policy. Admit that CBP Directive No. 3340-049A, dated January 4, 2018 (the "CBP Policy") provides guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in electronic devices.

7. In an "advanced" or "forensic" search, an officer connects external equipment to a traveler's electronic device, with a wired or wireless connection, in order to access, review, copy, and/or analyze the contents of the device. Exh. 46 (Stipulations) at ¶ 1; Exh. 19 (CBP 2018 Directive) at § 5.1.4, Bates 117; Exh. 20 (ICE Broadcast) at Bates 1266; Exh. 14 (ICE 30(b)(6) depo.) at 54:14-23.

Response: Dispute that plaintiffs correctly characterized the referenced Stipulation and refer the Court to the Stipulation and CBP 2018 Directive for an accurate statement.

Do not dispute that an advanced search is defined in both the Stipulation and CBP 2018 Directive as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."

8. In a "basic" or "manual" search, an officer reviews the content of a traveler's electronic device without using external equipment. Exh. 19 (CBP 2018 Directive) at § 5.1.3, Bates 116; Exh. 14 (ICE 30(b)(6) depo.) at 54:14-55:3.

Response: Dispute that the CBP 2018 Directive uses the term "manual" to describe a search. Exh 19 at § 5.1.3 (describing a basic search) Do not dispute that the term

“manual” is sometimes used to describe a basic search.

9. The CBP Policy allows advanced searches of electronic devices based on either “reasonable suspicion of activity in violation of the laws enforced or administered by CBP” or a “national security concern.” Exh. 19 (CBP 2018 Directive) at § 5.1.4, Bates 117.

Response: No dispute.

10. The CBP Policy allows basic searches of electronic devices without any suspicion. Exh. 19 (CBP 2018 Directive) at § 5.1.3, Bates 116.

Response: No dispute.

11. The CBP Policy allows officers to retain travelers’ electronic devices for on-site or off-site searches, which “ordinarily” should not exceed five days, but can be prolonged with supervisory approval based on “extenuating circumstances.” Exh. 19 (CBP 2018 Directive) at §§ 5.4.1–5.4.1.1, Bates 119.

Response: No dispute.

12. The CBP Policy places no ultimate limit on how long a device can be kept for search. Exh. 13 (CBP 30(b)(6) depo.) at 223:21–224:7.

Response: No dispute.

13. The CBP Policy permits CBP to retain information from a traveler’s device that is related to “immigration, customs, and other enforcement matters,” even if there is no probable cause to suspect a violation of law. Exh. 19 (CBP 2018 Directive) at § 5.5.1.2, Bates 121.

Response: No dispute.

14. The CBP Policy permits officers to share information retained from electronic devices with federal, state, local, and foreign law enforcement agencies. Exh. 19 (CBP 2018 Directive) at § 5.5.1.3, Bates 122.

Response: No dispute.

15. CBP does not know how long other government entities keep the information they

receive from CBP's border searches of electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 200:2–12.

Response: No dispute.

16. CBP does not monitor whether other government entities impermissibly retain the information CBP shares from border searches of electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 203:7–204:3.

Response: No dispute.

C. The ICE Policy

17. U.S. Immigration and Customs Enforcement's ("ICE") border searches and confiscations of electronic devices are governed by ICE Directive No. 7–6.1 (also known as ICE Policy 10044.1), dated August 18, 2009, as superseded in part by an ICE/Homeland Security Investigations ("HSI") Broadcast, dated May 11, 2018 (collectively, the "ICE Policy"). Exh. 21 (ICE 2009 Directive) at Bates 260–69; Exh. 20 (ICE Broadcast) at Bates 1266–67; Exh. 14 (ICE 30(b)(6) depo.) at 149:10–20,187:21–188:2.

Response: No dispute.

18. The ICE Policy allows advanced searches of electronic devices with reasonable suspicion. Exh. 20 (ICE Broadcast) at Bates 1266–67.

Response: No dispute.

19. The ICE Policy allows basic or manual searches of electronic devices without any suspicion. Exh. 21 (ICE 2009 Directive) at § 6.1, Bates 261.

Response: Dispute that the ICE policy uses the term "manual" to describe a search. The correct term is basic. *Id.*

20. When CBP turns an electronic device over to ICE for a search, ICE policy applies. Exh. 21 (ICE 2009 Directive) at § 6.2, Bates 261; Exh. 19 (CBP 2018 Directive) at § 2.7, Bates 114.

Response: No dispute.

21. The ICE Policy allows agents to take and retain travelers' electronic devices for on-site or off-site searches. Exh. 21 (ICE 2009 Directive) at § 8.1(4), Bates 263. The ICE Policy states that such searches should "generally" be completed within 30 days, but can be prolonged with supervisory approval. *Id.* at § 8.3(1), Bates 263–64.

Response: Dispute plaintiffs' characterization of the ICE policy which requires agents "to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time give the facts and circumstances of the particular search" and refer the Court to the policy (Exh 21 §8.3) for an accurate statement.

22. The ICE Policy permits ICE to retain information from travelers' devices that are "relevant to immigration, customs, and other law enforcement matters." Exh. 21 (ICE 2009 Directive) at § 8.5(1)(b), Bates 266.

Response: No dispute that the ICE policy permits retention of information to the extent authorized by law and if retention is consistent with the privacy and data protection policies of the system in which the information is retained. *Id.*

23. The ICE Policy states that copies of information from travelers' devices that are "determined to be of no relevance to ICE" must be destroyed, and the destruction must be documented. Exh. 21 (ICE 2009 Directive) at § 8.5(1)(e), Bates 267.

Response: No dispute.

24. The ICE Policy permits ICE to share information retained from electronic devices with federal, state, local, and foreign law enforcement agencies. Exh. 21 (ICE 2009 Directive) at § 8.5(1)(c), Bates 266.

Response: No dispute that the ICE policy allows sharing of information in accordance with applicable law and policies.

D. Border Screening Databases

1. CBP's TECS

25. TECS is CBP's main database. Exh. 13 (CBP 30(b)(6) depo.) at 46:9–11. It facilitates the maintenance and sharing of law enforcement records. *Id.* at 47:5–15.

Response: No dispute.

26. TECS includes information about prior encounters between CBP officers and travelers at the U.S. border. Exh. 13 (CBP 30(b)(6) depo.) at 119:7–17.

Response: No dispute.

27. TECS includes “lookouts” created by CBP or other government agencies. Exh. 13 (CBP 30(b)(6) depo.) at 98:20–99:7; Exh. 14 (ICE 30(b)(6) depo.) at 211:14–22.

Response: No dispute.

28. A “lookout” is an alert about a traveler or vehicle that is entered into a database by CBP, ICE, or another law enforcement agency. Exh. 13 (CBP 30(b)(6) depo.) at 97:5–11; Exh. 14 (ICE 30(b)(6) depo.) at 205:2–23; Exh. 22 (CBP 2018 PIA) at Bates 177.

Response: No dispute

29. At primary inspection, CBP officers query TECS to identify “lookouts” and recent border crossings. Exh. 13 (CBP 30(b)(6) depo.) at 85:14–86:24, 93:12–19.

Response: No dispute.

30. If a traveler has a “lookout,” the primary inspection CBP officer will refer the traveler to secondary inspection. Exh. 13 (CBP 30(b)(6) depo.) at 101:25–102:12; Exh. 14 (ICE 30(b)(6) depo.) at 206:19–207:19. A CBP officer may also refer the traveler to ICE. Exh. 14 (ICE 30(b)(6) depo.) at 205:2–23, 207:22–208:3, 209:6–210:2.

Response: Dispute characterization that all travelers with a “lookout” *will* be referred to secondary inspection. Admit that a “lookout” *may* result in a referral to secondary inspection.

31. “Lookouts” can be a reason why some travelers are subjected to border searches of their electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 103:15–104:2, 208:5–10.

Response: Dispute plaintiff’s characterization that “travelers are subjected to border searches” but admit that “lookouts” can be a reason why CBP conducts a border search of an electronic device.

32. “Lookouts” last as long as CBP deems them pertinent. Exh. 13 (CBP 30(b)(6) depo.) at 101:19–23.

Response: No dispute.

33. CBP officers use TECS to document border searches of electronic devices. Exh. 13 (CBP 30(b)(6) depo.) at 90:15–21, 119:18–21. This includes the officers’ reasons for search, *id.* at 125:19–126:18, 151:5–11, and information the officers discover that they deem of law enforcement benefit, *id.* at 169:19–21. *See also* Exh. 22 (CBP 2018 PIA) at Bates 186.

Response: No dispute.

34. During secondary inspections, CBP officers consider information in TECS, including information about prior border screenings. Exh. 13 (CBP 30(b)(6) depo.) at 117:7–119:21.

Response: No dispute.

35. When ICE agents are deciding whether to conduct a border search of an electronic device, they have access to information in TECS. Exh. 14 (ICE 30(b)(6) depo.) at 90:24–92:5.

Response: No dispute.

2. CBP’s Automated Targeting System

36. CBP’s Automated Targeting System (“ATS”) uses “rules” to conduct risk assessments that “flag[]” certain travelers for “additional inspection.” Exh. 13 (CBP 30(b)(6) depo.) at 107:7–25. *See also id.* at 104:11–14, 106:8–16; Exh. 23 (CBP 2017 ATS PIA) at Bates 997, 999, 1003.

Response: No dispute.

37. When assessing risk, ATS uses information from TECS. Exh. 13 (CBP 30(b)(6) depo.) at 107:22–25. *See also* Exh. 23 (CBP 2017 ATS PIA) at Bates 1000.

Response: No dispute.

38. ATS provides CBP officers with access to dozens of other government databases. Exh. 23 (CBP 2017 ATS PIA) at Bates 997–99.

Response: No dispute.

39. If ATS flags a traveler, then a CBP officer conducting a primary inspection must refer the traveler to secondary inspection. Exh. 13 (CBP 30(b)(6) depo.) at 109:4–13.

Response: Dispute characterization and state that a CBP officer’s reason for referring a traveler to secondary inspection may be based upon a review of the results of an ATS risk assessment.

40. If an advanced search of an electronic device yields information that a CBP officer deems of law enforcement benefit, then the officer will copy it into ATS. Exh. 13 (CBP 30(b)(6) depo.) at 104:18–105:2; Exh. 22 (CBP 2018 PIA) at Bates 184, 186; Exh. 23 (CBP 2017 ATS PIA) at Bates 1034; Exh. 27 (DHS OIG 2018 Report) at Bates 975.

Response: Dispute characterization and state that articulated in the ATS PIA, Bates 0996, a CBP Officer is authorized to include information from the border search of an electronic device in ATS if the subject of the search is of significant law enforcement, counterterrorism, or national security concerns.

41. ATS stores copies of data from travelers’ devices, not officers’ narrative descriptions of that data. Exh. 13 (CBP 30(b)(6) depo.) at 190:10–19.

Response: No dispute.

42. ATS stores copies of data from travelers’ devices for 15 years or “the life of the law enforcement matter,” whichever is longer. Exh. 23 (CBP 2017 ATS PIA) at Bates 1037.

Response: No dispute.

43. ATS may use the information copied from a traveler's device to flag the traveler for heightened screening in the future. Exh. 13 (CBP 30(b)(6) depo.) at 114:10–18, 115:12–25; Exh. 22 (CBP 2018 PIA) at Bates 184; Exh. 23 (CBP 2017 ATS PIA) at Bates 1034.

Response: No dispute that Officers may flag a traveler for additional scrutiny on the basis of information maintained in ATS.

44. When ICE agents decide whether to conduct a border search of an electronic device, they have access to ATS. Exh. 14 (ICE 30(b)(6) depo.) at 99:4–10.

Response: No dispute.

3. ICE's Investigative Case Management

45. ICE operates a database called Investigative Case Management ("ICM"). Exh. 14 (ICE 30(b)(6) depo.) at 163:20–164:4.

Response: No dispute.

46. ICM contains (a) "reports of investigation," and (b) "subject records," which identify people and things that are connected to investigations. Exh. 14 (ICE 30(b)(6) depo.) at 164:13–165:8.

Response: No dispute.

47. ICM contains nearly all of ICE's case information. Exh. 14 (ICE 30(b)(6) depo.) at 160:3–13.

Response: No dispute.

48. When ICE agents decide whether to conduct border searches of electronic devices, they have access to ICM information. Exh. 14 (ICE 30(b)(6) depo.) at 164:5–12.

Response: No dispute.

49. ICM information that can be relevant to whether to conduct a border search of an electronic device includes prior encounters between ICE and travelers at the border, including

whether travelers were subjected to device searches. Exh. 14 (ICE 30(b)(6) depo.) at 166:13–168:14.

Response: No dispute.

50. If an ICE agent conducts a border search of an electronic device, they may use an ICM report of investigation to store information about what they found. Exh. 14 (ICE 30(b)(6) depo.) at 169:10–22. ICM contains an agent’s descriptions of data in a traveler’s device, but not the data itself. *Id.* at 172:5–14. This may include, for example, a “verbatim transcript of a conversation,” or a “summary” of a conversation or a photograph. *Id.* at 172:15–174:11.

Response: No dispute.

51. ICM information about the contents of travelers’ devices can be relevant to whether to conduct a future border search of an electronic device. Exh. 14 (ICE 30(b)(6) depo.) at 174:12–24.

Response: No dispute.

II. The Frequency of Border Searches and Confiscations of Electronic Devices

A. Defendants’ Statistical Data

52. CBP conducted the following total number of border searches of electronic devices during each fiscal year (“FY”) from 2012 through 2018:

- FY 2012: 5,085
- FY 2013: 5,709
- FY 2014: 6,029
- FY 2015: 8,503
- FY 2016: 19,051
- FY 2017: 30,524
- FY 2018: 33,295

Exh. 46 (Stipulations) at ¶ 13.

Response: No dispute.

53. CBP conducted the following number of basic searches of electronic devices at the border during each fiscal year from 2012 through 2018:

- 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 September 15, 2018): 28,429¹

Exh. 26 (Defs. Interrog. Responses) at #6.

Response: No dispute.

54. CBP conducted the following number of advanced searches of electronic devices at the border during each fiscal year from 2012 through 2018:

- 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 September 15, 2018): 3,485

Exh. 26 (Defs. Interrog. Responses) at #6.

Response: No dispute.

55. CBP conducted the following number of confiscations of travelers' electronic devices after they left ports of entry during each fiscal year from 2012 through 2018:

- FY 2012: 8
- FY 2013: 36
- FY 2014: 32
- FY 2015: 21
- FY 2016: 131
- FY 2017: 200
- FY 2018 (through September 15, 2018): 172

Exh. 26 (Defs. Interrog. Responses) at #6.

Response: Dispute the characterization of the fact because the wording differs from the wording used in Defendants' Response to Interrogatory 6. Defendants do not dispute that that CPB estimated that it "detained the [above] number of electronic devices after a traveler departed the port of entry or other location of inspection in each of the identified fiscal years."

B. Defendants' Statistics Do Not Reflect All Border Searches and Confiscations of Electronic Devices

56. ICE does not maintain records of the number of basic searches of electronic devices that it conducts. Exh. 46 (Stipulations) at ¶ 14.

Response: Dispute that this is a material fact as the number of basic searches conducted by ICE or whether ICE records those numbers is not material to the constitutionality of border searches of electronic devices.

57. ICE agents may conduct basic searches of electronic devices. Exh. 29 (DHS 2009 PIA) at Bates 224.

Response: No dispute.

58. ICE does not maintain records of the number of times it detains electronic devices after travelers leave ports of entry. Exh. 14 (ICE 30(b)(6) depo.) at 330:2–10.

Response: Dispute plaintiffs' characterization of the cited testimony. ICE records every instance that an electronic device is detained for a border search; it does not record those occurrences in a manner that permits for aggregable statistics. *Id.* at 331:6 – 332:6.]

Further dispute this is a material fact as the number of basic searches conducted by ICE or whether ICE records those numbers is not material to the constitutionality of border searches of electronic devices.

59. CBP determines the number of border searches of electronic devices in a given period by calculating the number of closed or completed Electronic Media Reports (“EMRs”). Exh. 26 (Defs. Interrog. Responses) at #11. EMRs are sometimes called “IOEMs.” Exh. 13 (CBP 30(b)(6) depo.) at 201:7–9.

Response: No dispute, except to dispute this is a material fact.

60. CBP officers sometimes do not complete EMRs after conducting border searches of electronic devices. Exh. 27 (DHS OIG 2018 Report) at Bates 973, 978; Exh. 13

(CBP 30(b)(6) depo.) at 248:18–249:9.

Response: Do not dispute that the 2018 DHS OIG report found, in the period of examination, that CBP officers sometimes did not complete EMRs. Further dispute that this is a material fact.

61. For example, on August 28, 2017, CBP officers searched the smartphone they seized from Plaintiff Nadia Alasaad’s bag. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 73–74, 76. Defendants have no records, including EMRs, documenting that search. Exh. 26 (Defs. Doc. Responses) at #17.

Response: Dispute the inference being drawn by the fact that CBP does not have any records documenting that alleged search and further dispute that this is a material fact.

62. When CBP officers do not fill out EMRs for border searches of electronic devices, those searches are not included in CBP’s calculation of the total number of searches for that period. Exh. 26 (Defs. Interrog. Responses) at #11; Exh. 13 (CBP 30(b)(6) depo.) at 251:3–15.

Response: Dispute that this is a material fact.

III. Privacy Implications of Device Searches

A. The Sensitivity of Content in Travelers’ Devices

63. Electronic devices carried by travelers, such as smartphones or laptops, can contain a very large volume of information. Exh. 13 (CBP 30(b)(6) depo.) at 161:25–162:3; Exh. 14 (ICE 30(b)(6) depo.) at 212:21–213:3.

Response: No dispute.

64. Travelers carry electronic devices that contain many different kinds of information, such as photos, contacts, emails, and text messages, and the devices may reveal such things as prescription information, information regarding employment, travel history, and browsing history. Exh. 13 (CBP 30(b)(6) depo.) at 161:21–24, 164:3–13, 167:12–17, 191:10–14;

Exh. 14 (ICE 30(b)(6) depo.) at 213:5–8.

Response: No dispute.

65. A CBP training document describes border searches of electronic devices as “very sensitive.” Exh. 31 (Pilot Program for CBP 2018 Directive) at Bates 143.

Response: No dispute.

66. ICE recognizes that electronic devices have the capacity to “store sensitive information.” Exh. 29 (DHS 2009 PIA) at Bates 231.

Response: No dispute.

B. The Invasiveness of Manual and Forensic Device Searches

67. Basic searches can access content from allocated space physically resident on an electronic device that is accessible using the native operating system of the device, including but not limited to its native graphical user interface and/or touchscreen. Exh. 46 (Stipulations) at ¶ 2.

Response: No dispute.

68. Basic searches can extend to any allocated file or information that is resident on the device and accessible using the device’s native operating system. Exh. 46 (Stipulations) at ¶ 4.

Response: No dispute.

69. Separate from the primary content stored on them, some electronic devices may also store data related to that content, such as the date and time associated with the content, usage history, sender and receiver information, or location data. That content may be revealed during a basic search, depending on the type of device, the operating system, the relevant settings, and the applications used to create and/or maintain the data. Exh. 46 (Stipulations) at ¶ 5.

Response: No dispute.

70. When conducting a basic search, officials are able to use the native search functions in the native operating system of the device, such as a key word search tool, if there is

one. Exh. 46 (Stipulations) at ¶ 3.

Response: No dispute.

71. A device's internal search tools can be used to search for particular words and images. Exh. 14 (ICE 30(b)(6) depo.) at 214:24–216:10, 216:25–217:4, 218:9–20, 219:16–221:11.

Response: No dispute.

72. Depending on the equipment, procedures, and techniques used, advanced searches of electronic devices are generally capable of revealing everything a basic search may reveal. Exh. 46 (Stipulations) at ¶ 6.

Response: No dispute, except dispute that it is material.

73. An advanced search of an electronic device, depending on the equipment, procedures, and techniques used, may be capable of revealing deleted or other data in unallocated storage space and password-protected or encrypted data. Exh. 46 (Stipulations) at ¶ 8. *See also* Exh. 13 (CBP 30(b)(6) depo.) at 298:3–17.

Response: No dispute.

74. An advanced search of an electronic device may be able to copy all information physically resident on the device or may be limited to only certain files, depending on the search equipment, procedures, and techniques used. Exh. 46 (Stipulations) at ¶ 12. *See also* Exh. 13 (CBP 30(b)(6) depo.) at 205:13–23.

Response: No dispute.

75. If information from the internet is cached on a device, such as web-based email, and the device is disconnected from the internet, border officers can still search the cached information. Exh. 14 (ICE 30(b)(6) depo.) at 222:9–223:15; Exh. 13 (CBP 30(b)(6) depo.) at 186:2–24.

Response: No dispute.

76. Some CBP officers may have accessed cloud-based content during searches of electronic devices, even after issuance of an April 2017 memorandum requiring that officers disable network connectivity prior to search, because more than one-third of EMRs lacked a statement confirming that the device's data connection had been disabled. Exh. 27 (DHS OIG 2018 Report) at Bates 979–980.

Response: Do not dispute that the 2018 DHS OIG report concluded that based on EMRs reviewed in the stated time period that some CBP officers did not document that they had disabled network connectivity prior to a search during the time period examined, which was after issuance of an April 2017 memorandum requiring that officers disable network connectivity prior to search. Dispute that this is a material fact.

C. Privacy Risks From Retention of Information

77. To the extent consistent with applicable system of records notices, ICE and CBP can retain information from a device in any of their record keeping systems when an electronic device search reveals information officers deem relevant to immigration, customs, or other laws enforced by the Department of Homeland Security. Exh. 46 (Stipulations) at ¶ 10.

Response: No dispute.

78. ICE generally stores information from travelers' devices in ICE's Investigative Case Management System, and the rules for that database do not limit storage of this information, beyond the requirement of relevance to immigration, customs, or other law enforcement matters. Exh. 14 (ICE 30(b)(6) depo.) at 323:16–324:4, 326:18–327:4.

Response: Dispute to the extent this statement suggests that exact or complete electronic copies of an electronic device's data are stored in ICM. Do not dispute that an ICE Special Agent can manually record a narrative description of information observed during a search of an electronic device in ICM. *Id.* at 324:16-325:2; 326:15-

327:4.

79. After a border search of an electronic device, the information contained on the device may be shared with other federal agencies for law enforcement and intelligence purposes. Exh. 13 (CBP 30(b)(6) depo.) at 44:18–45:12, 198:20–199:5; Exh. 30 (ICE 2007 Memorandum) at Bates 1265.

Response: Dispute plaintiffs’ characterization of this fact and refer Court to cited exhibits which make clear that the information sharing is permitted only if the information is related to immigration, customs, and other enforcement matters and if the sharing is consistent with applicable system of record notices. *See* Ex. 19 at 5.5.1.3 and 5.5.1.4; *see also* DHS/CBP/PIA-008(a) Border Searches of Electronic Devices at Bates 0174 (Ex. G); DHS/CBP/PIA-006(e) ATS at Bates 0996 (Ex. K).

80. After a border search of an electronic device, information retained in the TECS database may be shared with other agencies outside of DHS, including local, state, and foreign governments. Exh. 13 (CBP 30(b)(6) depo.) at 83:18–84:17; 198:11–19.

Response: Dispute plaintiffs’ characterization of this fact and refer Court to cited exhibits which make clear that the information sharing is permitted only if the information is related to immigration, customs, and other enforcement matters and if the sharing is consistent with applicable system of record notices.

IV. Government Interests

A. Defendants’ Asserted Purposes

81. CBP and ICE assert authority to conduct warrantless or suspicionless border searches of electronic devices to enforce hundreds of federal laws. Exh. 19 (CBP 2018 Directive) at Bates 115; Exh. 22 (CBP 2018 PIA) at Bates 189; Exh. 14 (ICE 30(b)(6) depo.) at 28:4–6.

Response: This is a conclusion of law and not a material fact. If deemed a material fact, no dispute.

82. CBP's asserted purposes in conducting warrantless or suspicionless border searches of electronic devices include general law enforcement, *i.e.*, finding potential evidence of illegal activity beyond violations of immigration and customs laws. Exh. 26 (Defs. Interrog. Responses) at #1 (“[B]order searches of electronic devices are conducted in furtherance of ... law enforcement[] and homeland security responsibilities and to ensure compliance with ... other laws that Defendants are authorized to enforce and administer. ... They are a crucial tool for detecting evidence relating to terrorism and other national security matters... They can also reveal information about financial and commercial crimes ...”). *See also* Exh. 19 (CBP 2018 Directive) at § 1, Bates 113; Exh. 13 (CBP 30(b)(6) depo.) at 20:19–21:9, 32:23–33:6; Exh. 33 (CBP “Tear Sheet”) at Bates 163 (“domestic law enforcement”); Exh. 23 (CBP 2017 ATS PIA) at Bates 1034 (“other enforcement matters”) & 1035 (“other laws enforced by CBP”); Exh. 27 (DHS OIG 2018 Report) at Bates 975 (“any violation of laws”), 981 (“law enforcement-related information”), 982 (use of “new technologies to commit crimes”); Exh. 34 (CBP Written Statement for the Record for Senate Homeland Security Committee, July 11, 2018) at Bates 277 (use of “new technologies to commit crimes”); Exh. 35 (CBP Instructor Guide—P180C) at Bates 1279.

Response: Dispute plaintiffs’ characterization that CBP’s asserted purpose for conducting border searches include general law enforcement. The cited exhibits demonstrate that CBP officers’ searches are related to the agency’s broad law enforcement and national security responsibilities. *See also* 6 U.S.C. § 211.

83. ICE’s asserted purposes for warrantless or suspicionless border searches of electronic devices include general law enforcement, *i.e.*, finding potential evidence of illegal activity beyond violations of immigration and customs laws. Exh. 26 (Defs. Interrog. Responses) at #1; Exh. 21 (ICE 2009 Directive) at § 4, Bates 261 (“other Federal laws at the border”); Exh. 30 (ICE 2007 Memorandum) at Bates 1264 (“anything that may be evidence of a crime”); Exh.

14 (ICE 30(b)(6) depo.) at 35:15–17, 36:23–37:5, 40:10–20.

Response: Dispute plaintiffs’ characterization that ICE’s asserted purpose for conducting border searches include general law enforcement and for finding illegal activity beyond violations of immigration and customs laws. The cited exhibits demonstrate that ICE agents’ searches are related to the agency’s broad law enforcement and national security responsibilities. *See also* 6 U.S.C. §§ 202, 251-52

84. ICE asserts that agents may conduct a warrantless or suspicionless border search of the electronic device of a traveler:

a. Who is suspected of violating tax laws, to find emails reflecting the tax law violations. Exh. 14 (ICE 30(b)(6) depo.) at 29:4–8, 31:5–12.

b. Who is suspected of hiding assets in bankruptcy, to find emails reflecting the hiding of assets. *Id.* at 33:4–22.

c. Who is an executive of a company suspected of criminally dumping toxins into a river, to find emails reflecting the illegal dumping. *Id.* at 31:14–23, 32:2–8.

d. Who is suspected of violating consumer protection laws, to find evidence reflecting the consumer protection law violations. *Id.* at 32:10–33:2.

e. Who is suspected of money laundering, to find emails or other evidence reflecting money laundering, including the creation of corporations and accounts and the structuring of deposits. *Id.* at 41:3–42:13.

Response: Dispute the characterizations of the deposition testimony which make clear that border searches of an individual under any of the above circumstances would only be conducted if ICE was also investigating that individual for violation of a cross-border crime within the jurisdiction of ICE. *Id.* at 52:4-14.

85. CBP and ICE’s asserted purposes in conducting warrantless or suspicionless border searches of electronic devices include finding potential evidence of customs violations,

including evidence of importing or exporting contraband, in contrast to finding contraband itself. Exh. 26 (Defs. Interrog. Responses) at #1 (“detecting evidence relating to . . . human and bulk cash smuggling, contraband, and child pornography”); Exh. 13 (CBP 30(b)(6) depo.) at 62:19–21; Exh. 35 (CBP Instructor Guide—P180C) at Bates 1279 (“evidence related to . . . [h]uman/cash smuggling” and “[n]arcotics and contraband”); Exh. 36 (ICE/HSI Priority Requests) at Bates 93 (“ . . . if an individual is encountered smuggling methamphetamine . . . a border search would be conducted on his devices for co-conspirators”).

Response: No dispute.

86. CBP and ICE’s asserted purposes in conducting warrantless or suspicionless border searches of electronic devices include intelligence gathering. Exh. 13 (CBP 30(b)(6) depo.) at 46:24–47:3, 47:16–48:7; Exh. 23 (CBP 2017 ATS PIA) at Bates 1003, 1034; Exh. 30 (ICE 2007 Memorandum) at Bates 1265 (“intelligence interest[s]”).

Response: Dispute that the cited references support plaintiffs’ characterization of Defendants’ purposes for conducting border searches. Defendants refer the Court to the referenced documents which, for the most part, discuss the agencies’ record keeping systems. In addition, Exh 30 does not state that intelligence gathering is a purpose of border searches. *Id.* at 1264 (stating that the two general objectives of a border search is “to inspect for merchandise imported contrary to law” and “to obtain information or evidence relating to an individual’s admissibility.”); *See also* Defs.’ Response to Pls.’ First Set of Interrog, Interrog. No.1 (Ex. I)

87. CBP’s decisions to conduct warrantless or suspicionless border searches of electronic devices are informed by information or requests from other government agencies. Exh. 26 (Defs. Interrog. Responses) at #17 (“CBP decisions to perform border searches of electronic devices benefit from information provided by other law enforcement agencies”); Exh. 13 (CBP 30(b)(6) depo.) at 75:8–76:5, 76:11–25, 77:13–14, 83:18–84:12; Exh. 37 (CBP Briefing for

Senate Committee) at Bates 288 (“CBP coordinates with FBI”).

Response: No dispute, except to dispute that this is a material fact.

88. ICE’s decisions to conduct warrantless or suspicionless border searches of electronic devices are informed by information or requests from other government agencies. Exh. 26 (Defs. Interrog. Responses) at #17. *See also* Exh. 14 (ICE 30(b)(6) depo.) at 189:9–190:21, 191:18–192:3. These agencies include the Bureau of Alcohol, Tobacco, Firearms and Explosives, Internal Revenue Service, Secret Service, Federal Bureau of Investigation, State Department, state and local police departments and county sheriffs, and foreign law enforcement agencies. Exh. 14 (ICE 30(b)(6) depo.) at 194:13–201:25.

Response: Dispute plaintiffs’ characterization of the cited evidence but do not dispute that the cited evidence shows that ICE makes independent determinations on the necessity for every border search they undertake and that information provided by other law enforcement agencies *may* inform the agency’s decision to conduct a border search of an electronic device. *See also* Exh. 26. at No. 17. Further dispute that this is material.

89. CBP asserts it may conduct warrantless or suspicionless border searches of electronic devices when the subject is someone other than the traveler. Exh. 13 (CBP 30(b)(6) depo.) at 57:3–17 (another person’s crime), 58:6–59:9 (same), 59:11–60:10 (another person’s admissibility).

Response: No dispute except to clarify that CBP has authority to search any traveler at the border and CBP policies permit a basic search of an electronic device with or without suspicion.

90. ICE asserts that warrantless or suspicionless border searches of electronic devices may be conducted when the subject of interest is someone other than the traveler. This includes:

a. When the traveler is a U.S. citizen and ICE is seeking information about a suspected undocumented immigrant. Exh. 14 (ICE 30(b)(6) depo.) at 64:18–65:19.

b. When the traveler is a reporter who is known to have had contact with a suspected terrorist, where there is no suspicion that the reporter engaged in wrongdoing. Exh. 14 (ICE 30(b)(6) depo.) at 56:25–58:14. *See also id.* at 74:14–75:6.

c. When the traveler is a journalist or a scholar with foreign sources who are of interest to the U.S. government. Exh. 14 (ICE 30(b)(6) depo.) at 75:14–25.

d. When the traveler is business partners with someone who is under investigation for tax fraud. Exh. 14 (ICE 30(b)(6) depo.) at 50:15–51:4.

e. When the traveler is a family member of a person under investigation, in conjunction with other factors. Exh. 14 (ICE 30(b)(6) depo.) at 130:16–131:3.

Response: Dispute plaintiffs’ characterization of the cited evidence and clarify that ICE has the authority to search an electronic device of any traveler at the border in furtherance of its mission.

91. CBP and ICE conduct warrantless or suspicionless border searches of electronic devices to advance pre-existing investigations. Exh. 35 (CBP Instructor Guide—P180C) at Bates 1281 (“ongoing INVESTIGATIONS”); Exh. 26 (Defs. Interrog. Responses) at #16 (“the potential for that search to further a particular investigation”); Exh. 14 (ICE 30(b)(6) depo.) at 193:2–15; Exh. 29 (DHS 2009 PIA) at Bates 222.

Response: No dispute.

B. Digital Contraband at the Border

92. Child pornography is primarily transferred into the United States via the internet. Exh. 14 (ICE 30(b)(6) depo.) at 297:9–12.

Response: Dispute that this is a material fact.

93. ICE considers few things to be digital contraband: child pornography, malware, information that cannot lawfully be exported, and unreported digital currency. Exh. 14 (ICE 30(b)(6) depo.) at 37:25–38:24, 39:3–19.

Response: Dispute that this is an exhaustive list of digital contraband and further dispute that this is a material fact.

94. CBP cannot identify any type of digital contraband beyond child pornography. Exh. 13 (CBP 30(b)(6) depo.) at 62:8–66:15.

Response: Dispute plaintiffs’ characterization of the deposition testimony. Howe Declaration (Ex. A) ¶__.

95. Digital data can be posted, shared, or transmitted via the internet and stored on an electronic device. Exh. 46 (Stipulations) at ¶ 9.

Response: No dispute, except dispute that it is a material fact.

96. Defendants are aware that digital contraband may in certain circumstances be accessible from the United States via the internet. Exh. 26 (Defs. Interrog. Responses) at #5.

Response: Dispute that this is a material fact.

97. ICE acknowledges that child pornography can enter or be viewed in the United States via the internet in many ways:

a. By viewing content on servers located outside the United States. Exh. 14 (ICE 30(b)(6) depo.) at 286:5–13.

b. As email attachments. *Id.* at 286:15–19.

c. As text messages. *Id.* at 286:20–25.

d. Via live streaming. *Id.* at 288:20–289:7.

e. Via a listserv or chat group. *Id.* at 289:20–24.

f. Via the Dark Web. *Id.* at 290:7–9.

Response: Dispute that this is a material fact.

98. When Defendants confiscate digital contraband at the border, they either (a) cannot determine whether that digital contraband is already present in the United States, or (b) can determine, through a method known as “hashing,” that the digital contraband is already

present in the United States. Exh. 14 (ICE 30(b)(6) depo.) at 299:5–24.

Response: Dispute that defendants “confiscate” digital contraband and that this is a material fact.

C. Lack of Evidence That Defendants’ Policies and Practices Are Effective

99. CBP and ICE do not know how many warrantless or suspicionless border searches of electronic devices uncover digital contraband. Exh. 26 (Defs. Interrog. Responses) at #13; Exh. 13 (CBP 30(b)(6) depo.) at 68:10–14; Exh. 14 (ICE 30(b)(6) depo.) at 44:25–45:7.

Response: Dispute that this is a material fact

100. CBP and ICE do not know how many warrantless or suspicionless border searches of electronic devices uncover potential evidence of criminal activity. Exh. 13 (CBP 30(b)(6) depo.) at 68:15–20; Exh. 14 (ICE 30(b)(6) depo.) at 338:18–24.

Response: Dispute that this is a material fact

101. CBP does not know how many warrantless or suspicionless border searches of electronic devices result in prosecution or conviction. Exh. 27 (DHS OIG 2018 Report) at Bates 982.

Response: Dispute that this is a material fact

102. ICE does not know how many warrantless or suspicionless border device searches result in criminal arrests or indictments, or referrals to other law enforcement agencies. Exh. 36 (ICE/HSI Priority Requests) at Bates 93.

Response: Dispute plaintiffs’ characterization of the cited evidence because the referenced exhibit provides statistics for arrests, indictments, seizures, search warrants, and administrative arrests resulting from investigations that included a border search of an electronic device. Bates 0094. Also dispute that this is a material fact.

D. CBP and ICE Obtain Warrants and Apply a Reasonable Suspicion Standard

1. CBP Obtains Warrants

103. CBP sometimes conducts searches of electronic devices pursuant to warrants.

Exh. 38 (Border Patrol 2018 Digital Forensics Program PIA) at Bates 1130–31.

Response: Dispute plaintiffs' characterization of cited document which applies only when agency employees in a separate operational office within CBP are not operating pursuant to border search authority. Further dispute that this is a material fact.

104. CBP sometimes applies a probable cause standard for the seizure of an electronic device. Exh. 13 (CBP 30(b)(6) depo.) at 260:11–15.

Response: Dispute plaintiffs' characterization of the fact and refer to the CBP Directive which specifies that 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 the device, or copy of the contents of the device, contains evidence of a violation of a law that CBP is authorized to enforce or administer. *See* Exh. 19 at 5.5.1.1. Further dispute that this is a material fact.

105. CBP provides officers written guidance and training on what constitutes probable cause. Exh. 13 (CBP 30(b)(6) depo.) at 260:16–261:16. CBP also provides training on how to obtain warrants. *Id.* at 279:25–280:4.

Response: Dispute plaintiffs' characterization of the fact. Although officers are provided guidance and training on probable cause and warrants, it is only for specific situations and as it relates to certain distinct legal authorities (other than border search authority) under which CBP officers may operate. Further, dispute that this is a material fact.

106. CBP sometimes obtains warrants for searches of international mail. Exh. 13 (CBP 30(b)(6) depo.) at 267:3–5. Specifically, if the officer has reasonable suspicion that a sealed parcel contains contraband, they may open it, but still need a warrant to read any

correspondence. *Id.* at 268:12–25, 270:20–271:7; Exh. 39 (2001 International Mail Handbook) at Bates 1269. Without reasonable suspicion of contraband, CBP needs a warrant to open the mail. Exh. 13 (CBP 30(b)(6) depo.) at 268:12–25; 270:20–271:7; *see also* Exh. 39 (2001 International Mail Handbook) at Bates 1269.

Response: Dispute plaintiffs’ characterization of the deposition testimony and cited exhibits. Admit that CBP sometimes works with other agencies to obtain warrants for searches of international mail and that in limited situations, officers need a warrant to read correspondence contained in sealed letter class mail that is transmitted within the international postal system and not letters carried by individuals or private carriers. Further dispute that this is a material fact.

107. Although CBP must obtain a warrant to read correspondence in international mail, CBP asserts it may read correspondence on an electronic device without any suspicion. Exh. 13 (CBP 30(b)(6) depo.) at 278:14–20.

Response: Dispute plaintiffs’ characterization of the testimony and refer to the International Mail handbook (Exh. 39) for an accurate interpretation of the policy. The policy applies only when sealed international letter-class mail is in the custody of the postal service. It does not apply to border searches. Further dispute that this is a material fact.

108. CBP officers sometimes obtain warrants at the border to conduct:

a. Involuntary x-ray searches. Exh. 13 (CBP 30(b)(6) depo.) at 262:13–17; Exh. 40 (CBP 2004 Personal Search Handbook) at § 6.h., Bates 1095.

b. Involuntary body cavity searches. Exh. 13 (CBP 30(b)(6) depo.) at 263:13–15; Exh. 40 (CBP 2004 Personal Search Handbook) at § 8.I.d., Bates 1101.

c. Prolonged detentions for medical examinations. Exh. 40 (CBP 2004 Personal Search Handbook) at § 2.p., Bates 1076.

Response: Dispute characterization of the Handbook and refer court to the document for an accurate statement of its contents. Further, dispute that this is a material fact.

109. CBP's Air and Marine Operations is required to get a warrant before searching an electronic device whenever it is operating outside the border environment. Exh. 13 (CBP 30(b)(6) depo.) at 286:25–287:3, 287:7–12; Exh. 41 (CBP AMO Guidance) at Bates 1169; Exh. 42 (CBP 2017 AMCIT Memorandum) at Bates 1153.

Response: Dispute plaintiffs' characterization of the deposition testimony and cited guidance. Further dispute that this is a material fact.

2. ICE Obtains Warrants

110. ICE advises its agents to obtain a warrant "if time permits" and if agents have "any doubt" concerning whether a warrant is required. Exh. 43 (HSI 2012 Search and Seizure Handbook) at § 6.3, Bates 1187, § 7.11.4, Bates 1201.

Response: Dispute this characterization. ICE advises that its agents "*operating in a non-border* environment should make every effort to obtain a warrant prior to searching, even if an exception to the warrant requirement appears to exist." *Id.* at § 8, Bates 1203. Do not dispute this statement in a non-border environment.

111. ICE trains agents on how to seek a warrant. Exh. 14 (ICE 30(b)(6) depo.) at 251:4–7, 261:2–10. This training occurs at the ICE academy, on the job, from supervisors and senior officers, from the local U.S. Attorney's office, and from the Office of the Principal Legal Advisor. *Id.* at 261:15–25, 262:9–16, 263:5–14, 263:24–264:15, 264:21–265:8.

Response: No dispute.

112. ICE's written training materials provide details on how to prepare an affidavit to establish probable cause for a warrant. Exh. 43 (HSI 2012 Search and Seizure Handbook) at § 7.11.4, Bates 1201–02, § 8.2, 1204–05.

Response: No dispute.

113. ICE policy on international mail requires:

- a. A warrant to search inbound international mail that is sealed and appears to contain only correspondence. Exh. 44 (MOU Between ICE/HSI and USPS) at § 4.A.3, Bates 1272; Exh. 14 (ICE 30(b)(6) depo.) at 248:5–9.
- b. A warrant to search outbound international mail that is sealed and weighs less than 16 ounces. Exh. 44 (MOU Between ICE/HSI and USPS) at § 4.B.3, Bates 1273.
- c. A warrant to read correspondence contained in other types of inbound and outbound international mail. *Id.* at § 4.A.2, § 4.B.2., Bates 1272–73.
- d. Reasonable suspicion of contraband to open a parcel, and a warrant to read correspondence in that parcel. *Id. See also* Exh. 14 (ICE 30(b)(6) depo.) at 248:10–15.

Response: No dispute.

114. If an ICE agent opens sealed mail on reasonable suspicion, and it contains correspondence on digital storage media, ICE policy requires a warrant to read that digital correspondence. Exh. 14 (ICE 30(b)(6) depo.) at 249:6–250:10.

Response: Dispute this characterization of ICE policy. An electronic device in the mail would not be treated as solely correspondence for purposes of a border search of mail because the electronic device is merchandise itself, regardless of the data on the device. Accordingly, the laws, regulations, and policy regarding searching sealed mail containing solely correspondence do not apply. *See* Exh. 44 at §§ 4.A.2, Bates 1272.

115. ICE agents sometimes obtain warrants at the border to conduct:

- a. X-ray searches. Exh. 14 (ICE 30(b)(6) depo.) at 259:11–16.
- b. Involuntary body cavity searches. *Id.* at 260:14–25.
- c. Detentions that last longer than eight hours. *Id.* at 254:19–255:6, 255:13–

21, 256:7–258:3.

Response: No dispute.

3. CBP and ICE Apply the Reasonable Suspicion Standard

116. Since at least 2015, CBP has had procedures for conducting advanced device searches based on reasonable suspicion. Exh. 13 (CBP 30(b)(6) depo.) at 254:7–14; 256:9–19; Exh. 45 (CBP 2015 Memorandum on *Cotterman*) at Bates 129–30.

Response: No dispute that CBP has procedures for conducting advanced device searches based on reasonable suspicion of laws it enforces or administers. Dispute that this is a material fact since the Amended Complaint does not contain a claim for relief involving reasonable suspicion.

117. CBP officers are accustomed to applying the reasonable suspicion standard for advanced device searches. Exh. 13 (CBP 30(b)(6) depo.) at 259:8–15.

Response: No dispute, except to dispute that this is a material fact since the Amended Complaint does not contain a claim for relief involving reasonable suspicion.

118. CBP has written guidance and training on reasonable suspicion. Exh. 13 (CBP 30(b)(6) depo.) at 257:11–259:7. ICE provides training to its agents on reasonable suspicion. Exh. 14 (ICE 30(b)(6) depo.) at 279:22–280:8.

Response: No dispute, except to dispute that this is a material fact since the Amended Complaint does not contain a claim for relief involving reasonable suspicion.

119. ICE policy requires agents at the border to have reasonable suspicion for:

a. Strip searches. Exh. 14 (ICE 30(b)(6) depo.) at 278:8–15. *See also* Exh. 43 (HSI 2012 Search and Seizure Handbook) at § 11.1, Bates 1224 (requiring reasonable suspicion for “partial body search[es]”).

b. X-ray or body cavity searches. Exh. 14 (ICE 30(b)(6) depo.) at

278:18– 279:11, 279:13–20; Exh. 43 (HSI 2012 Search and Seizure Handbook) at §10.9, Bates 1219. A destructive search of a vehicle or other object. Exh. 43 (HSI 2012 Search and Seizure Handbook) at §11.1, Bates 1224.

Response: No dispute, except to dispute that this is a material fact since the Amended Complaint does not contain a claim for relief involving reasonable suspicion.

V. Plaintiffs’ Experiences at the Border

Defendants dispute that any of the facts below relating to Plaintiffs’ experiences at the border are material to the Plaintiffs’ First and Fourth Amendment facial challenges. To the extent these facts are material it would only be to their standing to bring this lawsuit.

A. Past Border Searches of Devices

1. Ghassan and Nadia Alasaad

120. Plaintiffs Ghassan and Nadia Alasaad are U.S. citizens who reside in Massachusetts and are married to each other. Exh. 1 (G. Alasaad Dec.) at ¶¶ 2–4; Exh. 2 (N. Alasaad Dec.) at ¶¶ 2–4. He works as a limousine driver, and she is a nursing student. Exh. 1 (G. Alasaad Dec.) at ¶ 1; Exh. 2 (N. Alasaad Dec.) at ¶ 1.

Response: No dispute that Plaintiffs Ghassan and Nadia Alasaad made these statements, but dispute they are material facts.

121. On January 12, 2017, they returned by car to the United States at Highgate Springs, Vermont. Exh. 1 (G. Alasaad Dec.) at ¶ 5; Exh. 2 (N. Alasaad Dec.) at ¶ 5. Ghassan Alasaad was traveling with an unlocked Samsung Note smartphone. Exh. 1 (G. Alasaad Dec.) at ¶ 5. Nadia Alasaad was traveling with a locked iPhone 7 smartphone. Exh. 2 (N. Alasaad Dec.) at ¶ 5. CBP officers conducted a manual search of Mr. Alasaad’s phone. Exh. 2 (N. Alasaad Dec.) at ¶ 8; Exh. 1 (G. Alasaad Dec.) at ¶ 7; Exhs. 15 & 16 (Answer and Complaint) at ¶ 65. CBP officers later searched Ms. Alasaad’s phone. Exh. 47 (EMR) at Bates 337–38, 340.

Response: The referenced exhibits indicate that encounter occurred on July 12, 2017, not January. Further dispute that these facts are material.

122. Nadia Alasaad objected to the search of her phone on the ground that she wears a headscarf in public in accordance with her religious beliefs, and she had photos in her phone of herself without a headscarf on and of her daughters that she did not want any CBP officers, especially male officers, to view. Exh. 2 (N. Alasaad Dec.) at ¶¶ 10, 13.

Response: No dispute, except dispute that this fact is material.

123. On August 28, 2017, Nadia Alasaad arrived at John F. Kennedy International Airport with her 11-year-old daughter. *Id.* at ¶ 19. Her daughter was traveling with a locked iPhone 6+ smartphone. *Id.* CBP officers searched Nadia Alasaad’s handbag, where they found the smartphone that her daughter was using. *Id.* at ¶ 20; Exhs. 15 & 16 (Answer and Complaint) at ¶ 74. CBP officers searched the phone. Exhs. 15 & 16 (Answer and Complaint) at ¶ 76.

Response: No dispute, except dispute that this fact is material.

2. Suhaib Allababidi

124. Plaintiff Suhaib Allababidi is a U.S. citizen who resides in Texas. Exh. 3 (Allababidi Dec.) at ¶¶ 2–3. He owns and operates a business that sells security technology. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Allababidi made these statements in his declaration, but dispute they are material.

125. On January 24, 2017, Allababidi returned to Dallas, Texas, after an international trip. *Id.* at ¶ 4; Exhs. 15 & 16 (Answer and Complaint) at ¶ 77. He was traveling with a locked Samsung S7 Edge smartphone and an unlocked iPhone smartphone. Exh. 3 (Allababidi Dec.) at ¶ 4. A CBP officer seized and manually searched Allababidi’s unlocked iPhone for at least 20 minutes. *Id.* at ¶ 5. After Allababidi declined to provide the password to his locked Samsung phone, CBP officers confiscated both phones in order to conduct an “examination.” *Id.* at ¶ 6;

Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 79–80; Exh. 17 (Detention Notice and Custody Receipt) at Pls. Bates 62; *see also* Exh. 47 (Detention Notice and Custody Receipt) at Bates 107.

Response: Do not dispute that Plaintiff Allababidi’s phones were initially searched by CBP and then detained for further examination by an ICE Special Agent as indicated by the signature and organization listed on the cited Detention and Custody Receipt (Ex. 17). Further dispute this is a material fact.

3. Sidd Bikkannavar

126. Sidd Bikkannavar is a U.S. citizen and a resident of California. Exh. 4 (Bikkannavar Dec.) at ¶¶ 2–3. He is an optical engineer at NASA’s Jet Propulsion Laboratory. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Bikkannavar made these statements in his declaration, but dispute they are material.

127. On January 31, 2017, Bikkannavar flew into Houston, Texas, after an international trip. *Id.* at ¶ 4. He was traveling with a locked Samsung Galaxy Note 5 smartphone. *Id.* CBP officers searched Bikkannavar’s phone for 19 minutes. Exh. 47 (EMR) at Bates 621. Afterwards, a CBP officer stated they had used “algorithms” to search the phone. Exh. 4 (Bikkannavar Dec.) at ¶ 12.

Response: No dispute that Plaintiff Bikkannavar made these statements in his declaration, but dispute that this correctly characterizes paragraph 12 of the declaration. Further dispute that these facts are material.

4. Jérémie Dupin

128. Jérémie Dupin is a lawful permanent resident who resides in Massachusetts. Exh. 5 (Dupin Dec.) at ¶ 2–3. He is a journalist. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Dupin made these statements in his declaration but

dispute they are material.

129. On December 22, 2016, Dupin flew to Miami, Florida after an international trip. *Id.* at ¶ 4. He was traveling with a locked iPhone 5 smartphone, which he used for his journalism work. *Id.* A CBP Officer conducted a basic search of Dupin's phone for about 15 minutes. Exhs. 15 & 16 (Answer and Complaint) at ¶ 90. *See also* Exh. 47 (EMR) at Bates 689; Exh. 5 (Dupin Dec.) at ¶ 8.

Response: No dispute that Plaintiff Dupin made these statements in his declaration, but dispute they are material.

130. On December 23, 2016, Dupin traveled by bus with his seven-year-old daughter from Montreal to New York City. He carried the same locked iPhone. Exh. 5 (Dupin Dec.) at ¶ 11. At the U.S. border customs checkpoint, a CBP officer took the phone into another room for approximately four hours. *Id.* at ¶¶ 12–15. CBP searched it. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 94, 96; *see also* Exh. 47 (EMR) at Bates 690–91. An officer periodically returned to ask Dupin questions about the contents of his phone. Dupin. Exh. 5 (Dupin Dec.) at ¶ 15; Exhs. 15 & 16 (Answer and Complaint) at ¶ 96.

Response: No dispute that Plaintiff Dupin made these statements in his declaration, but dispute they are material, but dispute that the records show that his phone was taken out of the room. *See* Ex.47 at Bates 711. Further dispute that these facts are material.

5. Aaron Gach

131. Aaron Gach is a U.S. citizen who resides in California. Exh. 6 (Gach Dec.) at ¶¶ 2–3. He is an artist. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Gach made these statements in his declaration but dispute they are material.

132. On February 23, 2017, Gach arrived at San Francisco International Airport after an international trip. *Id.* at ¶ 4. Gach traveled with a locked iPhone SE smartphone. *Id.* CBP

searched it. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 102–03; Exh. 47 (EMR) at Bates 714–15.

Response No dispute that Plaintiff Gach made these statements in his declaration, but dispute they are material.

6. Ismail Abdel-Rasoul aka Isma'il Kushkush

133. Isma'il Kushkush is a U.S. citizen who resides in Virginia. Exh. 7 (Kushkush Dec.) at ¶¶ 2–3. He is a freelance journalist. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Kushkush made these statements in his declaration, but dispute they are material

134. On March 18, 2013, Kushkush arrived at Washington Dulles International Airport after an international trip. Exh. 47 (EMR) at Bates 913. At Washington Dulles, CBP officers searched Kushkush's Blackberry Bold cell phone, two electronic storage media, and two SIM cards. *Id.* at Bates 913–14.

Response: No dispute that Plaintiff KushKush made these statements in his declaration, but dispute they are material.

135. On July 30, 2017, Kushkush entered the United States at Highgate Springs, Vermont, via bus from Canada. Exh. 7 (Kushkush Dec.) at ¶ 14. He was carrying a locked iPhone 7 smartphone. *Id.* CBP officers conducted a manual search of Kushkush's phone for about one hour. Exhs. 15 & 16 (Answer and Complaint) at ¶ 117. *See also* Exh. 47 (TECS records) at Bates 304, 332–33; Exh. 47 (HSI Report of Investigation) at Bates 105.

Response: No dispute that Plaintiff KushKush made these statements in his declaration, but dispute they are material.

7. Zainab Merchant

136. Zainab Merchant is a U.S. citizen who resides in Toronto, Canada. Exh. 8 (Merchant Dec.) at ¶¶ 2–3. She is a writer, graduate student, and the founder and editor of a

media website. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Merchant made these statements in her declaration, but dispute they are material.

137. On March 5, 2017, Merchant arrived at the Toronto airport for a flight to Orlando. *Id.* at ¶ 4. She traveled with a locked Samsung smartphone. *Id.* CBP searched Merchant's phone. Exhs. 15 & 16 (Answer and Complaint) at ¶ 135. *See also* Exh. 47 (EMR) at Bates 754. The search lasted 25 minutes. Exh. 47 (EMR) at Bates 754.

Response: No dispute that Plaintiff Merchant made these statements in her declaration, but dispute they are material.

138. CBP officers questioned her about her religious affiliation and her blog, including asking her about an article she had written on the blog that described a previous border crossing experience. Exh. 8 (Merchant Dec.) at ¶ 11.

Response: No dispute that Plaintiff Merchant made this statement in her declaration, but dispute it accurately characterizes the encounter and refer the Court to Ex. 47, Bates 766. Further dispute this fact is material.

139. Merchant was concerned about CBP officers searching her phone because she wears a headscarf in public in accordance with her religious beliefs, and the phone contained pictures of her without her headscarf that she did not want officers to see. *Id.* at ¶ 6.

Response: No dispute that Plaintiff Merchant expressed this concern in her declaration but dispute that the statement accurately characterize the encounter and refer the Court to Ex. 47, Bates 766. This concern appears to have been expressed in the search conducted on July 7, 2018. *See* Ex. 47. Bates 757. Further dispute this fact is material.

140. On April 5, 2018, Merchant arrived in Orlando, Florida, after an international trip. Exh. 8 (Merchant Dec.) at ¶ 14. She carried a locked Samsung Note 8 smartphone. *Id.* CBP

officers searched it. Exh. 47 (EMR) at Bates 908.

Response: No dispute, except dispute that these facts are material.

141. On July 7, 2018, Merchant arrived in Fort Lauderdale, Florida, after an international trip. Exh. 8 (Merchant Dec.) at ¶ 22. She carried a locked Samsung Note 8 smartphone. *Id.* A CBP officer searched Merchant’s phone for about 15 minutes. Exh. 47 (EMR) at Bates 755, 758.

Response: No dispute, except dispute that these facts are material.

142. On September 9, 2018, Merchant traveled from Toronto, Ontario, to Orlando, Florida. Exh. 8 (Merchant Dec.) at ¶ 27. She carried a locked Samsung Note 8 smartphone. *Id.* A CBP officer directed Merchant to turn over her smartphone. Merchant told the officer that she did not consent to the search and that her device contained attorney-client privileged communications. *Id.* at ¶ 28. Nonetheless, “CBP conducted a basic search of Ms. Merchant’s cell phone,” which lasted about ten minutes. Exh. 24 (Email from Marsha Edney, Sept. 20, 2018). *See also* Exh. 47 (EMR) at Bates 759–60. Merchant saw the officer viewing emails and text messages between herself and her lawyer. Exh. 8 (Merchant Dec.) at ¶ 31.

Response: No dispute except to dispute that the third and last sentences accurately characterize the encounter and refer the Court to Ex. 47, Bates 757-58 for an accurate description. Further dispute these facts are material.

8. Akram Shibly

143. Mohammed Akram Shibly is a U.S. citizen who currently lives in Los Angeles. Exh. 9 (Shibly Dec.) at ¶¶ 2–3. He is a filmmaker and a graduate student. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Shibly made these statements in his declaration, but dispute they are material.

144. On January 1, 2017, Shibly entered the United States at the Lewiston-Queenston Bridge in New York. *Id.* at ¶ 4. He was carrying a locked iPhone 6+ smartphone. *Id.* A CBP officer

searched it. Exhs. 15 & 16 (Answer and Complaint) at ¶ 140. *See also* Exh. 47 (EMR) at Bates 847, 849. The search lasted 37 minutes. Exh. 47 (EMR) at Bates 847.

Response: No dispute, except dispute that the facts are material. .

9. Matthew Wright

145. Matthew Wright is a U.S. citizen who resides in Colorado. Exh. 10 (Wright Dec.) at ¶¶ 2–3. He is a computer programmer. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Wright made these statements in his declaration, but dispute they are material.

146. On April 21, 2016, Wright arrived in Denver, Colorado, after an international trip. *Id.* at ¶ 5. Wright was traveling with a locked iPhone 6 smartphone, a locked MacBook Pro laptop, and an unlocked GoPro camera. *Id.* Wright declined a CBP officer’s demand to unlock his laptop. As a result, CBP officers confiscated his laptop, phone, and camera. *Id.* at ¶ 6.

Response: No dispute, except dispute that they are material.

147. “CBP extracted and obtained information from Plaintiff Wright’s devices.” Exhs. 15 & 16 (Answer and Complaint) at ¶ 155. Specifically, 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 Wright’s phone and from his camera.” Exhs. 15 & 16 (Answer and Complaint) at ¶ 44. *See also* Exh. 25 (June 6, 2016 CBP email) at Pls. Bates 953; Exh. 47 (HSI Digital Forensic Report) Bates 98.

Response: No dispute, except dispute that they are material

10. Diane Mave Zorri

148. Diane Mave Zorri is a U.S. citizen who resides in Florida. Exh. 11 (Zorri Dec.) at ¶¶ 2–3. She is a university professor and a former United States Air Force captain. *Id.* at ¶ 1.

Response: No dispute that Plaintiff Zorri made these statements in her declaration, but dispute they are material.

149. On June 25, 2017, Zorri arrived in Miami, Florida, after an international trip. *Id.* at ¶ 4. Zorri was traveling with a MacBook Pro laptop and an iPhone 7 smartphone, both locked. *Id.* CBP searched Zorri's phone for about 45 minutes. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 121, 124. *See also* Exh. 47 (EMR) at Bates 729, 731.

Response: No dispute that Plaintiff Zorri made these statements in her declaration but Defendants note that the referenced EMR pages (729-731) only mention an iPhone. Further dispute these facts are material.

B. Ongoing Retention of Information From Past Device Searches

150. Defendants have retained in TECS information its officers observed during the search of the contents of seven Plaintiffs' phones: Ghassan Alasaad, Nadia Alasaad, Bikkannavar, Dupin, Merchant, Shibly, and Zorri. Exh. 26 (Defs. Interrog. Responses) at #10 (Nadia Alasaad, Bikkannavar, Dupin, Merchant, and Zorri); Exh. 47 (TECS records) at Bates 340, 351, 355, 359 (Ghassan Alasaad); Exh. 47 (TECS records) at Bates 340, 351, 355, 359 (Nadia Alasaad); Exh 47 (TECS records) at Bates 691, 711 (Dupin); Exh 47 (TECS records) at Bates 849, 873, 878 (Shibly).

Response: No dispute.

151. Defendants also have retained information copied from Wright's electronic devices.

a. The data extracted from Wright's devices was stored on three thumb drives. Exh. 25 (EMR) at Pls. Bates 938.

Response: No dispute.

b. Two months after CBP returned Wright's devices to him, CBP continued to retain the thumb drives. Exh. 47 (EMR) at Bates 888; Exh. 47 (log of items received by CBP laboratory) at Bates 909; Exh. 28 (Def. Privilege Log of 12/7/18) (describing Bates 909 as "[l]og of items received by CBP laboratory"); Exh. 24 (Email from Marsha Edney, Nov. 21, 2018)

(describing Bates 909 as “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”).

Response: Dispute that these facts are material and the inference being drawn by the absence of a document showing destruction. Defendants aver that all copies of Wright’s data have been deleted . *See* Declaration of Jenny Tsang (Ex. L.). There is no material dispute because this information is uniquely with in Defendants’ knowledge and does not matter as a matter of law.

c. DHS policy requires that “a record of the destruction [of information from a traveler’s device] is documented in the TECS Report of Investigation (ROI).” Exh. 29 (DHS 2009 PIA), at Bates 228. In both civil discovery in this case and in response to a FOIA request from Wright, CBP and ICE produced no records showing that the data retained on the thumb drives was destroyed. Exh. 12 (Cope Dec.) at ¶¶ 4–5.

Response: No dispute.

C. Past Device Confiscations¹

1. Ghassan and Nadia Alasaad

152. CBP officers retained Ghassan and Nadia Alasaad’s phones after the Alasaads left the border area on July 12, 2017. Exh. 1 (G. Alasaad Dec.) at ¶ 15; Exh. 47 (EMR) at Bates 340.

Response: Dispute only to the extent that that the undefined term “retained” is used.

Admit that the phones were detained. Ex. 47 at Bates 340.

153. Ghassan and Nadia Alasaad had to spend approximately \$1,000 to purchase two new phones. Exh. 1 (G. Alasaad Dec.) at ¶ 17; Exh. 2 (N. Alasaad Dec.) at ¶ 17.

¹ Defendants disagree with the use of the term “confiscations” but admit that they do sometimes detain and/or seize electronic devices.

Response: No dispute that Plaintiffs Ghassan and Nadia Alasaad made this statement in their declarations, but dispute that the fact is material.

154. Twelve days after Ghassan and Nadia Alasaad crossed the border, CBP officials sent their phones back to them. Exhs. 15 & 16 (Answer and Complaint) at ¶ 72.

Response: No dispute, except dispute that it is material.

155. Soon after receiving his phone from CBP, Ghassan Alasaad 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 did not occur prior to CBP's confiscation of the phone. Exh. 1 (G. Alasaad Dec.) at ¶ 19.

Response: No dispute that Plaintiff Alasaad made these statements in his declaration, but Defendants lack knowledge or information to determine if they are true or not. Further, dispute that the facts are material.

2. Suhaib Allababidi

156. On January 24, 2017, CBP officers detained Allababidi's unlocked iPhone and locked Samsung smartphone after he had been permitted to leave the border area. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 79–80; Exh. 3 (Allababidi Dec.) at ¶ 6.

Response: No dispute, except dispute that it is material.

157. CBP officers confiscated Allababidi's unlocked phone even though an officer had already manually searched the phone and returned it to Allababidi. Exhs. 15 & 16 (Answer and Complaint) at ¶¶ 79–80; Exh. 3 (Allababidi Dec.) at ¶¶ 5–6.

Response: Dispute only to the extent that the undefined term confiscate is used. Further dispute that this is material.

158. Allababidi had to spend more than \$1,000 on replacement phones. Exh. 3 (Allababidi Dec.) at ¶ 9.

Response: No dispute that Plaintiff Allababidi made this statement in his

declaration, but dispute that the fact is material.

159. Allababidi's phones were sent to the "Regional Computer Forensic Lab" on February 15, 2017, and then sent to another location on March 3, 2017. Exh. 47 (Detention Notice and Custody Receipt) at Bates 107.

Response: No dispute, except dispute that it is material.

160. The unlocked iPhone was returned to Allababidi more than two months after confiscation. Exh. 3 (Allababidi Dec.) at ¶ 7. *See also* Exh. 47 (Detention Notice and Custody Receipt) at Bates 107.

Response: No dispute, except dispute that it is material.

161. The locked Samsung smartphone was returned to Allababidi on December 13, 2017, more than ten months after confiscation, and just two days before Defendants moved to dismiss in this case. Exh. 3 (Allababidi Dec.) at ¶ 8; Exh. 32 (Defs. Motion to Dismiss) at p. 9.

Response: No dispute, except dispute that it is material.

3. Matthew Wright

162. CBP officers seized Wright's smartphone, laptop, and GoPro camera on April 21, 2016. Exh. 25 (Detention Notice and Custody Receipt) at Pls. Bates 945.

Response: Dispute only to the extent that that the term "seized" is used. Admit that the devices were detained. Ex. 25 at Bates 945.

163. An officer informed Wright that it might take CBP as long as a year to return his devices to him. Exh. 10 (Wright Dec.) at ¶ 7.

Response: No dispute that Plaintiff Wright states this in his declaration, but dispute that his is a material fact.

164. Wright spent \$2,419.97 for a new laptop and phone. Exh. 10 (Wright Dec.) at ¶ 8. As a computer programmer, Wright's livelihood depends on these tools. *Id.*

Response: No dispute that Plaintiff Wright states this in his declaration, but Defendants

lack any knowledge of these facts. Further dispute these are material facts.

165. Wright's electronic devices were transferred between CBP and ICE facilities multiple times. Exh. 25 (EMR) at Pls. Bates 936–38.

Response: No dispute, except dispute that it is material.

166. CBP returned Wright's electronic devices to him after 56 days, on June 16, 2016. Exh. 25 (EMR) at Pls. Bates 938; Exh. 10 (Wright Dec.) at ¶ 9.

Response: No dispute, except dispute that it is material.

D. Other Recurring Border Scrutiny

167. Eight Plaintiffs have been subjected to recurring secondary inspections during border crossings. Exh. 47 (TECS records) at Bates 338, 348, 350–51, 362–367 (six of Ghassan Alasaad); Exh. 47 (TECS records) at Bates 338, 350, 363–64 (three of Nadia Alasaad); Exh. 47 (TECS records) at Bates 586–88, 590, 592–95, 600, 602–04, 606, 608–620 (nine of Allababidi); Exh. 47 (TECS records) at Bates 678, 680–82, 684–85, 688 (seven of Bikkannavar); Exh. 47 (TECS records) at Bates 704–05, 707–13 (six of Dupin); Exh. 47 (TECS records) at Bates 319-322, 324–25, 327, 329–30, 332–35, 913–15 (eight of Kushkush); Exh. 47 (TECS records) at Bates 817, 819–22, 824–26, 828–30, 832, 834, 836–39, 841–45 (eight of Merchant); Exh. 47 (TECS records) at Bates 868, 870, 880, 884–85 (four of Shibly).

Response: Do not dispute that these Plaintiffs have been referred to secondary inspections on multiple occasions but dispute that the cited TECS records for Nadia Alasaad and Bikkannavar indicate that they were searched 3 or 7 times, respectively. Further dispute that this is a material fact.

168. Seven Plaintiffs are subjected to recurring bag searches at the border. Exh. 47 (TECS records) at Bates 348, 365–66 (three of Ghassan Alasaad); Exh. 47 (TECS records) at Bates 348, 910–11 (two of Nadia Alasaad); Exh. 47 (TECS records) at Bates 395–96, 593, 602–03 (three of Allababidi in 2017 alone); Exh. 47 (TECS records) at Bates 709–10, 713 (three of

Dupin); Exh. 47 (TECS records) at Bates 299, 306, 915 (three of Kushkush); Exh. 47 (TECS records) at Bates 766, 824–26, 828, 830, 832, 838–39, 843, 845 (six of Merchant); Exh. 47 (TECS records) at Bates 868, 875, 880 (three of Shibly).

Response: Do not dispute that these Plaintiffs have been subject to at least one bag search at the border but dispute that the cited TECS records for Ghassan Alasaad, Nadia Alasaad and Dupin indicate that their bags were searched 3, 2 and 3 times respectively. Further dispute that this is a material fact.

E. Regular International Travel, Past and Future

1. Ghassan and Nadia Alasaad

169. Ghassan Alasaad has returned to the United States from an international trip at least 13 times since January 1, 2013. Exh. 1 (G. Alasaad Dec.) at ¶ 22. Nadia Alasaad has done so at least 15 times during this period. Exh. 2 (N. Alasaad Dec.) at ¶ 27.

Response: No dispute that Plaintiffs Ghassan and Nadia Alasaad made these statements in their declarations.

170. Ghassan and Nadia Alasaad intend to continue traveling internationally for personal reasons, and will carry electronic devices with them when they do so. Exh. 2 (N. Alasaad Dec.) at ¶¶ 26, 28; Exh. 1 (G. Alasaad Dec.) at ¶¶ 21, 23. For example, in the summer of 2019, they intend to travel to Egypt, Jordan, and/or Turkey. Exh. 1 (G. Alasaad Dec.) at ¶ 24; Exh. 2 (N. Alasaad Dec.) at ¶ 29. Likewise, during the summer of 2019, Nadia Alasaad may travel to Canada. Exh. 2 (N. Alasaad Dec.) at ¶ 30.

Response: No dispute that Plaintiffs Ghassan and Nadia Alasaad made these statements in their declarations but Defendants lack knowledge of their future travel plans.

2. Subaib Allababidi

171. Allababidi has returned to the United States from an international trip at least seven times since January 1, 2013. Exh. 3 (Allababidi Dec.) at ¶ 12.

Response: No dispute that Plaintiff Allababidi made this statement in his declaration.

172. Allababidi intends to continue traveling internationally for business and personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 11, 13. For example, he has reserved flights to Turkey in May and home in July of this year, and he may visit China later this year. *Id.* at ¶¶ 14–15.

Response: No dispute that Plaintiff Allababidi made this statement in his declaration but Defendants lack knowledge of his future travel plans.

3. Sidd Bikkannavar

173. Bikkannavar has returned to the United States from an international trip at least 36 times since January 1, 2013. Exh. 4 (Bikkannavar Dec.) at ¶ 17.

Response: No dispute that Plaintiff Allababidi made this statement in his declaration.

174. Bikkannavar intends to continue traveling internationally for personal reasons, and will carry electronic devices with him when he does so. Exh. 4 (Bikkannavar Dec.) at ¶¶ 16, 18. For example, he plans to take eight international trips by September 2020 to participate in solar car races and related activities. *Id.* at ¶ 19.

Response: No dispute that Plaintiff Bikkannavar made this statement in his declaration but Defendants lack knowledge of his future travel plans.

4. Jérémie Dupin

175. Dupin has returned to the United States from an international trip at least 21 times since January 1, 2013. Exh. 5 (Dupin Dec.) at ¶ 19.

Response: No dispute that Plaintiff Dupin made this statement in his declaration.

176. Dupin intends to continue traveling internationally for business and personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 18, 20. For

example, he intends to visit his daughter in Canada. *Id.* at ¶ 21. Also, as a journalist, he intends to travel to Haiti in May or June of 2019, and he may travel to Venezuela later this year. *Id.* at ¶ 22.

Response: No dispute that Plaintiff Dupin made this statement in his declaration but Defendants lack knowledge of his future travel plans.

5. Aaron Gach

177. Gach has returned to the United States from an international trip at least seven times since January 1, 2013. Exh. 6 (Gach Dec.) at ¶ 14.

Response: No dispute that Plaintiff Gach made this statement in his declaration.

178. Gach intends to continue traveling internationally for business and personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 13, 15. For example, he has purchased airline tickets to Germany in June and home in July. *Id.* at ¶ 16.

Response: No dispute that Plaintiff Gach made this statement in his declaration but Defendants lack knowledge of his future travel plans.

6. Isma'il Kushkush

179. Kushkush has returned to the United States from an international trip at least eight times since January 1, 2013. Exh. 7 (Kushkush Dec.) at ¶ 22.

Response: No dispute that Plaintiff KushKush made this statement in his declaration.

180. Kushkush intends to continue traveling internationally for his journalism and for personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 21, 23.

Response: No dispute that Plaintiff KushKush made this statement in his declaration but Defendants lack knowledge of his future travel plans

7. Zainab Merchant

181. Merchant has returned to the United States from an international trip at least 12 times since January 1, 2013. Exh. 8 (Merchant Dec.) at ¶ 35.

Response: No dispute that Plaintiff Merchant made this statement in her declaration.

182. Merchant intends to continue traveling internationally for professional and personal reasons, and will carry electronic devices with her when she does so. *Id.* at ¶¶ 34, 36. For example, from now through May 2020, she plans to periodically travel from her current residence in Canada to her university in Boston in order to complete graduate studies. *Id.* at ¶ 37.

Response: No dispute that Plaintiff Merchant made this statement in her declaration but Defendants lack knowledge of her future travel plans.

8. Akram Shibly

183. Shibly has returned to the United States from an international trip at least 18 times since January 1, 2013. Exh. 9 (Shibly Dec.) at ¶ 18.

Response: No dispute that Plaintiff Shibly made this statement in his declaration.

184. Shibly plans to continue traveling internationally for business and personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 17, 19.

Response: No dispute that Plaintiff Shibly made this statement in his declaration but Defendants lack knowledge of his future travel plans.

9. Matthew Wright

185. Wright has returned to the United States from an international trip at least 22 times since January 1, 2013. Exh. 10 (Wright Dec.) at ¶ 16.

Response: No dispute that Plaintiff Wright made this statement in his declaration.

186. Wright plans to continue traveling internationally for personal reasons, and will carry electronic devices with him when he does so. *Id.* at ¶¶ 15, 17.

Response: No dispute that Plaintiff Wright made these statements in his declaration, but Defendants lack knowledge of his future travel plans.

187. Wright attends ultimate Frisbee tournaments outside the United States regularly, and has attended a tournament in Portugal in June or July each year for the past five years. Wright's brother lives in Scotland, and it is common for him to take at least one trip a year to visit him there or elsewhere in Europe. Wright also has a group of friends who enjoy travel and Wright typically plans a trip or two abroad each year. *Id.* at ¶ 17. Wright has booked plane tickets for one international trip from June 24, 2019 through July 1, 2019. *Id.* at ¶ 18.

Response: No dispute that Plaintiff Wright made these statements in his declaration but Defendants lack knowledge of his future travel plans.

10. Diane Mave Zorri

188. Zorri has returned to the United States from an international trip at least 10 times since January 1, 2013. Exh. 11 (Zorri Dec.) at ¶ 11.

Response: No dispute that Plaintiff Zorri makes this statement in her declaration.

189. Zorri plans to continue traveling internationally for professional and personal reasons, and will carry electronic devices with her when she does so. *Id.* at ¶¶ 10, 12. For example, it is significantly possible that Zorri will travel to Italy in June or July 2019, and Zorri has tentative plans to attend conferences in Europe in June and November 2019. *Id.* at ¶¶ 13–14.

Response: No dispute that Plaintiff Zorri makes this statement in her declaration but Defendants lack knowledge of her future travel plans.

Dated: June 6, 2019

Respectfully submitted:

JOHN R. GRIFFITHS
Director, Federal Programs Branch

DIANE KELLEHER
Assistant Director, Federal Programs Branch

/s/ Marsha Edney

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

Attorneys for Defendants