UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

Ghassan Alasaad, Nadia Alasaad, Suhaib Allababidi, Sidd Bikkannavar, Jérémie Dupin, Aaron Gach, Ismail Abdel-Rasoul aka Isma'il Kushkush, Diane Maye, Zainab Merchant, Mohammed Akram Shibly, and Matthew Wright, Plaintiffs, v. Elaine Duke, Acting Secretary of the U.S. Department of Homeland Security, in her official capacity; Kevin McAleenan, Acting Commissioner of U.S. Customs and Border Protection, in his official capacity; and Thomas Homan, Acting Director of U.S. Immigration and Customs Enforcement, in his official capacity, Defendants.	COMPLAINT FOR INJUNCTIVE AND DECLARATORY RELIEF (Violation of First and Fourth Amendment rights) No. 1:17-cv-11730-DJC

AMENDED COMPLAINT

PRELIMINARY STATEMENT

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

their owners' lives. Because government scrutiny of electronic devices is an unprecedented invasion of personal privacy and a threat to freedom of speech and association, searches of such devices absent a warrant supported by probable cause and without particularly describing the information to be searched are unconstitutional.

2. Plaintiffs are ten U.S. citizens and a lawful permanent resident who regularly travel outside the country with their electronic devices and intend to continue doing so. Federal officers seized and searched Plaintiffs' electronic devices at U.S. ports of entry without probable cause to believe that the devices contained contraband or evidence of a violation of immigration or customs laws. Four of the Plaintiffs had their devices retained for weeks or months beyond the time they entered the country, and were deprived of the use of their devices.

3. Defendants, who are responsible for the challenged searches, seizures, practices, and policies, are the heads of the U.S. Department of Homeland Security ("DHS"), and two of its units, CBP and ICE.

4. CBP and ICE have searched the mobile electronic devices of tens of thousands of individuals, and the frequency of such searches has been increasing. While border officers conduct some searches manually, they conduct other searches with increasingly powerful and readily available forensic tools, which amplify the intrusiveness and comprehensiveness of the searches.

5. The effect of searches of mobile electronic devices on individual privacy and expression can hardly be overstated. Travelers' electronic devices contain massive amounts of personal information, including messages to loved ones, private photographs of family members, opinions and expressive material, and sensitive medical, legal, and

financial information. The volume and detail of personal data contained on these devices provides a comprehensive picture of travelers' private lives, making mobile electronic devices unlike luggage or other items that travelers bring across the border.

6. The U.S. Supreme Court recognized that searches of mobile electronic devices implicate unique privacy interests in *Riley v. California*, 134 S. Ct. 2473 (2014). The Court observed that "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" The Court rejected the government's argument that "a search of all data stored on a cell phone is 'materially indistinguishable' from searches of . . . physical items." In the Court's words, "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon." The Court held that the Fourth Amendment requires police to obtain a warrant based on probable cause before searching a phone seized during an arrest. *Id.* at 2488, 2494–95.

7. In this lawsuit, Plaintiffs challenge: (a) searches by CBP and ICE of travelers' electronic devices in violation of the First and Fourth Amendments; and (b) prolonged seizures, *i.e.*, confiscation of travelers' electronic devices for weeks or months to effectuate searches after travelers leave the border, in violation of the Fourth Amendment.

8. Two written directives expressly authorize the challenged searches and confiscations:

a. CBP's 2009 directive titled "Border Searches of Electronic Devices Containing Information" ("CBP's 2009 Policy");[1] and

[1] https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.

b. ICE's 2009 directive titled "Border Searches of Electronic Devices" ("ICE's 2009 Policy").[2]

9. Each directive permits warrantless and suspicionless searches and confiscations of mobile electronic devices. Neither directive requires that searches of electronic devices be authorized by a warrant based on probable cause to believe that the device contains contraband or evidence of a violation of immigration or customs laws.

10. Searching personal electronic devices without a warrant based on probable cause violates the constitutional rights of individuals to keep the private and expressive details of their lives free from unwarranted government scrutiny. Defendants' policies and practices in searching and seizing personal electronic devices at the border eviscerate Americans' constitutional rights to privacy and freedom of speech and association.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over Plaintiffs' federal claims pursuant to 28 U.S.C. § 1331.

12. This Court has authority to issue declaratory and injunctive relief under 28 U.S.C. § 2201 and § 2202, Rules 57 and 65 of the Federal Rules of Civil Procedure, and its inherent equitable powers.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391.

[2] https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

PARTIES

Plaintiffs

14. Plaintiffs Ghassan and Nadia Alasaad are married U.S. citizens. They reside in Revere, Massachusetts, where Mr. Alasaad is a limousine driver and Ms. Alasaad is a nursing student.

15. Plaintiff Suhaib Allababidi is a U.S. citizen who resides in Texas. He owns and operates a business that sells security technology, including to federal government clients.

16. Plaintiff Sidd Bikkannavar is a U.S. citizen who resides in California. He is an optical engineer at NASA's Jet Propulsion Laboratory.

17. Plaintiff Jérémie Dupin is a U.S. lawful permanent resident, a citizen of Haiti, and a resident of Massachusetts. He is a journalist.

18. Plaintiff Aaron Gach is a U.S. citizen who resides in California. He is an artist.

19. Plaintiff Ismail Abdel-Rasoul aka Isma'il Kushkush is a U.S. citizen who resides in Virginia. He is a freelance journalist.

20. Plaintiff Diane Maye is a U.S. citizen who resides in Florida. She is an Assistant Professor of Homeland Security at Embry-Riddle Aeronautical University and a former captain in the United States Air Force.

21. Plaintiff Zainab Merchant is a U.S. citizen who resides in Florida. She is a writer and a graduate student in international security and journalism at Harvard University.

22. Plaintiff Mohammed Akram Shibly is a U.S. citizen who resides in New York. He is a filmmaker.

23. Plaintiff Matthew Wright is a U.S. citizen who resides in Colorado. He is a computer programmer.

Defendants

24. Defendant Elaine Duke is Acting DHS Secretary. She has authority over all DHS policies and practices, including those challenged here. Plaintiffs sue her in her official capacity.

25. Defendant Kevin M. McAleenan is Acting Commissioner of CBP, which controls U.S. ports of entry. He has authority over all CBP policies and practices, including those challenged here. Plaintiffs sue him in his official capacity.

26. Defendant Thomas D. Homan is Acting Director of ICE, which assists CBP in searching electronic devices seized at the border. He has authority over all ICE policies and practices, including those challenged here. Plaintiffs sue him in his official capacity.

ELECTRONIC DEVICES CARRIED OVER THE U.S. BORDER

27. Nearly everyone who crosses U.S. borders each day carries an electronic device of some kind. These include mobile phones (most commonly smartphones), laptops, tablets, digital cameras, and portable digital storage devices. The use of mobile phones among U.S. adults is pervasive: 95 percent own a cell phone, with 77 percent owning a smartphone.[3] Similarly, more than 50 percent of U.S. adults own a tablet

[3] http://www.pewinternet.org/fact-sheet/mobile/.

computer.[4] Travelers rely on these devices for communication (via text messages, calls, email, and social networking), navigation, shopping, banking, entertainment, news, and photography, among other functions.

28. People consistently carry electronic devices with them when they travel. Many travelers carry several electronic devices at a time, thus multiplying the data in their possession.

29. Today's electronic devices are unlike luggage or other items a person might carry across the border.

30. Electronic devices contain massive amounts of data, and their storage capacities continue to grow. Laptops sold in 2017 can store up to two terabytes.[5] Even tablet computers can be purchased with a terabyte of storage, and smartphones can store hundreds of gigabytes of data. The availability of cloud storage (*i.e.*, data located on remote servers), email, and social media services that are accessible from electronic devices via the Internet can dramatically increase the functional capacity of a device. The storage capacity of a smartphone, laptop, or tablet can be the equivalent of hours of video files, thousands of pictures, or millions of pages of text.[6]

31. Electronic devices also contain a diverse array of personal, expressive, and associational information, including emails, text messages, voice mails, communications and location history, contact lists, social media postings, Internet browsing history, medical records, financial records, privileged information, videos, photos, other images,

[4] http://www.pewinternet.org/fact-sheet/mobile/.
[5] Apple, *Compare Mac models*, https://www.apple.com/mac/compare/.
[6] LexisNexis, *How Many Pages in a Gigabyte?* (2007), http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf.

calendars, and notes. Government officers can learn a great deal about people just by looking at the "apps" (*i.e.*, applications) they have chosen to install, such as apps related to news, dating, religious communities, health, or foreign languages. Many people store sensitive information about other people in their devices, including professionals who have duties to secure sensitive information about their clients.

32. Electronic devices can act as portals to access cloud content, which is stored on or pulled from the remote servers of private companies. Cloud services and apps can reveal, for example, years' worth of emails, photos, or health data such as heart rates and reproductive cycles.

33. Owners of electronic devices may not even be aware of some types of data that their devices contain, which can include historical location information, so-called "deleted" items that actually remain in digital storage, or metadata about digital files or the device itself such as time stamps or GPS coordinates created automatically by software on the device.

34. Electronic devices can also contain data that span years, particularly given that data can readily be transferred from an old device to a new one.

35. Because electronic devices contain enormous quantities of information reflecting a range of conduct over extended periods of time, their contents can be used to assemble pictures of their owners' lives that are far more detailed, intimate, and personal than would be possible even through comprehensive searches of those individuals' homes.

36. Electronic devices are often essential to people's work, including that of the Plaintiffs. Many individuals rely on their mobile phones or laptop computers to

respond to work-related email, create or edit important documents, or run their businesses. Thus, devices are essential possessions for most people. As explained below, officials' confiscation of such devices not only violates Plaintiffs' Fourth Amendment rights, it also significantly interferes with their economic livelihoods.

SEARCHES OF ELECTRONIC DEVICES AT THE U.S. BORDER

37. All eleven Plaintiffs were subjected to searches of their electronic devices at the U.S. border.

38. The number of border searches of electronic devices by CBP and ICE has been growing rapidly. According to CBP data, CBP conducted 14,993 electronic device searches in the first half of fiscal year 2017, meaning that CBP is on track to conduct approximately 30,000 searches this fiscal year, compared to just 8,503 searches in fiscal year 2015.[7] If the rate of searches continues to grow, CBP may conduct even more searches in the next fiscal year.

39. The searches of electronic devices that border officials conduct can be (a) "manual," (b) "forensic," or (c) both manual and forensic searches for a single device.

40. During manual searches, officers review the contents of the device by interacting with it as an ordinary user would, through its keyboard, mouse, or touchscreen interfaces. For example, Mr. Allababidi watched a CBP officer manually search one of his phones for at least 20 minutes.

41. Given the great volume and detail of personal information that electronic devices contain, and the ease of manually navigating them, manual searches are

[7] https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0. The fiscal year runs from October 1 of the year before to September 30 of that same year. So, for example, fiscal year 2017 runs from October 1, 2016 to September 30, 2017.

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

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

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

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

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

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

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

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

other ports of entry. During the inspection process, officers take possession of travelers' passports and other belongings.

48. CBP officers often use the coercive nature of the secondary inspection environment to compel travelers to unlock their devices or disclose their device passwords. Officers also threaten to confiscate travelers' devices if they decline to provide access to the devices. For example, Mr. and Ms. Alasaad had no meaningful choice but to disclose to a CBP officer the password to Ms. Alasaad's phone, because the officer told them that CBP would confiscate and keep the phone if they did not provide the password.

49. CBP officers even resort to physical force in order to conduct electronic device searches. For example, when Mr. Shibly refused to hand over his phone after having done so three days earlier at the same port of entry, three CBP officers physically restrained him and took his phone. One officer squeezed his hand around Mr. Shibly's throat, which caused him great pain and emotional distress.

CONFISCATION OF ELECTRONIC DEVICES AT THE U.S. BORDER

50. Four Plaintiffs were subjected to confiscation and prolonged seizure of their electronic devices at the U.S. border: Ghassan and Nadia Alasaad, Suhaib Allababidi, and Matthew Wright.

51. When travelers decline to comply with government officers' orders to unlock their devices or provide their device passwords, officers often respond by confiscating those devices. In such cases, CBP officers may also confiscate unlocked devices (*i.e.*, devices whose content can be accessed without entering a password or other security authentication), including devices that CBP officers have already searched.

52. These confiscations can last for months. For example, when Mr. Allababidi refused to unlock one of his phones, officers confiscated that phone and also his unlocked phone that officers had already searched. The government returned his unlocked phone more than two months later. After more than seven months, CBP still has not returned his locked phone. Similarly, when Mr. Wright refused to unlock his laptop, officers confiscated that laptop, and also his locked phone, and his camera, which did not have a locking feature. Mr. Wright received his confiscated devices 56 days later.

53. Even when travelers comply with officers' demands to unlock their devices or provide their device passwords, officers sometimes confiscate the devices anyway. For example, even though Ms. Alasaad provided the password to her phone, and CBP officers had already searched Mr. Alasaad's unlocked phone, officers still confiscated both of the couple's phones. CBP kept both phones for approximately 15 days.

54. These lengthy device confiscations cause significant harm. Many travelers, including Plaintiffs, rely on their electronic devices for their work and livelihoods, as well as for communicating with family members. Losing access to electronic devices and the information they contain for extended periods of time can disrupt travelers' personal and professional lives. Confiscation of electronic devices is especially harmful to those who need, but do not have or cannot afford, replacement devices, and those who need but did not back up stored data.

55. For example, a CBP officer told Mr. Wright that it could take a year for his devices to be returned. Mr. Wright needs these tools to perform his job as a computer programmer. Soon after CBP confiscated his laptop and phone, Mr. Wright had to spend

$2,419.97 to buy a new laptop and phone. Similarly, Mr. Alasaad needs his phone for his work as a limousine driver, and Ms. Alasaad needs her phone for daily responsibilities, so the Alasaads had to spend approximately $1,000 to purchase two new phones. Likewise, Mr. Allababidi had to spend more than $1,000 on replacement phones.

56. When CBP and ICE officers confiscate electronic devices pursuant to their policies and practices for the purpose of searching those devices' content, such confiscations violate the Fourth Amendment in at least three distinct ways:

a. First, these confiscations are not justified at their inception when they are affected absent probable cause.

b. Second, these confiscations are excessive in scope, because officers confiscate not just the locked devices they are unable to search at the port of entry, but also the unlocked devices they are able to search and that they sometimes have already searched.

c. Third, these confiscations are excessive in duration where the duration of confiscation of locked devices is unreasonable in relation to the time actually needed to search the devices.

DEFENDANTS' POLICIES ON DEVICE SEARCH AND CONFISCATION

57. CBP and ICE policies expressly authorize warrantless and suspicionless searches and confiscations of electronic devices at the border.

Data Searches

58. The 2009 CBP and ICE Policies authorize border officials to search travelers' electronic devices without a warrant or any basis for suspecting that the devices

contain contraband or evidence of a violation of immigration or customs laws. Nor do the policies require that travelers consent to searches of their devices.

a. CBP's 2009 Policy authorizes CBP officers to "examine electronic devices" and "review and analyze the information encountered at the border"— "with or without individualized suspicion." ¶ 5.1.2. On information and belief, this policy is currently in force.

b. ICE's 2009 Policy authorizes ICE agents to search electronic devices "with or without individualized suspicion." ¶ 6.1. On information and belief, this policy is currently in force.

59. The 2009 Policies permit warrantless and suspicionless searches of content that raises heightened privacy concerns. Under CBP's 2009 Policy, if digital information is protected by the attorney-client or attorney work product privilege, it is "not necessarily exempt from a border search." ¶ 5.2.1. While officers "must seek advice from the CBP Associate/Assistant Chief Counsel before" searching it, *id.*, that requirement provides no substantive protection. Likewise, the policy provides that "[o]ther possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy." ¶ 5.2.2. By referencing "any applicable" law and policy, CBP's 2009 Policy does not make clear whether there are any limits on its search authority. If there are any limits, the CBP policy provides no guidance on how agents should comply with such limits.

60. Similarly, under ICE's 2009 Policy, "a claim of privilege or personal information" may justify "special handling," but it "does not prevent the search of a

traveler's information . . . ." ¶ 8.6.1. Likewise, the ICE policy acknowledges that confidential business information "may" be subject to the Trade Secrets Act, the Privacy Act, and "other laws" (¶ 8.6.2.a), but it provides no guidance on how agents should process such materials. The ICE rules on information subject to the attorney-client or attorney work product privilege (¶ 8.6.2.b), and "[o]ther possibly sensitive information, such as medical records and work-related information carried by journalists" (¶ 8.6.2.c), suffer the same flaws as the corresponding CBP rules.

Device Confiscations

61. The 2009 CBP and ICE Policies authorize confiscation of travelers' electronic devices for weeks or months at a time in order to effectuate searches after travelers leave the border, without probable cause or any basis for suspecting that the devices contain contraband or evidence of a violation of immigration or customs laws. Nor do the policies require that travelers consent to confiscation of their devices.

a. Under CBP's 2009 Policy, officers may confiscate devices from travelers for a "thorough" search, on-site or off-site. ¶ 5.3.1. The policy does not require that any such confiscation be pursuant to individualized suspicion of wrongdoing.

b. ICE's 2009 Policy permits agents to confiscate devices for a "further review" on-site or off-site. ¶ 8.1.4. The policy expressly provides that agents need no individualized suspicion to do so. ¶ 6.1.

c. The policies also allow for lengthy confiscations. While the default period of CBP confiscation is five days, CBP supervisors may extend this period based on undefined "extenuating circumstances." ¶¶ 5.3.1, 5.3.1.1. Likewise, while the default

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

BORDER SEARCHES AND CONFISCATIONS OF PLAINTIFFS' ELECTRONIC DEVICES

Ghassan Alasaad and Nadia Alasaad

Search 1

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

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

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

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

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

67. After approximately five hours of detention, a CBP officer ordered Ms. Alasaad to provide the password to her locked phone. The Alasaads objected, especially because Ms. Alasaad wears a headscarf in public in accordance with her religious beliefs, and she has photos in her phone of herself without a headscarf and of her daughters that she did not want any CBP officers, especially male officers, to view.

68. The CBP officer told the Alasaads that if they did not disclose the password to Ms. Alasaad's phone, the phone would be confiscated. Because they had no meaningful choice, the Alasaads wrote down the password.

69. The officer coerced the Alasaads into disclosing the password to Ms. Alasaad's phone. Specifically:

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

b. The family had already been detained in the customs inspection building for approximately five hours.

c. The CBP officer threatened to confiscate the phone if they declined to provide the password.

d. The Alasaads were increasingly concerned about their daughter, who was ill and urgently required care and rest.

70. After the Alasaads disclosed the password, the officer told them that they could remain while their phones were searched, or depart and leave their phones behind. Ms. Alasaad told the officer that a male officer could not search her phone because it had photos of herself without a headscarf. The officer told them that it would take two hours for a female officer to arrive, and then more time to search the phone. Based on what they

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

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

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

Search 2

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

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

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

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

Suhaib Allababidi

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

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

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

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

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

Sidd Bikkannavar

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

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

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

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

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

information: Collection of this information is mandatory . . . . Failure to provide information to assist CBP or ICE in the copying of information from the electronic device may result in its detention and/or seizure."

c. Mr. Bikkannavar understood this form to mean that CBP was asserting a legal prerogative to search the contents of his phone, and that if he refused to disclose his phone password, CBP would respond by seizing his device and copying his information.

d. The first time the officer ordered Mr. Bikkannavar to disclose his phone password, Mr. Bikkannavar refused to do so, and explained that the phone belonged to his employer. He pointed out the JPL barcode and the JPL asset tag on the back of the phone. The agent then repeated his order to disclose the phone's password. Mr. Bikkannavar complied because the agent insisted.

e. Officers did not answer Mr. Bikkannavar's questions.

f. Mr. Bikkannavar was in danger of missing his connecting flight from Houston to Los Angeles.

83. When Mr. Bikkannavar disclosed his phone password, the officer wrote it down and took the password and the phone to another room.

84. After about 30 minutes, the officer returned the phone to Mr. Bikkannavar and informed him that officers had used "algorithms" to search the contents of the phone, indicating that they used one or more forensic tools.

85. The officer also informed Mr. Bikkannavar that officers had not found any "derogatory" information about him.

Jérémie Dupin

Search 1

86. On December 22, 2016, Mr. Dupin flew from Port-au-Prince, Haiti, to Miami, Florida, where he had a connecting flight to Montreal, Quebec, to visit his daughter and take her by bus to New York City for Christmas. He had a locked smartphone with him that he used for both his work as a journalist and personal matters.

87. At the passport control area of the Miami airport, a CBP officer directed Mr. Dupin to a secondary inspection area. Mr. Dupin waited there for more than two hours. Three officers then escorted him to a smaller room, where they asked him specific questions about his work as a journalist, including the names of the organizations and specific individuals within those organizations for whom he had worked.

88. During the questioning, the officers seized Mr. Dupin's phone and ordered him to provide the password to the phone. Because he had no meaningful choice, Mr. Dupin provided the password.

89. The officers coerced Mr. Dupin into disclosing his phone password. Specifically:

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

b. Mr. Dupin was alone in an interrogation room with three CBP officers. He understood, based on the CBP officers' tone and demeanor, that they were commanding him to disclose his password.

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

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

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

Search 2

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

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

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

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

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

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

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

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

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

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

Aaron Gach

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

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

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

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

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

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

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

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

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

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

Isma'il Kushkush

Search 1

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

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

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

Search 2

108. On January 4, 2017, Mr. Kushkush traveled to Washington, D.C. from Israel, where he had completed an internship with the Associated Press through funding from the Overseas Press Club Foundation. He carried with him a locked smartphone that he used for both professional and personal matters, and that contained his journalistic work product, work-related photos, and lists of contacts. He also carried the same locked laptop that had been previously seized by CBP, an unlocked digital camera, an unlocked voice recorder, and multiple unlocked flash drives.

109. When Mr. Kushkush arrived at Dulles International Airport, CBP officers took him to a secondary inspection area, where they questioned him, searched his notebooks, and asked about his reporting activities. They also asked Mr. Kushkush for his social media identifiers and his email address.

110. A CBP officer demanded to see Mr. Kushkush's phone and told him to unlock it. Because he had no meaningful choice, Mr. Kushkush reluctantly complied.

111. The CBP officer coerced Mr. Kushkush into unlocking his phone. Specifically:

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

b. Mr. Kushkush understood, based on the CBP officer's tone and demeanor, that he was commanding Mr. Kushkush to unlock his phone.

112. Mr. Kushkush observed the CBP officer manually searching through the contents of his phone. CBP officers also took Mr. Kushkush's laptop, voice recorder, camera, flash drives, and notebooks into another room for approximately 20 minutes. On

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

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

Search 3

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

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

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

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

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

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

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

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

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

Diane Maye

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

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

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

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

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

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

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

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

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

Zainab Merchant

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

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

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

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

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

CBP officer told her that if she gave them the password, they would look through the phone quickly, but if she did not give them the password, they would detain the phone indefinitely.

130. Ms. Merchant said she was traveling alone, and that if she did not have a phone she would have no means of communicating. She also said that she needed the phone for her work and studies. A CBP officer reiterated that she could choose to unlock the phone, or have it seized indefinitely.

131. In tears, Ms. Merchant unlocked her phone. She also provided the password to unlock her laptop.

132. The CBP officers coerced Ms. Merchant into unlocking her phone and providing the password to her laptop. Specifically:

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

b. CBP officers told Ms. Merchant that they would seize her phone indefinitely if she did not unlock it.

c. Ms. Merchant was traveling alone and needed her phone to communicate with her family.

133. CBP officers then began questioning Ms. Merchant about the purpose of her trip, her religious affiliation, and her blog. They specifically asked about an article she had written on her blog that described a previous border crossing experience.

134. After approximately two hours, officers gave Ms. Merchant her phone and laptop and permitted her to leave the U.S. customs preclearance area.

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

Akram Shibly

Search 1

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

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

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

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

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

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

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

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

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

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

Search 2

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

144. At the customs checkpoint, a CBP officer again directed Mr. Shibly to a secondary inspection area inside the border station. There, a CBP officer ordered Mr. Shibly to hand over his phone. Mr. Shibly declined to do so, since officers had seized and searched his phone only three days earlier.

145. Three CBP officers approached him and used physical force to seize his phone. One of the officers squeezed his hand around Mr. Shibly's throat, causing Mr. Shibly to suffer great pain and fear of death. Another officer restrained Mr. Shibly's legs, and a third officer pulled Mr. Shibly's phone from his pocket. Additional officers stood in a circle around Mr. Shibly. At no time did Mr. Shibly physically resist.

146. A CBP officer took Mr. Shibly's phone to a separate room, out of his sight. On information and belief, one or more CBP officers searched Mr. Shibly's phone during this time: they had the means to do so (the screen lock was still not engaged), and they had no reason to seize the phone other than to search it.

Matthew Wright

147. During March and April 2016, Matthew Wright traveled through Southeast Asia, where he participated in four Ultimate Frisbee tournaments and spent time with friends. On April 21, 2016, he flew from Tokyo, Japan, to Denver, Colorado. He had a locked smartphone, a locked laptop computer, and a camera without a locking feature.

148. At the passport control area of the Denver airport, a CBP officer directed Mr. Wright to a separate inspection area. The officer removed Mr. Wright's laptop from its bag and ordered Mr. Wright to unlock it. Mr. Wright declined to do so. In response, CBP officers confiscated Mr. Wright's locked laptop, locked phone, and camera.

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

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

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

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

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

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

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

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

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

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

FACTS RELEVANT TO ALL PLAINTIFFS

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

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

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

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

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

based accounts observed during the searches, (c) their social media identifiers, and/or (d) their device passwords.

158. Plaintiff Allababidi is suffering the ongoing harm of the confiscation of his device. He is also at imminent risk of suffering a device search so long as his device remains in CBP or ICE's possession.

159. For these reasons, Plaintiffs are suffering and will continue to suffer irreparable harm, and have no adequate remedy at law.

160. Plaintiffs have a reasonable expectation of privacy in the content their electronic devices contain, in the content they store in the cloud that is accessible through their electronic devices, in their device passwords, and in the nature of their online presence and their social media identifiers.

161. Plaintiffs use their devices to communicate, associate, and gather and receive information privately and anonymously. Plaintiffs Dupin and Kushkush also use their devices to store sensitive journalistic work product and identifying information about their confidential sources.

162. Plaintiffs, and the many other travelers who cross the United States border every year with electronic devices, will be chilled from exercising their First Amendment rights of free speech and association, in knowing that their personal, confidential and anonymous communications and expressive material may be viewed and retained by government agents without any wrongdoing on their part.

163. Plaintiffs feel confused, embarrassed, upset, violated, and anxious about the search and confiscation of their devices. They worry that the CBP officers viewed personal information from their devices, including photos and messages; downloaded and

retained that information; and shared it with other government agencies. This worry includes their own personal information, and also personal information from and about other people, including friends, family, and professional associates.

164. Defendants have directly performed, or aided, abetted, commanded, encouraged, willfully caused, participated in, enabled, contributed to, or conspired in the device searches, device confiscations, policies, and practices alleged above.

165. By the acts alleged above, Defendants have proximately caused harm to Plaintiffs.

166. Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of Plaintiffs' constitutional rights.

167. Defendants will continue to violate Plaintiffs' constitutional rights unless enjoined from doing so by this Court.

COUNT I:
Fourth Amendment claim for searching electronic devices
(by all Plaintiffs against all Defendants)

168. Plaintiffs herein incorporate by reference the allegations above.

169. Defendants violate the Fourth Amendment by searching the content that electronic devices contain, absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws, and without particularly describing the information to be searched.

COUNT II:
First Amendment claim for searching electronic devices
(all Plaintiffs against all Defendants)

170. Plaintiffs herein incorporate by reference the allegations above.

171. Defendants violate the First Amendment by searching electronic devices that contain expressive content and associational information, absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws, and without particularly describing the information to be searched.

COUNT III:
Fourth Amendment claim for confiscating electronic devices
(by Plaintiffs Ghassan and Nadia Alasaad, Allababidi, and Wright against all Defendants)

172. Plaintiffs herein incorporate by reference the allegations above.

173. Defendants violate the Fourth Amendment by confiscating travelers' electronic devices, for the purpose of effectuating searches of those devices after travelers leave the border, absent probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws. These confiscations are unreasonable at their inception, and in scope and duration.

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully request that this Court:

A. *Declare* that Defendants' policies and practices violate the First and Fourth Amendments by authorizing searches of travelers' electronic devices, absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws, and without particularly describing the information to be searched.

B. *Declare* that Defendants violated Plaintiffs' First and Fourth Amendment rights by searching their electronic devices absent a warrant supported by probable cause

that the devices contained contraband or evidence of a violation of immigration or customs laws, and without particularly describing the information to be searched.

C. *Enjoin* Defendants from searching electronic devices absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws, and without particularly describing the information to be searched.

D. *Declare* that Defendants' policies and practices violate the Fourth Amendment by authorizing the confiscation of travelers' electronic devices, for the purpose of effectuating searches of those devices after travelers leave the border, absent probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws.

E. *Declare* that Defendants violated the Fourth Amendment rights of Plaintiffs Ghassan and Nadia Alasaad, Suhaib Allababidi, and Matthew Wright by confiscating their electronic devices, to effectuate searches of their devices after they left the border, absent probable cause that the devices contained contraband or evidence of a violation of immigration or customs laws.

F. *Declare* that Defendants violated the Fourth Amendment rights of Plaintiffs Ghassan and Nadia Alasaad, Suhaib Allababidi, and Matthew Wright by confiscating their electronic devices, both locked and unlocked, for a period of unreasonable duration.

G. *Enjoin* Defendants (i) from confiscating travelers' electronic devices, to effectuate searches of those devices after travelers leave the border, absent probable

cause that the devices contain contraband or evidence of a violation of immigration or customs laws, and (ii) in such cases, promptly to seek a warrant to search the device.

H. *Enjoin* Defendants to return Plaintiff Allababidi's phone.

I. *Enjoin* Defendants to expunge all information gathered from, or copies made of, the contents of Plaintiffs' electronic devices, and all of Plaintiffs' social media information and device passwords.

J. *Award* Plaintiffs reasonable attorney's fees and costs.

K. *Grant* such other and further relief as the Court deems proper.

DATED: September 13, 2017

Respectfully submitted:

Adam Schwartz
(*pro hac vice* pending)
Sophia Cope
(*pro hac vice* pending)
Aaron Mackey
(*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333 (phone)
(415) 436-9993 (fax)
adam@eff.org
sophia@eff.org
amackey@eff.org

Esha Bhandari
(*pro hac vice* pending)
Hugh Handeyside
(*pro hac vice* pending)
Nathan Freed Wessler
(*pro hac vice* pending)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street,
18th Floor
New York, NY 10004
(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

/s/ *Jessie J. Rossman*
Jessie J. Rossman
BBO #670685
Matthew R. Segal
BBO #654489
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS
211 Congress Street
Boston, MA 02110
(617) 482-3170 (phone)
(617) 451-0009 (fax)
jrossman@aclum.org
msegal@aclum.org

Counsel for Plaintiffs

Certificate of Service

I, Jessie J. Rossman, hereby certify that on September 13, 2017, I filed the foregoing document electronically with the Clerk of the Court through ECF, which will send a Notice of Electronic Filing to the registered participants.

DATE: September 13, 2017 */s/ Jessie J. Rossman*

Jessie J. Rossman