CHARLES D. SWIFT, TX SB# 24091964, *Pro Hac Vice* pending
E-Mail: cswift@clcma.org
CHRISTINA A. JUMP, TX SB# 00795828, *Pro Hac Vice* pending
E-Mail: cjump@clcma.org
Constitutional Law Center for Muslims in America (CLCMA)
833 E. Arapaho Rd., Ste. 102
Richardson, Texas 75081
Telephone: 972.914.2507; Facsimile: 972.692.7454

JEFFREY S. RANEN, CA SB# 224285
E-Mail: Jeffrey.Ranen@lewisbrisbois.com
PARISA KHADEMI, CA SB# 271897
E-Mail: Parisa.Khademi@lewisbrisbois.com
MARGARET R. WRIGHT, CA SB# 312272
E-Mail: Margaret.Wright@lewisbrisbois.com
Lewis Brisbois Bisgaard & Smith LLP
633 West 5th Street, Suite 4000
Los Angeles, California 90071
Telephone: 213.250.1800; Facsimile: 213.250.7900

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

HAISAM ELSHARKAWI,

Plaintiff,

vs.

UNITED STATES OF AMERICA;

KIRSTJEN NIELSEN, THE DEPARTMENT OF HOMELAND SECURITY, *in her official capacity*;

KEVIN K. MCALEENAN, CUSTOMS AND BORDER PROTECTION, *in his official capacity*;

OFFICER FNU RIVAS, *in his individual*

Case No.: _____

COMPLAINT FOR DAMAGES

capacity;

OFFICER FNU RODRIGUEZ, *in his individual capacity*;

OFFICER FNU STEVENSON, *in his individual capacity*;

OFFICER JENNIFER LNU, *in her individual capacity*,

Defendants.

PLAINTIFF'S ORIGINAL COMPLAINT

Plaintiff Haisam Elsharkawi, through his attorneys, hereby files this Plaintiff's Original Complaint, alleging violations of the First, Fourth, and Fifth Amendments of the U.S. Constitution, and the Federal Tort Claims Act, and in support thereof shows the following:

I. Nature of the Action

1. Plaintiff Haisam Elsharkawi ("Plaintiff" or "Mr. Elsharkawi") is a United States citizen of Egyptian descent residing in Orange County. Mr. Elsharkawi was departing the United States for religious pilgrimage to Saudi

2. Arabia when U.S. Customs and Border Protection ("CBP") agents[1] stopped Mr. Elsharkawi for an extensive, non-routine search as he boarded his outbound flight. On information and belief, neither individualized nor reasonable

[1] Though Mr. Elsharkawi is certain some of the agents involved were CBP agents, others introduced themselves simply as agents of the Department of Homeland Security ("DHS"), which could include Immigrations and Customs Enforcement ("ICE") and Homeland Security Investigations ("HSI") agents, among others.

suspicion supported this search. During this search, CBP agents so aggressively questioned Mr. Elsharkawi that he felt compelled to request an attorney. The CBP agents also searched Mr. Elsharkawi's checked and carry-on luggage, and asked him to unlock his cellphone. When Mr. Elsharkawi exercised his right to refuse to unlock his phone, the CBP agents handcuffed him, took him to a holding cell, and detained him until he had no reasonable alternative but to unlock his cellphone. Mr. Elsharkawi suffered physical and emotional harm and missed his scheduled flight as a result of the CBP agents' actions.

3. DHS and its constituent agencies stopped Mr. Elsharkawi, searched and reviewed the data accessible through and/or contained on his electronic devices. Upon information and belief, DHS and its constituent agencies retained and shared Mr. Elsharkawi's digital information pursuant to DHS policies regarding search of electronic devices at the border.

4. Mr. Elsharkawi brings this action against Defendants Kirstjen Nielsen and Kevin K. McAleenan in their official capacities to challenge the constitutionality of the Policy under the First, Fourth, and Fifth Amendments of the U.S. Constitution. Mr. Elsharkawi further seeks redress against Defendant the United States under the Federal Tort Claims Act, and against Defendants Officers Rivas, Rodriguez, Stevenson, and Jennifer in their individual capacities for violations of 42 U.S.C. § 1981.

/ / /

II. Jurisdiction and Venue

5. This Court has jurisdiction pursuant to 28 U.S.C. § 1331 and the Federal Tort Claims Act ("FTCA"), 28 U.S.C. § 1346(b)(1), 28 U.S.C. §§ 2201 and 2202, and Federal Rules of Civil Procedure 57 and 65 authorize declaratory and injunctive relief in this matter.

6. Venue is proper in the Central District of California under 28 U.S.C. § 1391(e)(1) because Mr. Elsharkawi resides in this District, specifically Orange County, and a substantial part of the events giving rise to Mr. Elsharkawi's claims occurred in this District, specifically Los Angeles County.

III. Parties

7. Plaintiff Haisam Elsharkawi is a U.S. citizen residing in Orange County, California. He is of Egyptian descent and is a practicing Muslim.

8. The United States of America is a sovereign entity that has waived its immunity in certain circumstances under the Federal Torts Claims Act, 28 U.S.C. §§ 1346(b) & 2671 *et seq*.

9. Kirstjen Nielsen is Secretary of the Department of Homeland Security ("DHS"). As head of DHS, Secretary Nielsen has authority over all DHS policies, procedures, and practices related to border searches, including those challenged in this lawsuit. Defendant Nielsen is sued in her official capacity.

10. Kevin K. McAleenan is Acting Commissioner of CBP. Acting Commissioner McAleenan has authority over all CBP policies, procedures, and

practices relating to border searches, including those challenged in this lawsuit. Defendant McAleenan is sued in his official capacity.

11. The CBP and DHS Officers involved in the search, interrogation, and detention of Mr. Elsharkawi include, but are not limited to, Officer FNU Rivas, Officer FNU Rodriguez, Officer FNU Stevenson, and Officer Jennifer LNU.[2] These Officers are sued in their individual capacities.

IV. Relevant Policies

12. CBP promulgated a policy in October 2009, CBP Directive No. 3340-049,[3] regarding the search of electronic devices at the U.S. border (the "2009 Policy"). The 2009 Policy permitted CBP to search travelers' electronic devices at the border without individualized or reasonable suspicion, and to copy, retain, and share the information found in such devices. The 2009 Policy, by its terms, applied equally to those entering and exiting the United States.

13. On January 4, 2018, CBP issued a directive superseding the 2009 Policy, CBP Directive No. 3340-049A ("2018 Policy"), purporting to clarify the

[2] Plaintiff Mr. Elsharkawi reserves the right to amend this Complaint to include claims against as yet unidentified Defendants, should Plaintiff uncover facts during discovery that would support such claims.

[3] The U.S. Immigration and Customs Enforcement ("ICE") has promulgated a comparable directive permitting it to search and copy electronic devices, as ICE has concurrent border search powers with CBP. *See generally* ICE Directive No. 7-6.1 (Border Searches of Electronic Devices), U.S. Immigration and Customs Enforcement (Aug. 18, 2009) (scheduled to be reviewed on Aug. 18, 2012) (hereinafter cited as "ICE Policy"). The ICE Policy has not been updated as of the filing of this Complaint, however, the 2018 Policy section 2.7 cites the ICE Policy and states "when CBP, seizes, or retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this [Policy] and ICE policy will apply upon receipt by ICE."

"standard operating procedures for searching, reviewing, retaining, and sharing information contained in [electronic devices] subject to inbound and outbound border searches by [CBP]."[4]

14. The stated purposes of the 2018 Policy are as follows: (1) "detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography"; (2) "reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations"; and (3) "determin[e] . . . an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws." The 2018 Policy's purpose also states searches incident to the 2018 Policy "can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information."[5]

15. The 2018 Policy's search provisions mirror the 2009 Policy's analogous provisions, except that the 2018 Policy purports (a) to clarify and make uniform the 2009 Policy by distinguishing between "basic" and "advanced"

[4] 2018 Policy, § 1 (Purpose). Notably, the 2018 Policy and 2009 Policy are substantially the same: their stated purposes and their substantive provisions governing search, seizure, retention, and sharing of data on electronic devices at the border are nearly identical when read side-by-side. Plaintiff provides parallel citations to the relevant sections of each of the Policies in the margin below.

[5] *Compare* 2018 Policy, § 1, *with* 2009 Policy, § 1. With the exception of the wording of the third numbered purpose identified in the text and the risk assessment language, the Policies' purposes are identical.

searches, and (b) to confirm and make explicit pre-existing practices developed under the 2009 Policy for handling cloud-based data.[6]

16. Specifically, the 2018 Policy requires reasonable suspicion for "advanced searches,"[7] but permits any other kind of search "with or without suspicion." Moreover, an advanced search in furtherance of a "national security concern" requires no level of suspicion at all.[8]

17. Further, the 2018 Policy "formally clarifies that a border search includes an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications."[9] In other words, CBP confirmed in the 2018 Policy its position that, "under no circumstances may Officers 'intentionally use the device [searched] to access information that is solely stored remotely'"—i.e., cloud-based data. The

[6] *Compare* 2018 Policy, § 5.1 (Border Searches), *with* 2009 Policy, § 5.1 (same).

[7] The 2018 CBP Policy 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."

[8] Although the 2018 CBP Policy purports to require "reasonable suspicion" for an advanced search, it also permits such a search, seemingly without reasonable suspicion, when a CBP Officer confronts a "national security concern." The Policy does not expressly define "national security concern." Instead, it provides only two examples of situations that might lead a CBP Officer to conclude a "national security concern" exists: "existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list." It is unclear on the face of the Policy—particularly in light of the provided examples—how an officer might conclude a device's digital content poses a national security concern without reasonable suspicion of the same. *See* 2018 Policy, § 5.1.4; *see also id.* § 1 (suggesting CBP may conduct such searches to inform "risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item").

[9] *Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices*, DHS/CBP/PIA-008(a) (Jan. 4, 2018), at 8 (citing 2018 Policy, § 5.1.2).

federal government's internal guidance has indicated since as early as 2014 that "a routine border search 'may not be stretched'" [10] to cover cloud-based data, and CBP acknowledged this restriction in April 2017.[11]

18. The 2018 Policy also permits CBP to seize an electronic device (and its data), retain the device or information for review, and share copies of information discovered as a result with other federal, state, and foreign agencies.[12]

19. Specifically, the 2018 Policy permits CBP to seize "electronic devices, or copies of information contained therein, . . . in order to perform a thorough border search." It sets time frames for seizure of the device and for destruction of any data copied therefrom; CBP may extend these time frames at its discretion. However, CBP may also retain a device or copies of its information if it finds probable cause exists to seize the device or the information. "Without probable cause . . . , CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice."

---

[10] Shappert, Gretchen C.F., *The Border Search Doctrine: Warrantless Searces of Electronic Devices after* Riley v. California, UNITED STATES ATTORNEYS' BULLETIN: BORDER ISSUES, at 13 (observing under *Riley v. California*, 134 S. Ct. 2473 (2014), that "[i]f a search incident to arrest 'may not be stretched' to cover cloud data, then a routine border search 'may not be stretched' either").

[11] In response to June 20, 2017 Due Diligence Questions for Kevin McAleenan from Senator Wyden, McAleenan explained "CBP does not access information found only on remote servers through an electronic device presented for examination" and referencing "a nationwide muster on April 2017 reminding [CBP] officers of this precise aspect of CBP's border search policy." *See* http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/170712-cpb-wyden-letter.pdf, at Questions 1.c., 4.

[12] *Compare* 2018 Policy, §§ 5.4-5.5, *with* 2009 Policy, §§ 5.3-5.4.

20. The 2018 Policy permits CBP to share devices and copies of information therein with federal, state, local, and foreign law enforcement agencies. Once CBP has shared a device or its data, the 2018 Policy does not guarantee the return of the device or its data from the other agency.

21. The 2018 Policy does not authorize detention of *an individual* whose electronic device is being searched.[13]

22. CBP has selectively released information about the searches it conducts and has failed to publicize basic information about its enforcement of either of the Policies.[14] For example, CBP has not publicized the number of advanced (as opposed to "basic") searches it has conducted, the number of phones it has detained, the number of copies of information it has made, or the number of times it has shared such information with other entities. At the time of this filing, CBP has merely released information about the overall number of searches conducted pursuant to the 2009 Policy.[15]

---

[13] The 2009 Policy did not authorize detention of an individual either. *See generally* 2009 Policy.

[14] CBP has in place systems for monitoring its enforcement of the Policies, and keeps data on this enforcement. *See* 2018 Policy, § 6 ("CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.").

[15] U.S. Customs and Border Protection, *CBP Releases Statistics on Electronic Device Searches* (Apr. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0; U.S. Customs and Border Protection, *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics* (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

23. Plaintiff requests that the Court take judicial notice of both the 2009 Policy, the 2018 Policy, and the ICE Policy.

V. Electronic Devices

24. Electronic devices are qualitatively and quantitatively different from any other type of object a person might carry with them across the border, such as a briefcase, luggage, or a backpack.

25. Almost every person crossing the U.S. border carries a cellphone or other electronic device in tow, as cellphone use is pervasive and essential. As of January 10, 2018, 95% of Americans owned a cellphone (with 77% owning a smartphone), and 53% owned a tablet computer.[16] These devices are multi-functional, serving as telephones, computers, cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

26. The modern cellphone has immense storage capacity, with the ability to hold 256GB of data, if not more.[17] Many travelers do not solely travel with a cellphone, but have their laptops and tablets with them as well, thereby enlarging the amount of data they carry across the border. Further, with cloud-based data, the amount of storage accessible through the modern cellphone is almost limitless.

[16] PEW RESEARCH CENTER, *Mobile Fact Sheet*, http://www.pewinternet.org/fact-sheet/mobile/ (Jan. 31, 2018).

[17] APPLE INC., *iPhone 8 Tech Specs*, https://www.apple.com/iphone-8/specs/ (accessed Feb. 1, 2018).

27. Cellphones today contain an immense amount of personal, expressive, and associational information. These devices collect in one place many distinct types of information that reveal much more in combination than any isolated record. Further, the depth of these records spans years. Indeed, individuals may not even be aware of all the information contained in their devices, as "deleted" items can remain in the device in other forms.

28. The use of electronic devices has become essential, especially during travel, such that to leave one's electronic devices at home is improbable, irresponsible, and difficult. Personal and professional communications, daily task-managing, and record-keeping overwhelmingly take place electronically in today's world.

VI. Facts

29. On February 9, 2017, Mr. Elsharkawi arrived at Los Angeles International Airport ("LAX") to board a flight via Turkish Airlines to Saudi Arabia for religious pilgrimage.[18]

30. Mr. Elsharkawi printed off his boarding pass and checked in one bag, with no issues.

[18] Mr. Elsharkawi has, in the past, regularly traveled to Egypt to visit his family in 2009, 2013, and 2016. At all times, he traveled with his electronic devices. Mr. Elsharkawi hopes to visit family abroad again this summer along with completing the pilgrimage CBP interfered with previously. At the very least, Mr. Elsharkawi will travel to Saudi Arabia to complete the Hajj in accordance with his sincerely held religious belief that such pilgrimage is religiously obligatory upon him at least once in his lifetime. He intends to continue to travel abroad with his electronic devices, as traveling without them would cause great hardship—he would be unable to communicate with his family, unable to conduct business, etc.

31. Mr. Elsharkawi does not believe he had a Secondary Security Screening Selection ("SSSS") designation from the Transportation Security Administration ("TSA") on his boarding pass that day, which usually causes an individual to receive extra security screening. Mr. Elsharkawi believes that he has never had an SSSS designation on any of his boarding passes.

32. Mr. Elsharkawi passed through the TSA security screening with no issues, as well.

33. Mr. Elsharkawi then waited at the gate to board his flight.

34. Mr. Elsharkawi was in the process of boarding his flight when he was pulled out of the boarding line by CBP Officer FNU Rivas ("Officer Rivas").

35. Officer Rivas asked Mr. Elsharkawi where he was traveling to, how long his stay was planned for, if he was meeting anyone during his stay, and how much currency he currently had on him.

36. Mr. Elsharkawi had a little over $2,500 on him, which he accurately declared.

37. After Mr. Elsharkawi answered all of these questions, Officer Rivas asked Mr. Elsharkawi to follow him to a table, where Officer Rivas repeated the same questions while searching his carry-on bag.

38. Officer Rivas then proceeded to ask Mr. Elsharkawi about his previous visits to Egypt and the reasons for those visits, what family Mr. Elsharkawi has in Egypt and Saudi Arabia, if any, when Mr. Elsharkawi had initially arrived to the

U.S., and when Mr. Elsharkawi had gained his citizenship. Mr. Elsharkawi calmly and politely answered all questions, despite many being repetitive.

39. As the questioning continued and became increasingly aggressive, Mr. Elsharkawi asked if there was a problem and whether he needed an attorney. Officer Rivas then accused Mr. Elsharkawi of hiding something because of his request for an attorney.

40. Five other CBP officers then approached the table where Mr. Elsharkawi was being questioned.

41. One of the officers, Officer FNU Rodriguez ("Officer Rodriguez"), asked Mr. Elsharkawi what his problem was and stated that the officers were just doing their job. Officer Rodriguez further threatened Mr. Elsharkawi that he should cooperate or he would miss his flight. Mr. Elsharkawi responded that he was merely asking if he needed an attorney. Officer Rodriguez reiterated Mr. Elsharkawi's risk of missing his flight if he did not cooperate with the questioning. Officer Rodriguez then told Mr. Elsharkawi to put his hands on his head and, following this admonishment, searched Mr. Elsharkawi. Officer Rodriguez pulled out Mr. Elsharkawi's phone from his pocket and asked him to unlock it. Mr. Elsharkawi responded that he was not going to unlock his phone and that he refused to answer any further questions until he had an attorney.

42. At this point, Mr. Elsharkawi's checked bag was brought to the gate by another CBP officer.

43. Officer Rodriguez told Mr. Elsharkawi that if he refused to unlock the phone, CBP would seize it. Mr. Elsharkawi responded that he would not unlock it, and was not giving permission for his phone to be seized.

44. Another CBP officer told Mr. Elsharkawi that if he cooperated, he would be released in no time. Mr. Elsharkawi responded that he wanted his rights, he did not want to be treated as a criminal for no apparent reason, and that he wanted an attorney. The CBP officer told Mr. Elsharkawi he was not under arrest so he had no right to an attorney. Mr. Elsharkawi then requested his release.

45. Officer Rivas ignored the request and began searching Mr. Elsharkawi's carry-on bag again.

46. Mr. Elsharkawi asked for his phone back to make a call. Officer Rodriguez responded by stating that Mr. Elsharkawi had an attitude, was obviously racist, and had a problem with the uniform of CBP officers. Officer Rodriguez told Mr. Elsharkawi to put his hands behind his back, and handcuffed him.

47. Officer Rodriguez, along with two other CBP officers, then began pulling Mr. Elsharkawi into an elevator.

48. At this point, Mr. Elsharkawi feared for his safety. He turned to a nearby flight attendant and yelled to her, "Please call a lawyer for me!"

49. When Mr. Elsharkawi was taken into the elevator and reached another floor of the airport, he again loudly yelled out, "Someone help, someone call a lawyer for me. They said I'm not under arrest even though I'm handcuffed and they

are taking me somewhere that I don't know and will not let me have a lawyer."

50. Officer Rodriguez then pushed Mr. Elsharkawi's arms up to his neck, to the point that Mr. Elsharkawi feared they would break.

51. One of the CBP officers stated that Mr. Elsharkawi was causing a lot of problems, and recommended taking him downstairs.

52. Mr. Elsharkawi was taken through a room, where again he yelled out.

53. Mr. Elsharkawi was then placed in a holding cell, with one of his hands handcuffed to a bench.

54. After some time passed, Officer FNU Stevenson ("Officer Stevenson") came to Mr. Elsharkawi, introduced himself as a supervisor, and asked Mr. Elsharkawi why he was not cooperating. Officer Stevenson stated that they had not wanted things to get to this point, they did not single Mr. Elsharkawi out, and they were just protecting the country. Officer Stevenson explained that they would only ask him a few questions, and if Mr. Elsharkawi unlocked his phone, he would be free to go. Mr. Elsharkawi responded that he would not unlock his phone because it was an invasion of his privacy, and that the CBP officers had already made him miss his flight. Officer Stevenson stated that the airline would refund his flight because it knew Mr. Elsharkawi was with CBP officers, or it would rebook the flight for tomorrow. Officer Stevenson further explained that they needed to check Mr. Elsharkawi's phone because CBP protects the country by checking for narcotics, child pornography, and terrorism.

55. Mr. Elsharkawi has never been charged with, or investigated for, allegations of narcotics or child pornography. He has never been charged with any terrorism-related offenses. Therefore, Mr. Elsharkawi remained unaware of why he was being held and unable to leave.

56. Officer Stevenson later returned, asking Mr. Elsharkawi if he was willing to come and answer a few questions while they searched his bags in front of him.

57. Mr. Elsharkawi left the holding cell and was questioned by Officer Stevenson again, while Officer Rivas searched his bags.

58. The officers expressed no interest in searching his iPad, despite seeing it and removing it while searching his bags.

59. Officer Stevenson questioned Mr. Elsharkawi about his work, whether he attended school, his address, how he became a citizen, his wife and her work and school, his children, how old they were, their names and the schools they attended. Officer Stevenson again asked Mr. Elsharkawi to unlock his phone. Mr. Elsharkawi again refused. Officer Stevenson informed Mr. Elsharkawi that he was seizing Mr. Elsharkawi's phones.

60. After more time passed, Officer Jennifer LNU ("Officer Jennifer") approached Mr. Elsharkawi and introduced herself as a DHS officer. Officer Jennifer stated DHS was protecting the country, she wanted to ask a few questions, and she wanted Mr. Elsharkawi to unlock his phone. Mr. Elsharkawi again

responded that he would not unlock his phone. Officer Jennifer stated that was fine, but they would, as a result, seize his phone and send it back to him in thirty days. Officer Jennifer asked Mr. Elsharkawi the same questions Officer Stevenson had. Officer Jennifer asked Mr. Elsharkawi his mailing address and began putting his phones in a bag, reiterating they would seize them and send them back to him.

61. Mr. Elsharkawi then asked Officer Jennifer "Are you okay with some stranger taking your phone and looking through your phone and pictures?" Officer Jennifer responded that she would not be okay with it, but she would do it if it were about someone doing his or her job to protect the country.

62. Mr. Elsharkawi stated that he had pictures of his wife without her headscarf on his phone, and this was an additional reason why he did not want his phone searched.

63. Officer Jennifer offered to search the phone herself. Mr. Elsharkawi asked how long the search would take and Officer Jennifer responded that it would take about ten to fifteen minutes.

64. Defeated, and seeing no alternative, Mr. Elsharkawi felt he had no choice but to acquiesce and unlocked his phone.

65. Officer Jennifer then searched his phone and began questioning him regarding his eBay and Amazon accounts, where he got merchandise for his e-commerce business, and what swap meets he frequents. Officer Jennifer also commented that Mr. Elsharkawi had a lot of apps and a lot of unread emails on his

phone.

66. Officer Jennifer asked Mr. Elsharkawi to unlock his other phone, which had been in his carry-on bag. Mr. Elsharkawi responded that it was not locked. Officer Jennifer searched the second phone and asked why he did not have anything on this phone. Mr. Elsharkawi responded that he recently got it for business, and he usually only uses it for receiving phone calls.

67. Officer Jennifer then informed him she was done and he was free to take his things and leave.

68. After being interrogated for four hours, Mr. Elsharkawi missed his flight. Turkish Airlines refused to give him a refund, contrary to Officer Stevenson's representation.

69. Mr. Elsharkawi has exhausted all available administrative remedies, by filing all appropriate complaints with DHS and CBP. Specifically, Mr. Elsharkawi submitted an application to the DHS Traveler Redress Inquiry Program ("DHS TRIP") on August 4, 2017, a complaint to the CBP Information Center on August 1, 2017, a report to the DHS Office of Inspector Genera ("DHS OIG") on August 1, 2017, and a Civil Rights Complaint to the DHS Office for Civil Rights and Civil Liberties ("DHS OCRCL") on August 15, 2017. To date, Mr. Elsharkawi has received no responses from the relevant agencies.

/ / /

/ / /

70. Pursuant to 28 U.S.C. § 2675 and 28 C.F.R. § 14.2(a), Mr. Elsharkawi presented his FTCA claims to DHS and CBP via letter with a completed Standard Form 95 on August 1, 2017. To date, Mr. Elsharkawi has received no response.

71. Mr. Elsharkawi will be irreparably harmed absent injunctive relief from this Court, as he will be unable to travel to Egypt to visit family or Saudi Arabia for religious pilgrimage, without fear that his electronic devices will be searched again, that his data will be seized, and that he will be arrested, all in violation of the Constitution. To avoid these harms, Mr. Elsharkawi will either have to give up his sincerely held religious beliefs, forgo international travel to visit his family, or endure the hardship of international travel without electronic devices. Further, Mr. Elsharkawi already has lost the benefit of one contract, namely his ticket with Turkish Airlines to fly to Saudi Arabia in February 9, 2017, due to Defendants' interference.

VI. Causes of Action

Count 1. Fourth Amendment Claim for Search of Electronic Devices

(against Defendants Nielsen and McAleenan in their official capacities)

72. Mr. Elsharkawi incorporates by reference the entirety of this Complaint as though fully set forth herein.

73. The search of Mr. Elsharkawi's phone was not supported by any real suspicion of ongoing or imminent criminal activity, and as such, no basis for a search existed. Mr. Elsharkawi accurately declared the amount of currency he had

on his person. In any event, CBP could have no reason to search his phone for physical currency. Further, Mr. Elsharkawi has never experienced anything prior to this incident that would indicate he is on any Terrorist Watch List or is being investigated for terrorism, such as SSSS on his boarding pass, or being subjected to additional screening at an airport. Furthermore, Plaintiff has never received any indication of an investigation into his e-commerce business. Finally, Mr. Elsharkawi has never produced, distributed, received, possessed, or otherwise engaged in trafficking of child pornography, or been charged with ever doing so.

74. Accordingly, Defendants Nielsen and McAleenan in their official capacities violated the Fourth Amendment by searching the content of Mr. Elsharkawi's electronic devices, without a warrant supported by probable cause that the devices contained contraband or evidence of a violation of customs laws, and without particularly describing the information to be searched.

Count 2. Fourth Amendment Claim for Seizure of Data

(against Defendants Nielsen and McAleenan in their official capacities)

75. Mr. Elsharkawi incorporates by reference the entirety of this Complaint as though fully set forth herein.

76. Mr. Elsharkawi did not have his cellphone in his possession or sight during his detention. On information and belief, CBP and DHS forensically examined Plaintiff's cellphone, made copies of Plaintiff's cellphone for later forensic examination, and/or transmitted such copies to other agencies for either

technical or subject matter assistance. Defendants needed probable cause to support these actions, but not even reasonable suspicion existed.

77. Accordingly, Defendants Nielsen and McAleenan in their official capacities violated, and continue to violate, the Fourth Amendment by confiscating the data located on and/or accessible through Mr. Elsharkawi's electronic devices, without probable cause that the data contain contraband or evidence of a violation of customs laws. The confiscations were unreasonable from their inception and thereafter in scope and duration.

Count 3. First Amendment Claim for Search of Electronic Devices

(against Defendants Nielsen and McAleenan in their official capacities)

78. Mr. Elsharkawi incorporates by reference the entirety of this Complaint as though fully set forth herein.

79. Defendants Nielsen and McAleenan in their official capacities violated the First Amendment by searching Mr. Elsharkawi's electronic devices that contained expressive content and associational information, without a warrant supported by probable cause that the devices contained contraband or evidence of a violation of customs laws, and without particularly describing the information to be searched.

/ / /

/ / /

/ / /

Count 4. Section 1981 of the Civil Rights Act of 1866 Claim

(against Defendants Rivas, Rodriguez, Stevenson, and Jennifer in their individual capacities)

80. Mr. Elsharkawi incorporates by reference the entirety of this Complaint as if set forth herein.

81. Mr. Elsharkawi, as an American of Egyptian descent, is a member of a racial minority protected by the Civil Rights Act of 1866, as amended in 1991, at 42 U.S.C. § 1981.

82. Defendants Rivas, Rodriguez, Stevenson, and Jennifer improperly interfered with Mr. Elsharkawi's right to exercise and enforce a contract, namely Mr. Elsharkawi's contract with Turkish Airlines to fly as scheduled with his purchased ticket to Saudi Arabia.

83. Defendants Rivas, Rodriguez, Stevenson, and Jennifer intentionally interfered with Mr. Elsharkawi's right to exercise and enforce his contract with Turkish Airlines, and did so because of Mr. Elsharkawi's Egyptian descent and race. Defendant Rivas repeatedly asked Mr. Elsharkawi about Mr. Elsharkawi's previous trips to Egypt and the reasons for those visits, what family Mr. Elsharkawi had in Egypt and Saudi Arabia, if any, when Mr. Elsharkawi had initially arrived to the U.S., and when Mr. Elsharkawi had gained his citizenship. Further, Defendant Rodriguez expressly referenced the difference between his and Mr. Elsharkawi's respective races just before restraining Mr. Elsharkawi.

84. Accordingly, Defendants Rivas, Rodriguez, Stevenson, and Jennifer, in their individual capacities, violated 42 U.S.C. § 1981 by intentionally interfering with Mr. Elsharkawi's right to make and enforce his existing contract with Turkish Airlines, because of Mr. Elsharkawi's Egyptian ancestry and/or race.

Count 5. Federal Tort Claims Act Claims

(against Defendant United States)

85. Mr. Elsharkawi incorporates by reference the entirety of this Complaint as though fully set forth herein.

86. Mr. Elsharkawi brings the claims set forth below against Defendant United States of America under the authority of the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b) & 2671 *et seq*., through which United States has waived its sovereign immunity to the extent that any private person, under like circumstances, would be liable under the relevant substantive state law of the state where the harm occurred.

87. Defendants Nielsen, McAleenan, Rivas, Stevenson, and Jennifer are employees of Defendant United States of America. (For purposes of this Count, Defendants Nielsen, McAleenan, Rivas, Stevenson, and Jennifer are hereinafter and collectively referred to as "Defendant's Employees.")

1. False Arrest/False Imprisonment

88. The allegations set out in this Complaint establish that Defendant's Employees intentionally deprived Mr. Elsharkawi of his freedom of movement by

use of physical barriers, force, and threats of force. The restraint, confinement, and detention compelled Mr. Elsharkawi to stay somewhere for an appreciable time. Mr. Elsharkawi did not knowingly or voluntarily consent to this detention. Mr. Elsharkawi suffered harm. Defendant's Employees' conduct was a substantial factor in causing Mr. Elsharkawi's harm.

89. In the alternative, the acts set forth above establish that Defendant's Employees arrested Mr. Elsharkawi without a warrant. Mr. Elsharkawi suffered harm. Defendant's Employees' conduct was a substantial factor in causing Mr. Elsharkawi's harm.

90. Due to his false arrest and imprisonment, Mr. Elsharkawi suffered harm, and is entitled to damages in an amount to be proved at trial.

2. Battery

91. The allegations set out in this Complaint establish that Defendant's Employees touched Mr. Elsharkawi with the intent to harm or offend him. Mr. Elsharkawi did not consent to this touching. Mr. Elsharkawi was harmed and offended by this conduct. A reasonable person in Mr. Elsharkawi's situation would have been offended by the touching.

92. In the alternative, the acts set out above establish Defendant's Employees intentionally touched Mr. Elsharkawi. Defendant's Employees used unreasonable force to arrest Mr. Elsharkawi. Mr. Elsharkawi did not consent to the use of that force. Mr. Elsharkawi suffered harm as a result of that force; specifically,

Defendant's Employees' use of unreasonable force was a substantial factor in causing Mr. Elsharkawi's harm.

93. Due to the battery, Mr. Elsharkawi suffered physical injuries and emotional distress. He is entitled to damages in an amount to be proved at trial.

3. Negligence

94. The allegations set out in this Complaint establish that Defendant's Employees either did not act or failed to act as a reasonable person would in a similar situation. Such negligent conduct was a substantial factor in causing the harm Mr. Elsharkawi sustained. Defendant's Employees' negligent conduct consisted of wrongfully searching Mr. Elsharkawi's phone, and unlawfully arresting him.

95. Due to this negligence, Mr. Elsharkawi suffered harm, and is entitled to damages in an amount to be proved at trial.

4. Intentional Infliction of Emotional Distress

96. The allegations set out in this Complaint establish that Defendant's Employees' conduct was outrageous. Defendant's Employees intended to cause Mr. Elsharkawi emotional distress and/or acted with reckless disregard of the probability that Mr. Elsharkawi would suffer emotional distress, knowing Mr. Elsharkawi was present when the conduct occurred. Mr. Elsharkawi suffered severe emotional distress. This conduct was a substantial factor in causing Mr. Elsharkawi's severe emotional distress.

97. As a result of this intentional and reckless conduct, Mr. Elsharkawi suffered harm, and is entitled to damages in an amount to be proved at trial.

5. Intrusion into Private Affairs

98. The allegations set out in this Complaint establish that Mr. Elsharkawi had a reasonable expectation of privacy in his cellphone. Defendant's Employees intentionally intruded Mr. Elsharkawi's cellphone. This intrusion would be highly offensive to a reasonable person. Mr. Elsharkawi was harmed. This conduct was a substantial factor in causing Mr. Elsharkawi's harm.

99. Due to this invasion of privacy, Mr. Elsharkawi suffered harm from the loss of his privacy and his emotional distress. He is entitled to damages in an amount to be proved at trial.

VII. Prayer

Wherefore, Plaintiff Mr. Elsharkawi respectfully requests that this Court grant the following relief:

A. Declare that Defendants Nielsen and McAleenan in their official capacities violate the First and Fourth Amendments of the U.S. Constitution by authorizing search of electronic devices carried by persons exiting the United States without a warrant supported by probable cause that the devices contain contraband or evidence of a violation of customs laws, and without particularly describing the information to be searched.

/ / /

B. Declare that Defendants Nielsen and McAleenan in their official capacities violate the Fourth Amendment of the U.S. Constitution by confiscating the data located on and/or accessible through electronic devices carried by persons exiting the United States without probable cause that the data contain contraband or evidence of a violation of customs laws and that the confiscations are unreasonable from their inception and thereafter in scope and duration.

C. Enjoin Defendants Nielsen and McAleenan in their official capacities from acting pursuant to Policy or permitting any federal agent to act pursuant to the Policy so as to search electronic devices and seize data from electronic devices, respectively, without a warrant supported by probable cause that the devices contain contraband or evidence of a violation of customs laws, and without particularly describing the information to be searched, when such persons are exiting the United States;

D. Enjoin Defendants Nielsen and McAleenan in their official capacities to expunge all information gathered from or copies made of the contents of Plaintiff's electronic devices, and all of Plaintiff's device passwords;

E. Order general and compensatory damages, in an amount to be proved at trial, against the United States for its violations of the Federal Tort Claims Act;

F. Order general, compensatory, and punitive and/or exemplary damages in an amount to be proved at trial against the CBP and DHS officers, including but not limited to Defendants Officers Rivas, Rodriguez, Stevenson, and Jennifer;

G. Order that Defendants pay Mr. Elsharkawi reasonable costs and attorneys' fees; and

H. Award such other and further relief as this Court deems just and proper.

DATED: October 31, 2018

Respectfully submitted,

By: /s/ Christina A. Jump
Charles D. Swift
Christina A. Jump
CONSTITUTIONAL LAW CENTER FOR MUSLIMS IN AMERICA (CLCMA)
Pro Hac Vice Counsel for Plaintiff

/s/ Jeffrey S. Ranen
Jeffrey S. Ranen
Parisa Khademi
Margaret R. Wright
LEWIS BRISBOIS BISGAARD & SMITH LLP
Local Counsel for Plaintiff