

**UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF NEW JERSEY**

REJHANE LAZOJA,

Plaintiff

v.

Case No. 18-cv-_____

KRISTJEN NIELSEN, in her official capacity as Secretary of UNITED STATES DEPARTMENT OF HOMELAND SECURITY; KEVIN K. MCALEENAN, in his official capacity as Commissioner, UNITED STATES CUSTOMS AND BORDER PROTECTION; ADELE FASANO, in her official capacity as Port Director, UNITED STATES CUSTOMS AND BORDER PROTECTION; JANE DOE, in her official capacity as an officer, UNITED STATES CUSTOMS AND BORDER PROTECTION; and JOHN DOES 1-2, in their official capacities as officers, UNITED STATES CUSTOMS AND BORDER PROTECTION.

Defendants

MOTION DAY: September 17, 2018

ORAL ARGUMENT REQUESTED

**PLAINTIFF'S BRIEF IN SUPPORT OF MOTION FOR RETURN OF PROPERTY UNDER
FEDERAL RULE OF CRIMINAL PROCEDURE 41(g)**

TABLE OF CONTENTS

Preliminary Statement 1

Jurisdiction and Venue 3

Rule 41(g) of the Federal Rules of Criminal Procedure 3

Parties 4

Statement of Facts 5

Argument 9

 I. The Fourth Amendment Requires a Warrant Supported by Probable Cause to Search, Seize,
 or Copy Digital Data Storage Devices, or Share Copies of the Contents with Third Parties 9

 II. The Length of Time Property is Detained Raises a Separate Fourth Amendment Inquiry . 14

 III. Any Retention of Data, or Sharing of Data with Third Parties, Without a Warrant
 Supported by Probable Cause, Violates the Fourth Amendment 14

Conclusion 15

TABLE OF AUTHORITIES

Alasaad v. Nielsen
2018 U.S. Dist. LEXIS 78783 (D. Mass. May 9, 2018)..... 2, 10-11

Carpenter v. United States
585 U.S. ___, 2018 U.S. LEXIS 3844 (2018) 2, 10, 12-13

Doe v. United States
896 F. Supp. 2d 1184 (S.D. Fla. 2012) 4

House v. Napolitano
2012 U.S. Dist. LEXIS 42297 (D. Mass. Mar. 28, 2012) 14

Janfeshan v. United States Customs & Border Prot.
2017 U.S. Dist. LEXIS 151058 (S.D.N.Y. 2017) 12

Ordonez v. United States
680 F.3d 1135 (9th Cir. 2012) 3-4

Riley v. California
134 S. Ct. 2473 (2014) 10-12

Tellez-Sanchez v. United States
2014 U.S. Dist. LEXIS 92418 (D. Ariz. 2014) 4

Terry v. Ohio
392 U.S. 1 (1968) 13-14

United States v. Bennett
423 F.3d 271 (3d Cir. 2005) 4

United States v. Cortez
449 U.S. 411 (1981) 13

United States v. Djibo
151 F. Supp. 3d 297 (E.D.N.Y. 2015) 11-12

United States v. Kim
103 F. Supp. 3d 32 (D.D.C. 2015) 2, 12-13

United States v. Kalsuz
890 F.3d 133 (4th Cir. 2018) 12

United States v. Place
462 U.S. 696 (1983) 14

United States v. Ramsey
431 U.S. 606 (1977) 10

Statutes and Regulations

CBP Directive No. 3340-049A (Jan. 4, 2018) 1, 8-9

Fed. R. Crim. P. 41(g) *passim*

Law Review Articles

Thomas Mann Miller, *Digital Border Searches After* *Alley* v. California,
90 Wash. L. Rev. 1943, 1947 (2015) 11

PRELIMINARY STATEMENT

1. This is a motion pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure seeking the return of any personal data that Defendant U.S. Customs and Border Protection (“CBP”), its agents and employees copied from Plaintiff Rejhane Lazoja’s phone, which was taken from her unlawfully at the border and which contains privileged communications between Ms. Lazoja and her counsel. The seizure, retention, and any sharing of her property without reasonable suspicion, probable cause, or a warrant have violated Ms. Lazoja’s rights under the Fourth Amendment of the U.S. Constitution, and are at odds with recent Supreme Court holdings as well as District Court and Court of Appeals decisions scrutinizing CBP’s practices of seizing digital storage devices without a warrant.

2. When Ms. Lazoja landed at Newark Liberty International Airport (“Newark”), she was already exhausted from the nine-hour transatlantic flight. Instead of welcoming her back to the United States, her home country, Defendants’ agents and employees questioned Ms. Lazoja, searched her, took her to a small, windowless room, and even seized her cell phone. Ms. Lazoja is a Muslim woman and wears *hijab* (a headscarf) in accordance with her religious beliefs. Pursuant to her sincerely held beliefs, Ms. Lazoja cannot be seen in a state of undress by men who are not family members. The personal data on Ms. Lazoja’s phone included pictures of her in a state of undress, as well as privileged communications with her counsel.

3. U.S. Customs and Border Protection (“CBP”) follows a policy Directive that states “copies of information contained in electronic devices (or portions thereof) . . . are retained in accordance with this Directive” and are shared “with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.” CBP Directive No. 3340-049A, § 5.5.1.3. (Jan. 4, 2018), Ex. 3.

4. Today, over 150 days later, on information and belief, Defendants and their agents and employees still possess the personal data from Ms. Lazoja's cell phone. While Defendants returned Ms. Lazoja's cell phone 130 days after it was seized, they refuse to state what they did with her personal data, what third parties her personal data was shared with, and if let alone when they will return her data. At no time, not when Defendants' agents and employees seized Ms. Lazoja's cell phone, nor at any point in the over 150 days since, have Defendants articulated a reasonable suspicion for seizing the phone, let alone probable cause, let alone produced a warrant to search or seize Plaintiff's phone and personal data.

5. Seizing and searching a cell phone is unlike seizing or searching any other property. Cell phones are a uniquely intimate and expansive repository of our lives. They do far more than just make calls and send e-mails; they monitor and log much of our movement, activity, and even our thinking in real time. They enable us to stay connected with coworkers and loved ones—losing a phone essentially cuts one off from modern society. In June, the Supreme Court recognized the indispensability of cell phones and the heightened privacy interests at stake when they are utilized in warrantless investigations. *See Carpenter v. United States*, 585 U.S. ___, 2018 U.S. LEXIS 3844 at *23 (2018) (“While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time.”). Numerous District Courts, even prior to *Carpenter*, have scrutinized CBP's policy of seizing and searching cell phones without a warrant. *See, e.g., Alasaad v. Nielsen*, 2018 U.S. Dist. LEXIS 78783 *3 (D. Mass. May 9, 2018) (denying a government motion to dismiss on a Fourth Amendment challenge to warrantless digital device searches and seizures at the border); *United States v. King*, 2015 F. Supp. 3d 32, 54-58 (D.D.C. 2015) (finding that off-border search and copying of a laptop computer without a warrant was unreasonable).

6. Defendants and their agents and employees violated Ms. Lazoja's Constitutional rights in three discrete ways: first, by initially searching and seizing Ms. Lazoja's property without a warrant or reasonable suspicion; second, by failing to return Ms. Lazoja's property for over 120 days with no warrant or reasonable suspicion; and third, by continuing to retain any information copied from Ms. Lazoja's phone ("Data") without a warrant or reasonable suspicion long-after her passage through the border. Any ongoing retention by Defendants of Ms. Lazoja's Data is manifestly unreasonable and a continuing violation of Ms. Lazoja's Fourth Amendment rights. Therefore, Ms. Lazoja asks this Court to order Defendants to return her Data, order an expungement of any copies made of the Data, and disclose all third parties who received and/or retain copies, partial or complete, of the Data, as well as any information about the basis for the seizure and retention of her property.

JURISDICTION AND VENUE

7. Jurisdiction is conferred on this court by 28 U.S.C. §§ 1331, 1356, and Rule 41(g) of the Federal Rules of Criminal Procedure.

8. 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.

9. Venue properly lies within the District of New Jersey because Ms. Lazoja's property was seized at Newark, which is in this district. 28 U.S.C. § 1391(b)(2); Fed. R. Crim. P. 41(g).

RULE 41(g) OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

10. Rule 41(g) of the Federal Rules of Criminal Procedure empowers those "aggrieved by an unlawful search and seizure of property or by the deprivation of property" to "move for the

property's return . . . in the district where the property is seized.” *See Ordonez v. United States* 680 F.3d 1135, 1137 (9th Cir. 2012) (“[Rule 41(g)] provides a mechanism by which a person may seek to recover property seized by federal agents.”). Where the government terminates, or declines to initiate criminal proceedings, Rule 41(g) allows the wronged party to bring a civil claim under the court's equitable jurisdiction. *United States v. Bennett*, 421 F.3d 271, 274 (3d Cir. 2005) (“In a typical case under Rule 41(g), a district court exercises its equitable powers.”); *see also United States v. Bennett*, 414 F.3d 408, 411 (3d Cir. 2000) (“A district court has jurisdiction to entertain a motion for return of property even after the termination of criminal proceedings against the defendant and such an action is treated as a civil proceeding for equitable relief.”); *Doe v. United States*, 396 F. Supp. 2d 1184, 1187-88 (S.D. Fla. 2012) (exercising jurisdiction over a Rule 41(g) motion for return of property, where the property included data copied from digital devices detained at the border, after the physical property had been returned, and where the data contained attorney-client privileged materials).

11. After a Rule 41(g) movant demonstrates a possessory interest in the property, and in the absence of criminal proceedings, “the government bears the burden of establishing the movant is not entitled to relief.” *Tellez-Sanchez v. United States*, 2015 U.S. Dist. LEXIS 92418 at *3 (D. Ariz. 2014) (citing *United States v. Chambers*, 105 F.3d 374, 376 (3d Cir. 1999)).

PARTIES

12. Plaintiff Rejhane Lazoja is a national of the United States and holder of a valid United States Passport.

13. Defendant Kirstjen Nielsen is the Secretary of the Department of Homeland Security (“DHS”). She supervises Defendants McAleeman and Adele Fasano and is sued in her official capacity.

14. Defendant Kevin K. McAleeman is the Commissioner of CBP, which is an agency within DHS. He supervises Defendant Adele Fasano, and is sued in his official capacity.

15. Defendant Adele Fasano is the CBP Port Director for Newark, and is sued in her official capacity.

16. Defendants Jane Doe and John Does 1-2 are CBP Officers in Newark, and are sued in their official capacities.

STATEMENT OF FACTS

17. On the evening of February 26, 2018, Plaintiff Rejhane Lazoja arrived at Newark on a flight from Zurich, Switzerland with her six-year-old daughter. See Affidavit of Rejhane Lazoja, dated August 22, 2018 (“Rejhane Aff.”), Ex. 1 ¶ 2.

18. While passing through CBP primary inspection at Newark, Ms. Lazoja used a self-service Automated Passport Control kiosk, which prompts travelers to scan their passports, take a photograph, and answer a series of questions verifying biographic and flight information. The Kiosk provided Ms. Lazoja a receipt with an ‘X’ printed on her photograph. (Rejhane Aff. ¶ 3).

19. Ms. Lazoja was directed by a CBP Officer to move to a separate line at the inspection point. (Rejhane Aff. ¶ 4).

20. Two CBP Officers asked Ms. Lazoja several questions including where she traveled. (Rejhane Aff. ¶ 5).

21. Ms. Lazoja answered the questions. (Rejhane Aff. ¶ 6).

22. A male CBP Officer directed Ms. Lazoja to wait in a main seating area for several minutes. (Rejhane Aff. ¶ 7).

23. A female CBP Officer (“Jane Doe”) called Ms. Lazoja to follow her to a small room with CBP Officer John Doe 1 (“John Doe 1”). (Rejhane Aff. ¶ 8).

24. Jane Doe and John Doe 1 further questioned Ms. Lazoja about her travels, and asked questions including whether she was ever a refugee. (Rejhane Aff. ¶ 9).

25. Ms. Lazoja is a Muslim woman and wears a *hijab* in accordance with her religious beliefs. (Rejhane Aff. ¶ 10).

26. Ms. Lazoja's Apple iPhone 6S Plus ("iPhone") contained photos of her in a state of undress without her *hijab* (Rejhane Aff. ¶ 11).

27. Ms. Lazoja's iPhone contained legal communications with the Council on American-Islamic Relations, New York. (Rejhane Aff. ¶ 12).

28. Ms. Lazoja asked if she needed an attorney and whether the questions were a result of her wearing a *hijab* (Rejhane Aff. ¶ 13).

29. Jane Doe and John Doe 1 replied that there was no need to contact a lawyer. (Rejhane Aff. ¶ 14).

30. Jane Doe and John Doe 1 asked Ms. Lazoja if she carried any electronic devices on her person. (Rejhane Aff. ¶ 15).

31. Ms. Lazoja assented and produced the iPhone with accompanying subscriber identity module ("SIM Card"). (Rejhane Aff. ¶ 16).

32. Jane Doe and John Doe 1 confiscated Ms. Lazoja's iPhone and SIM Card. (Rejhane Aff. ¶ 17).

33. Like many cell phones, the contents of Ms. Lazoja's iPhone can only be accessed by inputting an alphanumeric password. Without said password, such cell phones are commonly described as being "locked," and when said password is successfully entered, they are commonly described as being "unlocked."

34. John Doe 1 asked Ms. Lazoja to unlock the iPhone, but did not state a reason for her to unlock the iPhone (Rejhane Aff. ¶ 18).

35. Since there was no stated reason for her to unlock the iPhone, Ms. Lazoja refused. (Rejhane Aff. ¶ 19).

36. Jane Doe led Ms. Lazoja out of the small room. (Rejhane Aff. ¶ 20).

37. A male CBP Officer John Doe 2 (“John Doe 2”) asked Ms. Lazoja to unlock the iPhone. (Rejhane Aff. ¶ 21).

38. Ms. Lazoja refused to unlock the iPhone. (Rejhane Aff. ¶ 22).

39. Jane Doe repeated her request that Ms. Lazoja unlock the iPhone, saying that she understood the sensitivity of sharing personal pictures, including any showing Ms. Lazoja undressed, without her *hijab* (Rejhane Aff. ¶ 23).

40. Ms. Lazoja refused to unlock the iPhone. (Rejhane Aff. ¶ 24).

41. After accompanying Ms. Lazoja to the baggage claim area, Jane Doe opened and searched Ms. Lazoja’s luggage, asking if she had more than \$10,000 or more in her possession. (Rejhane Aff. ¶ 25).

42. Jane Doe and John Does 1-2 did not return the iPhone. (Rejhane Aff. ¶ 26).

43. Jane Doe and John Does 1-2 provided Ms. Lazoja a receipt (No. 1199376) dated February 26, 2018, documenting CBP’s seizure of her iPhone and SIM Card, and indicating the iPhone and SIM Card were “Sent to DHS Lab.” (Rejhane Aff. ¶ 27); ~~see~~ Ex. A.

44. On July 6, 2018, Ms. Lazoja’s iPhone and SIM Card were returned to her counsel, Jay Rehman by Michael Firing, Assistant Port Director for CBP at Newark. ~~See~~ Declaration by Jay Rehman, Esq., dated August 23, 2018 (“Rehman Decl.”), ¶ 3.

45. Ms. Lazoja did not receive her iPhone and SIM Card back until more than 120 days after they were taken.

46. On July 9, 2018, Ms. Lazoja, through counsel and via e-mail to Michael Firing, confirmed receipt of the phone, and notified CBP that the phone contained pictures of her without her *hijab*s as well as privileged communications with her counsel. Ms. Lazoja requested that CBP: confirm whether CBP made any copies of the Data, and to provide its legal basis for doing so; expunge any copies of the Data; and confirm whether it has shared copies of the Data with any third parties, including but not limited to, local, state, or federal law enforcement agencies. (Rehman Decl. ¶ 4); ~~see~~ Ex. 2.

47. Ms. Lazoja has received no response to her July 9 request. (Rehman Decl. ¶ 5).

48. CBP's policy Directive provides that "[u]nless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days." CBP Directive No. 3340-049A, § 5.4.1 (Jan. 4, 2018), *available at* <https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf>, Ex. 3.

49. Ms. Lazoja has not received any copies made of the Data, or any assurances that Defendants, their agents or employees no longer possess copies of her Data. (Rehman Decl. ¶ 8).

50. Ms. Lazoja has not received any explanation for the seizure of the phone or for the length of time she was deprived of her property, including whether any "extenuating circumstances" existed. (Rehman Decl. ¶ 7).

51. On information and belief, CBP did not obtain a warrant to search, seize, or access Ms. Lazoja's property. (Rehman Decl. ¶ 7).

52. Defendants and their agents have a stated policy, custom, and practice of copying digital information from devices detained at the border, and sharing that information with third parties, including law enforcement agencies:

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

Ex. 3 at § 5.5.1.3.

53. Pursuant to CBP's own policies, if Defendants, their agents and employees do not assert probable cause to seize a device or the information it contains, "any copies of the information held by CBP must be destroyed." Ex. 3 at § 5.4.1.2. "Upon this determination, the copy of the information will be destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system and which must be no later than twenty-one (21) days after such determination." *Id.*

54. Ms. Lazoja has not received any assurances that Defendants, their agents or employees have not shared her Data, including privileged communications, with third parties. (Rehman Decl. ¶ 8).

ARGUMENT

I. The Fourth Amendment Requires a Warrant Supported by Probable Cause to Search, Seize, or Copy Digital Data Storage Devices, or Share Copies of Contents with Third Parties

55. The Fourth Amendment establishes that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S.

Const. amend. IV. The Supreme Court recently reiterated that “the ultimate touchstone of the Fourth Amendment is reasonableness” and that “reasonableness generally requires the obtaining of a judicial warrant.” *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006); *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)). Although border searches have been recognized as one exception to the warrant requirement, *United States v. Ramsey*, 431 U.S. 606, 620 (1977), “the exception is not limitless.” *Alasaad v. Nielser*, 2018 U.S. Dist. LEXIS 78783 *43 (D. Mass. May 9, 2018). “Border searches must still be ‘reasonable,’ and the Court must still—as with searches conducted in the interior—balance ‘the sovereign’s interests’ with the privacy interests of the individual.” *Id.* (citing *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985)). Searches and seizures of digital devices present new questions in the border search analysis. *Id.* at *53.

56. The Supreme Court has repeatedly held, including recently in *Carpenter*, that warrantless invasions of cell phones face heightened Fourth Amendment scrutiny. Cell phones “are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.” *Riley*, 134 S. Ct. at 2484; see also *Carpenter v. United States*, 585 U.S. ___, 2018 U.S. LEXIS 3844 *14-15 (2018) (noting the Court has kept “attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools” such as with “the vast store of sensitive information on a cell phone”). In *Riley* a near-unanimous court held that individual’s privacy interests outweighed any legitimate government interests in warrantless cell phone searches incident-to-arrest, since “cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.” 134 S. Ct. at 2488-89. “Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept

on an arrestee’s person.” *Id.* at 2489. The Court described how individuals cannot “lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read,” and that the “sum of an individual’s private life can be reconstructed through a thousand photographs.” *Id.* A person’s browsing history and location information “can form a revealing montage of the user’s life.” *Id.* at 2490. Importantly, “*Riley* opens up a doctrinal path for courts to reconsider whether to extend the border search exception to the warrant requirement . . . to searches of digital information.” Thomas Mann Miller, *Digital Border Searches After Riley v. California*, 90 Wash. L. Rev. 1943, 1947 (2015). Such heightened scrutiny of phone searches is even more urgent after *Carpenter*

57. In light of *Riley* some courts have already limited the scope of searches of digital devices pursuant to the border search exception. Recently, the U.S. District Court for the District of Massachusetts applied *Riley* to the border search context as part of ongoing litigation under the First and Fourth Amendments brought by individuals whose devices were searched and seized at the border. In that case, the court explained that “exceptions to the warrant requirement do not exist in isolation; rather, they are all part of Fourth Amendment jurisprudence.” *Alasaad* 2018 U.S. Dist. LEXIS 78783 at *53. The court similarly scrutinized the applicability of the border search exemption in the digital context, that “[a]lthough a warrant [requirement] might ‘have an impact on the ability of law enforcement to combat crime,’ *Riley* 134 S. Ct. at 2493], it is unclear . . . the extent to which such impediment justifies applying the border search exception to electronic devices.” *Alasaad* at *62. On those grounds, the court in *Alasaad* found that the plaintiffs plausibly alleged a Fourth Amendment claim against both the search and the seizure of their devices.

58. Several other Federal courts have applied the reasoning of *Riley* to narrow the border search exception in the context of searches of digital devices such as cell phones. *See, e.g.*

United States v. Djilali, 2015 F. Supp. 3d 297, 310 (E.D.N.Y. 2015) (granting motion to suppress documents obtained from warrantless search of the phone of an outbound passenger under *Riley*); *Janfeshan v. United States Customs & Border Prot.*, 2017 U.S. Dist. LEXIS 151058 (S.D.N.Y. 2017) (denying motion to dismiss a Fourth Amendment claim regarding a forensic cell phone search at the border); *United States v. Kolb*, 2018 F.3d 133, 146-47 (4th Cir. 2018) (“After *Riley* we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion.”); *United States v. Kim*, 2015 F. Supp. 3d 32, 54-58 (D.D.C. 2015) (“[T]he fact that the Supreme Court has specifically likened the border search warrant exception to the search incident to arrest exception reinforces the Court's view that an analysis similar to the one in *Riley* should be undertaken here.”). Note that these cases predate the June 2018 decision in *Carpenter*, where the Supreme Court further emphasized the heightened privacy interests implicated by cell phones, specifically through providing law enforcement access to cell phone location data.

59. In *Kim*, where DHS agents seized a laptop computer at Los Angeles International Airport and later sent it to a laboratory to be copied and searched, the district court found that the lengthy post-seizure retention of a laptop at a second site, outside the airport, “did not possess the characteristics of a border search or other regular inspection procedures,” and that it “more resembled the common nonborder search based on individualized suspicion, which must be prefaced by the usual warrant and probable cause standards.” *Id.* at 58 (citing *United States v. Brenna*, 1976 F.2d 711, 716 (5th Cir. 1976)). The court in *Kim* questioned whether the seizure and imaging of a laptop at the border “can accurately be characterized as a border search at all.” *Id.* at 57.

60. While noting that the characteristics of the seizure and search of the digital device triggered a warrant requirement, the court found that in the absence of a warrant, there was neither probable cause, nor even reasonable suspicion of ongoing or imminent criminal activity for the search:

Considering all of the facts and authorities set forth above, then, the Court finds, under the totality of the unique circumstances of this case, that the imaging and search of the entire contents of Kim's laptop, aided by specialized forensic software, for a period of unlimited duration and an examination of unlimited scope, for the purpose of gathering evidence in a pre-existing investigation, was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of Kim's privacy and so disconnected from not only the considerations underlying the breadth of the government's authority to search at the border, but also the border itself, that it was unreasonable.

Id. at 59. Importantly, in *Kim* the plaintiff was under investigation for alleged *past* criminal activity, but that did not even give rise to reasonable suspicion or justify in any way the high intrusiveness of the search and seizure.

61. The Supreme Court recently expanded the categorically heightened privacy interests in data located on cell phones, specifically addressing cell phones *location data*. *Location data* consists of the historic or contemporaneous geographic location of a cell phone. Cell phones store or provide location data in numerous ways, and when obtained, it enables the government to achieve “near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” *Carpenter*, 2018 U.S. LEXIS 3844 at *23. Cell phone owners’ privacy interest in location data is *so strong* that transmission to a third party did not vitiate Fourth Amendment protections, as is typically mandated by the third-party doctrine. *Id.* at *20.

62. Therefore, without individualized criminal suspicion, the off-site search of an electronic device taken at a border is unconstitutional. *See United States v. Carter*, 419 U.S. 411, 417-18 (1981) (holding that reasonable suspicion requires “a particularized and objective basis for suspecting the particular person stopped of criminal activity”); *see also Terry v. Ohio*, 392 U.S. 1

(1968) (holding that reasonable suspicion requires “specific and articulable facts” that criminal activity “may be afoot”). No such suspicion of ongoing or imminent criminal activity existed in the case of Ms. Lazoja giving rise to reasonable suspicion to search and seize her property. Consequently, neither was there probable cause, nor a warrant. Therefore, the search and seizure of Ms. Lazoja’s property violated her rights under the Fourth Amendment.

II. The Length of Time Property is Detained Raises a Separate Fourth Amendment Claim

63. Even if CBP could constitutionally seize Ms. Lazoja’s property, which it could not, CBP’s impermissibly-delayed return of said property, and failure to return her Data, constitutes an independent violation of the Fourth Amendment. Prolonged detentions of property must be reasonable for their duration. *United States v. Place*, 462 U.S. 696, 708-10 (1983) (holding that the “length of the detention”—ninety minutes—of an individual’s luggage gave rise to a seizure requiring probable cause). Specifically, even if CBP’s warrantless, suspicionless seizure and search of an electronic device is initially justifiable pursuant to CBP’s narrowly-defined border search authority, the length of time a device is held can give rise to a Fourth Amendment claim. *See House v. Napolitano*, 2012 U.S. Dist. LEXIS 42297 at *31 (D. Mass. Mar. 28, 2012) (holding that a forty-nine-day warrantless border detention of a locked laptop computer, computer storage medium, and digital camera raised a plausible Fourth Amendment claim even where the claim regarding the search itself is dismissed).

III. Any Retention of Data, or Sharing of Data with Third Parties, Without a Warrant Supported by Probable Cause, Violates the Fourth Amendment

64. Here, CBP retained Ms. Lazoja’s cell phone—an indispensable companion in modern society—without a warrant for more than 120 days. CBP has not returned any copies it has made of Ms. Lazoja’s Data, which contains personal photos of her in an exposed state without her *hijab* as well as attorney-client communications. Neither has CBP affirmed that it has

destroyed any copies made of Ms. Lazoja's Data, and not transmitted the Data to any third parties. There is no possible justification for this. Similarly, there is no justification for any warrantless duplication or transmission of Ms. Lazoja's Data. Such duplication or transmission of the Data would require a warrant supported by probable cause.

CONCLUSION

65. Plaintiff Rejhane Lazoja respectfully asks this Court to order Defendants to return her Data, to expunge any copies made of the Data, to disclose all third parties who received and/or retain copies, partial or complete, of the Data, and to provide information about the basis for the seizure and retention of the property. Further, Ms. Lazoja respectfully asks that this Court declare that Defendants, their agents and employees violated the Fourth Amendment of the U.S. Constitution through their policy of searching, seizing, detaining, copying, and sharing with third parties digital storage devices without a warrant. Finally, Ms. Lazoja respectfully asks that this Court enjoin Defendants from its practice of searching and seizing electronic storage devices without a warrant supported by probable cause.

DATED: August 23, 2018
[Newark, New Jersey]

Respectfully submitted,

COUNCIL ON AMERICAN-ISLAMIC
RELATIONS NEW JERSEY

By: s/ Jay Rehman
Jay Rehman
4475 S. Clinton Ave., Suite 202
South Plainfield, New Jersey 07080
jRehman@cair.com
(908) 668-5900

COUNCIL ON AMERICAN-ISLAMIC
RELATIONS NEW YORK

Albert Fox Cahn
(pro hac vice pending)
aCahn@cair.com
Carey Shenkman
(pro hac vice pending)
legal@ny.cair.com
46-01 Twentieth Avenue
Queens, New York 11105
(646) 665-7599

Attorneys for Plaintiff