IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

GEORGE ANIBOWEI,

Plaintiff,

v.

KIRSTJEN M. NIELSEN, U.S. Secretary of Homeland Security, in her official capacity; KEVIN K. MCALEENAN, Commissioner of U.S. Customs and Border Protection, in his official capacity; RONALD D. VITIELLO, Acting Director of U.S. Immigration and Customs Enforcement, in his official capacity; DAVID P. PEKOSKE, Administrator of the Transportation Security Administration, in his official capacity; WILLIAM P. BARR, Attorney General of the United States, in his official capacity; U.S. DEPARTMENT OF HOMELAND SECURITY; U.S. CUSTOMS AND BORDER PROTECTION; U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT; TRANSPORTATION SECURITY ADMINISTRATION,

Defendants.

Case No. 3:16-cv-03495-D

VERIFIED SECOND AMENDED COMPLAINT
FOR VACATUR OF UNLAWFUL AGENCY POLICIES
AND DECLARATORY AND INJUNCTIVE RELIEF

1. In *Riley v. California*, 573 U.S. 373 (2014), the Supreme Court unanimously held that law enforcement must not search digital information on a cell phone without first obtaining a warrant, except in narrow exigent circumstances. The Justices based this holding on the unique character of cell phones. *Id*. at 375. Nearly every person carries one, and nearly every cell phone has a "digital record of nearly every aspect" of a person's life stored on it. The Supreme Court thus held that warrants are required to search them, even in circumstances when government agents have long been allowed to search a person's other effects for some other function (such as a search incident to arrest) without a warrant or even suspicion.

2. This case is *Riley* at the border. *Riley* says that only a warrant supported by probable cause can justify the search of a cell phone except in exigent circumstances. But policies promulgated by U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE), invoking the "border search exception," permit border agents to search cell phones without warrants, probable cause, or reasonable suspicion for no other reason than that an individual is seeking to cross an international border. Those same policies allow border agents to download (*i.e.*, seize) and store the information on a seized cell phone forever without a warrant or probable cause. Again, all for no other reason but that an individual has crossed an international border.

3. In other words, according to CBP and ICE regulations, the government may require a person to turn over a "digital record of nearly every aspect" of that person's life to government agents, and the government may store it forever, for no other reason than because that person took a flight from Toronto to Dallas. The government could not search a person's house just because that person crossed the border. But "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 376.

4. CBP and ICE follow their policies. They perform tens of thousands of cell phone searches each year under their policies. CBP agents, relying on CBP and ICE directives and authority, have searched plaintiff George Anibowei's cell phone on at least five occasions. On one of those occasions, they downloaded all of the data off the phone and kept it. To the best of Mr. Anibowei's knowledge, they keep it to this day.

5. The need to apply *Riley*'s warrant requirement at the border only grows. Lawyers use electronic devices to store interview notes and briefs for their clients. Journalists do the same with their records of conversations with whistleblowers and confidential sources. And everyday

people use these devices to catalog their most sensitive and personal thoughts, conversations, and life events in extensive detail—from data about their health, to condolences on the loss of a loved one, to political rants emailed to friends, to gossip about other parents in the PTA, to intimate messages from a romantic partner.[1]

6. A person does not give up the right to privacy and invite scrutiny of "nearly every aspect" of their lives simply by crossing the U.S. border. The average person reasonably believes that the communications and photographs sent, received, and stored on a phone are protected from arbitrary and suspicionless searches by the government—not just some of the time, not just in the Nation's interior, but all of the time. But every time a person enters or exits the United States with a phone or laptop, that person's devices come within the scope of CBP and ICE policies that give agents unilateral authority to search every piece of stored information—without a warrant, probable cause, or even a reasonable suspicion of any wrongdoing.

7. CBP and ICE's arbitrary and suspicionless search policies violate the time-honored presumption of privacy in sensitive communications, intimate relationships, and confidential information. And they violate the First and Fourth Amendments to the Constitution.

[1] A recent survey suggests that half of all adults had not just received a sext or explicit photo, but had actually *stored* sexts and explicit images that they receive. *Sext Much? If So, You're Not Alone*, Sci. Am., https://www.scientificamerican.com/article/sext-much-if-so-youre-not-alone; *see also* Emily C. Stasko & Pamela A. Geller, *Reframing Sexting as a Positive Relationship Behavior*, Am. Psych. Ass'n (Aug. 2015), https://www.apa.org/news/press/releases/2015/08/reframing-sexting.pdf.

INTRODUCTION

8. By early 2018, 95% of Americans owned a cell phone, and 77% of Americans owned a smartphone.[2] Approximately two-thirds of all people alive in the world today, counting every age group and country, also own a cell phone.[3]

9. As the Supreme Court recognized in 2014, cell phones, and in particular today's smartphones, "place vast quantities of personal information literally in the hands of individuals." *Riley v. California*, 573 U.S. 373, 386 (2014). The nature of cell phones makes the search of a cell phone by law enforcement extraordinarily invasive and potentially humiliating. Thus, "[a]llowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case." *Id.* at 395.

10. For this reason, when the Supreme Court has been called to weigh in on law enforcement searches and seizures of cell phones, it has uniformly held that the collection of data from cell phones requires the safeguard of a particularized warrant supported by probable cause. *See Riley*, 573 U.S. 373; *Carpenter v. United States*, 138 S. Ct. 2206, 2209 (2018) .

11. Nonetheless, some relics of policy persist from the era before the Supreme Court decided its first cell-phone-search cases.

12. In August 2009, U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) issued a pair of directives that permitted officials of the two agencies to search "electronic devices"—defined as devices that "contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices"—"[i]n the

---

[2] *Mobile Fact Sheet*, Pew Research Center: Internet & Technology (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

[3] Paul Sawers, *5 Billion People Now Have a Mobile Phone Connection, According to GSMA Data*, Venture Beat (June 13, 2017), https://venturebeat.com/2017/06/13/5-billion-people-now-have-a-mobile-phone-connection-according-to-gsma-data/.

course of a border search, with or without individualized suspicion."[4] The directives specifically authorize CBP and ICE officials to conduct warrantless and suspicionless searches, including of privileged and sensitive information like "[l]egal materials," "medical records," and "work-related information carried by journalists."[5]

13. CBP updated its policy in 2018 to add nominal safeguards, none of which cures the structural constitutional defects of the 2009 policy. CBP's 2018 directive continues to authorize searches of electronic devices with zero individualized suspicion and without any protections for privileged and sensitive information.

14. CBP and ICE's extraordinarily broad policies expose one million travelers a day to the threat of having their most sensitive information searched and seized without any sort of individualized suspicion.

15. Among the untold number of people whose sensitive personal information has been swept up in this policy is plaintiff George Anibowei. Mr. Anibowei is a naturalized U.S. citizen born in Nigeria, and is the sole proprietor of his own law firm in Texas. Several times a year, he travels for work and personal reasons, including to see friends and relatives in Nigeria and other countries. Mr. Anibowei passed numerous and extensive security checks in the course of his journey from Nigerian immigrant to naturalized U.S. citizen. He also passed the additional

---

[4] U.S. Customs and Border Protection, Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-49 (Aug. 20, 2009), https://www.eff.org/document/customs-and-border-protection-directive-no-3340-049-border-search-electronic-devices; see also U.S. Immigration and Customs Enforcement, Border Searches of Electronic Devices, ICE Directive 7-6.1 (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf (containing nearly identical language).

[5] CBP Directive No. 3340-049 (Aug. 20, 2009).

security checks required for participation in CBP's Global Entry Trusted Traveler Program, and was issued membership in the program on November 1, 2012.

16. Nonetheless, for reasons unknown to Mr. Anibowei and that the government will not share, on October 10, 2016, CBP officers at the Dallas-Fort Worth Airport seized Mr. Anibowei's cell phone, saying that they were going to "copy the hard drive." The officers did not ask Mr. Anibowei for his consent or present him with a search warrant.

17. Mr. Anibowei has had his cell phone searched a total of at least five times by CBP agents, beginning with this first search and seizure in 2016. In four of these instances, Mr. Anibowei saw the agent search his text messages and other communications. Each of these searches was authorized by the 2009 ICE and CBP policies. Each of these searches would similarly be authorized by the 2018 CBP policy.

18. As an attorney, Mr. Anibowei regularly uses his smartphone to engage in sensitive and confidential communications with his immigration clients. During these searches, it is virtually certain that CBP viewed and copied privileged communications between Mr. Anibowei and his clients. CBP's searches and seizures of Mr. Anibowei's privileged client communications, as well as other sensitive and private information on his phone, violate both his and his clients' expectations of privacy in their privileged communications.

19. CBP's repeated searches and seizures of Mr. Anibowei's cell phone also have the potential to harm Mr. Anibowei's business. Given that some of Mr. Anibowei's clients are adverse to the U.S. Department of Homeland Security (DHS) in immigration proceedings, Mr. Anibowei's inability to safeguard their information from an agency of DHS threatens to damage the trust and confidence of his clients.

20. These warrantless and suspicionless searches of Mr. Anibowei's cell phone are "unreasonable searches and seizures" prohibited by the Fourth Amendment. The CBP and ICE policies authorizing warrantless and suspicionless searches of electronic devices facially violate the Fourth Amendment.

21. Moreover, these warrantless and suspicionless searches violate the First Amendment rights of individuals entering and exiting the United States. The CBP and ICE policies expose individuals' sensitive, expressive, and associational information to arbitrary search by government agents. The ever-present possibility of warrantless and suspicionless search chills protected expression. This specter encourages individuals to leave their devices at home so that they cannot communicate at all, or to censor their speech if they do carry them.

22. Every day that government agents keep Mr. Anibowei's data, the government holds in its possession the fruits of an unconstitutional search and seizure. The injury to Mr. Anibowei's constitutional rights wrought by the continued retention of this data continues to this day.

23. Mr. Anibowei seeks a declaration that CBP's searches of his cell phone were unlawful, and an injunction requiring that the government destroy his data. He also seeks vacatur of CBP and ICE's unlawful policies.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over Plaintiff's federal claims pursuant to 28 U.S.C. § 1331 because he challenges federal law and final agency action under the laws and Constitution of the United States.

25. 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.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

27. Plaintiff George Anibowei is a U.S. citizen licensed to practice law in the State of Texas since 2002. He resides at 934 Colorado Drive in Allen, TX.

28. Defendant Kirstjen M. Nielsen is the Secretary of the U.S. Department of Homeland Security. She oversees DHS and its sub-agencies. She is sued in her official capacity.

29. Defendant Kevin K. McAleenan is the Commissioner of U.S. Customs and Border Protection. He oversees CBP. He is sued in his official capacity.

30. Defendant Ronald D. Vitiello is the Acting Director of U.S. Immigration and Customs Enforcement. He administers ICE. He is sued in his official capacity.

31. Defendant David P. Pekoske is Administrator of the Transportation Security Administration (TSA). He administers TSA. He is sued in his official capacity.

32. Defendant William P. Barr is Attorney General of the United States. He oversees the Department of Justice and its sub-agencies. He is sued in his official capacity.

33. Defendant U.S. Department of Homeland Security (DHS) is a Department of the Executive Branch of the United States and is an "agency" within the meaning of 5 U.S.C. § 552(f)(1).

34. Defendant U.S. Customs and Border Protection (CBP) is a sub-agency of DHS. It is responsible for administering security checks at airports and other ports of entry.

35. Defendant U.S. Immigration and Customs Enforcement (ICE) is a sub-agency of DHS. It plays a supporting role in administering security checks at airports and other ports of entry.

36. Defendant Transportation Security Authority (TSA) is a sub-agency of DHS, housed within CBP. It has particular responsibility for administering security checks at airports.

BACKGROUND

A. Searches and Seizures of Electronic Data

37. Ninety-five percent of Americans and approximately two-thirds of all people in the world own a cell phone. These numbers are only projected to grow. By 2020, an estimated 80% of all adults in the world will own not just a cell phone but a smartphone, with all the enhanced storage capability this implies.

38. These devices are capable of containing extraordinary amounts of information, far beyond any other object a traveler could possibly carry. Today's iPhones, for instance, are capable of storing up to 256 gigabytes of data[6]—enough to hold hundreds of thousands of emails, documents, or images. A typical laptop computer can store double that.[7]

39. These devices not only store massive amounts of information, but also the most sensitive and personal information in a user's life. Electronic devices may store virtually all of an individual's communications—texts, voice mails, emails, and social-media posts—as well as detailed information on his location; his financial, legal, and medical history; his contacts; and his browsing and social-media history. Applications on the market today allow cell phone, tablet, and laptop users to store and analyze detailed information about such deeply personal topics as disease and pregnancy status, weight loss and physical fitness, income and credit history, and

---

[6] *About Storage on Your Device and in iCloud*, Apple.com, https://support.apple.com/en-us/HT206504 (last visited Mar. 12, 2019).

[7] *15-inch MacBook Pro*, Apple.com, https://www.apple.com/macbook-pro/specs/ (last visited Mar. 12, 2019).

relationship status. Other applications could be used to build a detailed record of a person's sexual orientation and sexual history, political beliefs, and religious affiliation.

40. The data on some electronic devices, in the aggregate, can be used to reconstruct virtually every aspect of a person's career, personal life, habits, beliefs, associations, and daily routines. Indeed, the explosive implications of these devices for personal privacy have become so alarming that they have spurred a national debate over technology, privacy, and the power of businesses—like Facebook and Google—that hold or can access personal data generated or stored on electronic devices.[8] The intensity of users' fears clearly demonstrates an emerging societal consensus that an expectation of privacy in these devices is "one that society is prepared to recognize as reasonable"—indeed, as essential. *See Smith v. Maryland*, 442 U.S. 735, 740 (1979).

41. As the Supreme Court has noted, "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house"—historically the piece of property that the Constitution has protected most. *See Riley*, 573 U.S. at 397. The Supreme Court has duly recognized that electronic devices are in a category apart for Fourth Amendment purposes given their extraordinary privacy implications.

42. Electronic devices not only hold our deepest secrets; they are practically extensions of our bodies, traveling with us everywhere we go. Many people would not be able to retain a job, receive help in an emergency, or maintain their personal relationships without the help

[8] *See, e.g.*, Steve Shillingford, *Facebook, Twitter, and Google Have Too Much Power—We Can't Just Legislate Ourselves Out of This Mess*, Fox News (Sept. 5, 2018), https://www.foxnews.com/opinion/facebook-twitter-and-google-have-too-much-power-we-cant-just-legislate-ourselves-out-of-this-mess; John Herrman, *Have the Tech Giants Grown Too Powerful? That's an Easy One*, N.Y. Times (July 11, 2018), https://www.nytimes.com/2018/07/11/magazine/facebook-google-uber-tech-giants-power.html.

of a cell phone, laptop, tablet, or in many cases all three. Many workers use their electronic devices daily to receive and respond to sensitive and pressing business communications. For most people, it is not an option to leave their electronic devices at home, including when they travel.

43. Every day, many of the 95% of Americans who own a cell phone enter and leave the United States, as do many thousands of foreign nationals. In 2017, CBP processed an average of over 1.1 million people per day coming into and leaving the United States by land, air, and sea.[9] Approximately half of these people are U.S. citizens.

44. Extrapolating from these figures, we can conservatively estimate that in a 24-hour period, approximately 885,000 cell phones enter or leave the United States at a port of entry. 522,500 of these cell phones belong to U.S. citizens.[10]

45. These travelers also carry thousands of other electronic devices across the border daily.

46. In great part due to the extraordinary capabilities of these devices, the Supreme Court affords far greater protection to cell phones and other electronic devices than to other objects subject to search, as explained in detail below. CBP and ICE nevertheless subject these most sensitive implements to extensive warrantless and suspicionless searches.

B. CBP and ICE Policies

47. On August 18, 2009, ICE issued an extraordinarily broad policy functionally permitting its border agents to conduct searches of all "electronic devices" in the possession of travelers into and out of the United States. *See* ICE Directive 7-6.1 (Aug. 18, 2009).

---

[9] *On a Typical Day in Fiscal Year 2018, CBP…*, U.S. Customs and Border Protection (March 7, 2019), https://www.cbp.gov/newsroom/stats/typical-day-fy2018.

[10] This estimate is conservative because people who travel internationally may be more likely than the general population to own a cell phone.

48. Two days later, on August 20, 2009, CBP issued a nearly identical directive. *See* CBP Directive No. 3340-049 (Aug. 20, 2009).

49. The majority of agents at ports of entry work for CBP, while ICE agents provide supplemental help in some cases.

50. The 2009 policies permitted CBP and ICE agents conducting border searches, "without individualized suspicion," to "examine electronic devices"; to "review and analyze the information" encountered during the course of the search; and to retain devices and data indefinitely. CBP Directive No. 3340-049, §§ 5.1.2, 5.3.1.

51. Under the agencies' 2009 policies, agents may confiscate devices from travelers for a "thorough" search, either on-site or off-site, without individualized suspicion. *See id.* § 5.3.1; ICE Directive 7-6.1, §§ 6.1, 8.1.4. While CBP confiscations presumptively last no more than five days, CBP supervisors may extend this period based on undefined "extenuating circumstances." CBP Directive No. 3340-049, §§ 5.3.1, 5.3.1.1. Confiscations by ICE can last up to 30 days without supervisor approval, and can be extended under "circumstances … that warrant more time." ICE Directive 7-6.1, § 8.3.1.

52. The 2009 policies instruct the agencies to delete data only "if, after reviewing information … there is not probable cause to seize it." CBP Directive No. 3340-049, § 5.3.1.2. As a result, agents may permanently detain an electronic device and its data without a warrant. And the probable cause necessary to permanently detain devices or information can be generated through the initial searches and seizures performed without any individualized suspicion.

53. On January 4, 2018, CBP issued a directive superseding its 2009 directive. *See* CBP Directive No. 3340-049A (Jan. 4, 2018) (the "2018 Policy").

54. While CBP's 2018 Policy supersedes its 2009 Policy, ICE has not issued a comparable new policy. Under ICE's 2009 Directive, ICE agents are currently authorized to search electronic devices and to review, analyze, and copy their contents without any individualized suspicion.

55. CBP's 2018 Policy covers "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players." § 3.2.

56. The 2018 Policy opens up this entire category to two types of searches—"basic" and "advanced"—neither of which must be supported by a particularized warrant or even by probable cause. §§ 5.1.3, 5.1.4.

57. A "basic search" is by no means "basic"; it is highly intrusive and allows officers to access all content and communications stored on the device. An agent conducting a basic search "may examine an electronic device and may review and analyze information encountered at the border." § 5.1.3. The 2018 Policy authorizes an agent to perform a "basic search" without any individualized suspicion. *Id.*

58. An "advanced search" allows for the connection of "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." § 5.1.4. The 2018 Policy authorizes an agent to perform an "advanced search" if he has either "reasonable suspicion of activity in violation of the laws enforced or administered by CBP" or where "there is a national security concern." § 5.1.4.

59. The 2018 Policy makes no effort to cabin its vague and capacious terms "reasonable suspicion" or "national security concern." The Policy explains that "[m]any factors may

create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national-security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list." § 5.1.4.

60. Moreover, the 2018 Policy does not require that "reasonable suspicion" be in any way related to the electronic device or its data. Rather, the 2018 Policy authorizes agents to review, copy, and analyze the content of an electronic device based only on suspicion that the owner of the device is violating CBP-administered laws, regardless of whether the agents reasonably suspect that the device or its data contain evidence of such a violation.

61. The 2018 Policy adds insult to injury by demanding that individuals facilitate these unlawful searches and seizures. Individuals must "present electronic devices and the information contained therein in a condition that allows inspection." This means that officers may require individuals to unlock or decrypt their devices or information and can "request[] and retain" "[p]asscodes or other means of access … as needed to facilitate the examination of an electronic device or [its] information." § 5.3.1.

62. While the 2018 Policy recommends that agents obtain supervisor approval before conducting a search, officers need only obtain such approval if it is "practicable." § 5.1.5. Similarly, while the 2018 Policy advises that "[s]earches of electronic devices should be conducted in the presence of the individual whose information is being examined," it permits agents to search devices outside their owners' presence if there are "national security, law enforcement, officer safety, or other operational considerations that make [owner presence] inappropriate." § 5.1.6.

63. Perhaps the most extraordinary part of the 2018 Policy relates to the detention of electronic devices and copying of their information. The policy gives officers power, absent any

individualized suspicion, to detain electronic devices and information copied from them "for a brief, reasonable period of time to perform a thorough border search." This period "ordinarily should not exceed five (5) days" but can be extended for undefined "extenuating circumstances." § 5.4.1. Detention can continue even after the individual has departed from the port of entry. § 5.4.1.1.

64. The 2018 Policy provides that electronic devices will be returned and data will be deleted only "if, after reviewing information, there exists no probable cause to seize the device or information." § 5.4.1.2. As a result, agents may permanently detain an electronic device and its data without a warrant. And the probable cause necessary to permanently detain devices or information can be generated through the initial searches and seizures performed without any individualized suspicion, absent any review from a neutral magistrate.

65. Agents are authorized to retain "information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of record notice," even absent any individualized suspicion. § 5.5.1.2.

66. Without individualized suspicion, the officer is authorized to transfer electronic devices and information thereon to other government agencies for a variety of purposes.

67. For example, without individualized suspicion, "[o]fficers may convey electronic devices or copies of information contained therein to seek technical assistance" so as to allow access to the device or its information. § 5.4.2.1. Officers may also convey devices or information to "subject matter experts" in other federal agencies "when there is a national security concern or … reasonable suspicion." § 5.4.2.2.

68. Individuals need not be notified when their devices or information are transmitted to other agencies. § 5.4.2.5.

69. The 2018 Policy also provides inadequate guidance on how officers should handle privileged and sensitive material. It contemplates that officers may "encounter[] information they identify as, or that is asserted to be, protected by attorney-client privilege or attorney work product doctrine." § 5.2.1. But the Policy provides no meaningful direction on how officers should handle that information. Rather, the Policy vaguely instructs officers to "ensure the segregation of any privileged material" so that it is "handled appropriately while also ensuring that CBP accomplishes its critical border security mission." § 5.2.1.2.

70. The 2018 Policy's guidance on "[o]ther possibly sensitive information" is even vaguer. "[M]edical records and work-related information carried by journalists … shall be handled in accordance with any applicable federal law and CBP policy." § 5.2.2. Business or commercial information shall be "protect[ed] from unauthorized disclosure." § 5.2.3.

71. The 2018 Policy contemplates that privileged or sensitive information may be shared with other federal agencies so long as those agencies "have mechanisms in place to protect appropriately such information." § 5.2.4.

72. The 2018 CBP Policy and 2009 ICE Policy essentially make the 885,000 cell phones that transit into and out of the United States every single day fair game for a warrantless and suspicionless search and seizure, alongside untold numbers of other devices containing sensitive information, like laptops.

73. These agency policies also promise to cause extraordinary inconvenience to travelers by authorizing detention of an electronic device for multiple days. For the many international travelers who do not intend to remain near their port of entry following admission to the United States, the policies constitute an extraordinary burden. And the burden is even greater for travelers whose electronics are detained as they are leaving the United States. These travelers are

given a choice of evils: abandoning their devices, with all of their personal information, to ICE and CBP; or losing up to thousands of dollars and many days of their time in order to reschedule their travel until their electronics clear inspection. Even burdening a million travelers a day with the *possibility* that they will be forced to endure these inconveniences to permit a warrantless and suspicionless search is an extraordinary intrusion on the liberty of citizens and visitors alike.

C. The Law of Electronic-Device Searches

74. CBP and ICE's electronic search policies are not only breathtakingly broad. They fly directly in the face of Supreme Court jurisprudence on protection for cell phones and other electronic devices and digital records and communications.

75. In *Riley v. California*, 573 U.S. 373 (2014), the Supreme Court recognized that the extraordinary powers and capabilities of cell phones place them in a class apart from other objects, requiring particularly robust Fourth Amendment protection. The *Riley* court unanimously held that law enforcement must not search digital information on a cell phone without first obtaining a warrant, except in a very narrow set of exigent circumstances.

76. Tellingly, all of the Justices based this holding on the unique characteristics of cell phones. Cell phones, the Court noted, 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." *Id.* at 385. Applying a traditional balancing assessment for warrant requirements, the Court concluded that the intrusion on privacy interests in a warrantless cell phone search far outweighs the government interest supporting it. *Id.* at 385-86. The Court noted that the only legitimate interest in a warrantless search—avoiding the remote deletion of evidence—was a relatively unlikely and weak one in most cases. *Id.* at 388-90. On the other hand, the Court recognized that allowing warrantless cell phone searches implicated stark and troubling privacy concerns. Noting the "immense storage capacity" of cell phones, the Court enumerated four distinct

ways that cell phones, among all objects law enforcement might search, have unique privacy implications: they collect "many distinct types of information … that reveal much more in combination than any isolated record"; they collect more of each individual type of information than previously possible; they collect this information over massive amounts of time, months or even years; and they are so pervasive in society that they function as a "digital record of nearly every aspect" of most Americans' lives, including their most personal information. *Id.* at 393-95. Taking these unique capacities together, the Supreme Court held that the balance of equities clearly favored requiring a warrant.

77. Similarly, courts have again and again found that people have a reasonable expectation of privacy in their computers and in folders and documents on their computers. *See United States v. Zavala*, 541 F.3d 562, 577 (5th Cir. 2008) (finding reasonable expectation of privacy in the contents of a person's cell phone and noting that "a cell phone is similar to a personal computer that is carried on one's person"); *see also, e.g., United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007); *United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir. 2007).

78. And, expectations of privacy aside, the Supreme Court has zealously guarded against "government trespass upon the areas ('persons, houses, papers, and effects')" that the Fourth Amendment enumerates. *United States v. Jones*, 565 U.S. 400, 406-07 (2012); *see also United States v. Ackerman*, 831 F.3d 1292, 1307 (10th Cir. 2016) (Gorsuch, J.).

79. Even some of the individual *functions* of cell phones and smartphones receive heightened constitutional protection. The Supreme Court recently held that law enforcement must secure a warrant to view data generated by the location-tracking functions of phones and other electronic devices. *Carpenter*, 138 S. Ct. at 2232-33. Several circuits have held that law enforcement officials may not access an individual's emails without a warrant; email is an essen-

tial function of virtually every smartphone. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288-89 (6th Cir. 2010). In other words, courts have overwhelmingly found that searches of phones, laptops, similar devices, and even some of their component functions require a warrant.

80. Nor are the courts particularly burdening law enforcement by requiring warrants. If technology has opened up vast troves of sensitive information to inspection by government agencies, it has also made it exceptionally easy for these agencies to secure a warrant with minimal effort and delay. As the Supreme Court noted in *Riley*, in one jurisdiction, "police officers can e-mail warrant requests' to judges' iPads [and] judges have signed such warrants and emailed them back to officers in less than 15 minutes." 573 U.S. at 401. Such a practice is not rare: the Supreme Court has previously noted that the Federal Rules of Criminal Procedure have permitted telephonic warrants since 1977. *Missouri v. McNeely*, 569 U.S. 141, 154 (2013). Law enforcement officials can secure a warrant quickly by a variety of means, including "telephonic or radio communication, electronic communication such as e-mail, and video conferencing." *Id.* The hurdle of securing a warrant is not high.

FACTUAL ALLEGATIONS

A. Mr. Anibowei Begins Receiving Intense Scrutiny at the Airport, and Is Removed Without Notice from CBP's Global Entry Trusted Traveler Program

81. Plaintiff George Anibowei was born in Port Harcourt, Rivers State, Nigeria and is originally from Agbere, Bayelsa State, in the Niger Delta region of Nigeria. Mr. Anibowei fled Nigeria in 1997 after his work as a pro-democracy activist put him in danger of retaliation by Nigeria's military dictatorship, then led by General Sani Abacha.

82. Seeking a life with more freedoms and civil liberties, Mr. Anibowei applied for and received asylum in the United States in 1998. He became a naturalized U.S. citizen in 2007.

83. A lawyer by profession in Nigeria, Mr. Anibowei completed a master's degree and Juris Doctor degree at Southern Methodist University Law School in Dallas. He is admitted to practice law before all courts in the State of Texas, the U.S. District Court for the Northern District of Texas, the U.S. Court of Appeals for the Fifth Circuit, and the U.S. Supreme Court. Originally drawn to Texas because one of his brothers lived there, he has settled in the Dallas suburbs and operates his own small legal practice, primarily representing immigrants.

84. To become a naturalized U.S. citizen in the years following the September 11th attacks, Mr. Anibowei had to pass an extensive security check.[11] The requirements for this background check are rigorous. All applicants must undergo fingerprinting, which the FBI then uses to run a full criminal background check. The FBI also conducts a "name check," which includes a search against a database that contains not only criminal files but also personnel, administrative, and applicant files. In addition to these FBI background checks, most applicants also go through additional inter-agency background checks coordinated by U.S. Citizenship and Immigration Services.

85. Mr. Anibowei is a frequent traveler. He typically travels to Nigeria several times a year to visit his brothers and sisters who still live there, as well as his extended family and friends. He is also a frequent tourist in Europe, the Caribbean, and other African countries.

86. In order to facilitate his travel, Mr. Anibowei applied for and eventually received membership in CBP's Global Entry Trusted Traveler Program, beginning on November 1, 2012. The Trusted Traveler Program requires applicants to pass another layer of extremely thorough security checks in order to receive membership. Successful applicants must pass a background

[11] *See USCIS Policy Manual: Chapter 2—Background and Security Checks*, U.S. Citizenship and Immigration Services, https://www.uscis.gov/policymanual/HTML/PolicyManual-Volume12-PartB-Chapter2.html (Feb. 12, 2019).

check against criminal, law enforcement, customs, immigration, agriculture, and terrorist indices, a process that includes fingerprinting.[12] Successful applicants also pass an in-person interview with a security officer.

87. In 2014, Mr. Anibowei took a leave of absence from his law practice to return to Nigeria in order to participate in a national constitutional conference called by the country's now democratically elected government. The convention, known as the 2014 Nigerian National Conference, brought together 492 distinguished delegates from Nigeria and the Nigerian Diaspora to debate structural problems with the country's constitution and propose reforms directly to the immediate past President, Goodluck Jonathan. Attendees at the conference included retired governors and ministers in the Nigerian Government and prominent Nigerian politicians and lawyers. Concerns at the conference included power-sharing among different states and the federal government and states' ability to profit off their own natural resources—a particular concern of states in the oil-rich Niger Delta, where Mr. Anibowei is from.

88. Mr. Anibowei spent much of his five months in Nigeria as one of the National Assembly's 492 delegates, while a colleague shouldered the matters pending at his solo practice. On breaks in the Assembly, he returned to Texas to check on his law office.

89. To the best of Mr. Anibowei's recollection, it was around the time of the Nigerian National Conference that TSA began to subject Mr. Anibowei to additional screening virtually every time he entered or left the United States, even as a member of the Trusted Traveler Program. Initially, this mainly consisted of putting Mr. Anibowei into secondary screening on his way to and from Nigeria to ask him about the purpose and length of his trip.

---

[12] *Is Criminal History a Disqualifier for Global Entry?* U.S. Customs and Border Protection (Aug. 2, 2017), https://help.cbp.gov/app/answers/detail/a_id/1309/~/is-criminal-history-a-disqualifier-for-global-entry%3F.

90. Mr. Anibowei believes he was initially flagged for routine additional screening because he was spending a long period of time in Nigeria and frequently traveling back to the United States.

91. TSA and CBP continued to question and detain Mr. Anibowei virtually every time he traveled internationally, and the screening of Mr. Anibowei gradually grew more intense. In spring of 2014, Mr. Anibowei was traveling with his son, who shares his name, from Houston, Texas to Lagos, Nigeria, when Mr. Anibowei's then-teenage son was taken aside by seven uniformed officers. The officers soon realized they were looking for Mr. Anibowei rather than his son. Subsequently, five officers took Mr. Anibowei into a small room for interrogation, inviting his son in too against the wishes of Mr. Anibowei. As a result, Mr. Anibowei's son witnessed his father's interrogation, a situation his father found humiliating.

92. The officers detained and questioned Mr. Anibowei for approximately two hours, resulting in his flight being delayed for that period. Mr. Anibowei did not realize that he was the reason for the flight delay until a manager from United Airlines walked into the interrogation room and asked one of the officers whether they could begin boarding the flight. The officer responded that the manager could proceed because they were almost done questioning Mr. Anibowei.

93. This treatment continued after the Nigerian National Conference had ended. In another incident from that period, Mr. Anibowei was stranded in Toronto for two days after the Canadian Border Services Agency subjected him to a five-hour interrogation at the request of CBP, causing him to miss his flight.

94. On May 12, 2015, when returning from another international trip, Mr. Anibowei learned that, for reasons unknown to him, his membership in the Global Entry Trusted Traveler

Program had been revoked on March 7, 2015. Mr. Anibowei received no notice of this development until he attempted to reenter the United States using a Global Entry kiosk at the airport only to be pulled once again into secondary inspection. In secondary inspection, the CBP agent told Mr. Anibowei that his Global Entry status had been revoked. CBP never sent Mr. Anibowei a letter notifying him of the change. Mr. Anibowei ultimately was able to download the revocation letter from his account on the Global Online Enrollment System, a website managed by CBP.

95. Mr. Anibowei has since made numerous and apparently unavailing efforts to appeal this decision. Mr. Anibowei first requested reconsideration of his application for the Trusted Traveler Program from CBP. In a response from the CBP Ombudsman dated March 11, 2016, the Ombudsman acknowledged receipt of Mr. Anibowei's request but reiterated, using the same language as the revocation letter, that Mr. Anibowei "d[id] not meet the eligibility requirements for the Trusted Traveler program."

96. Mr. Anibowei also filed a Redress Request (#2232471) with CBP on DHS's Traveler Redress Inquiry Program (TRIP) Website. In response to this Redress Request, Mr. Anibowei received a letter dated June 30, 2016 from Deborah O. Moore, the Director of TRIP. The letter stated:

> DHS has researched and completed our review of your case. Security Procedures and legal concerns mandate that we can neither confirm nor deny any information about you which may be within federal watch lists or reveal any law enforcement sensitive information. However, we have made any corrections to records that our inquiries determined were necessary, including, as appropriate, notations that may assist in avoiding incidents of misidentification.

B. Mr. Anibowei's Cell Phone Is Copied by CBP, and Subjected to a Search on No Fewer Than Five Occasions

97. At this point, Mr. Anibowei had simply accepted that he would be stopped and screened, sometimes for hours, any time he tried to leave or enter the United States. Trying to

adjust to this new reality, he mentally prepared (and still does) to be pulled into secondary interrogation on every trip. On occasions when another person intends to pick Mr. Anibowei up at the Dallas-Fort Worth Airport, he tells them to come two or three hours after his scheduled flight arrival time because he knows he will be put into inspection.

98. On October 10, 2016, Mr. Anibowei was returning to the Dallas area after a weekend spent visiting his best friend in Toronto. Upon landing in Dallas, the pilot announced that the passengers—who had begun to collect their luggage in preparation to exit the plane—should return to their assigned seats, because security had arrived at the gate to escort a passenger off.

99. Mr. Anibowei, who had slept through the flight, assumed that the announcement had to do with an unruly passenger. He was consequently surprised when a pair of agents boarded the flight, asked to see his identification, and told him to take his luggage and follow them. The officers subsequently escorted Mr. Anibowei off the plane and through three terminals at the airport, to his great humiliation and distress.

100. The officers eventually brought Mr. Anibowei to a small interrogation room, where they asked him for his phone. When Mr. Anibowei asked them why they wanted to see it, the agents told him that they planned to "copy the hard drive," taking his phone out of the room.

101. When Mr. Anibowei vigorously protested this action, the officers handed him a flyer explaining their legal authority, under the 2009 CBP Directive, to undertake the search and seizure.

102. The officers returned Mr. Anibowei's phone to him about thirty minutes after they seized it.

103. The phone the officers seized was Mr. Anibowei's work cell phone. As an attorney, Mr. Anibowei takes his work phone with him virtually everywhere, in order to be accessible for time-sensitive matters or in a client emergency, and he estimates that approximately 80 percent of his clients prefer to call him on his cell phone. Mr. Anibowei's phone contains extremely sensitive information about his clients and their cases, including call logs, voice mails, text message threads with clients, and perhaps worst of all an archive of Mr. Anibowei's work emails, which in turn contains drafts of confidential filings among other information.

104. This seizure was particularly distressing to Mr. Anibowei because a significant number of his clients are immigrants in removal proceedings adverse to DHS. The seizure and copying of Mr. Anibowei's phone by an agency of DHS was a gross violation of these clients' expectation of privacy in their privileged legal communications with their attorney, committed by the adverse party in those clients' cases.

105. This was the last time Mr. Anibowei carried his work phone with him on an international trip. But the damage was already done. To this day, Mr. Anibowei has no idea why the agency copied data from his cell phone and for what purpose, if any, it has used the data. He believes that, to this day, the agency never destroyed the data and continues to retain them.

106. Furthermore, Mr. Anibowei's decision to stop carrying his work phone was not a complete solution. Mr. Anibowei's work emails are also accessible on his personal phone. However, to stop carrying his personal phone would render Mr. Anibowei completely inaccessible in either a personal or work emergency.

107. Since the October 16, 2016 incident, Mr. Anibowei's phone has been searched a minimum of four additional times by officers of DHS.

108. An incident on February 12, 2017 was typical. Mr. Anibowei was returning from a visit to his friends and relatives in Nigeria, and was put into secondary inspection on returning to the Dallas-Fort Worth Airport. In secondary inspection, TSA agents performed an extremely thorough search of all of Mr. Anibowei's luggage and asked to see his phone. A TSA agent then performed an extensive search of Mr. Anibowei's phone in front of him. Mr. Anibowei believes that the officer viewed his text messages, as well as encrypted messages he sent and received through WhatsApp (a texting application very popular globally). Because Mr. Anibowei's email is not password protected on his phone, it is possible the officer viewed Mr. Anibowei's email, too.

109. There is an extraordinary irony to Mr. Anibowei's case. Mr. Anibowei came to the United States seeking freedom. He makes a living helping other people who wish to enjoy this country's freedoms. While Mr. Anibowei is not certain, he believes that the catalyst for CBP's increased interest in him was his frequent travel overseas. And, since 2016, that travel has resulted in scrutiny of every aspect of his personal and professional life, via CBP's free and un-inhibited access to all of the data on his phone.

110. Mr. Anibowei fears grave injury to his reputation and his business as a result of CBP and ICE's search and copying of his phone. Mr. Anibowei fears that if his clients knew or believed that CBP had copied their data from Mr. Anibowei's phone, it would diminish their trust and confidence in him as an attorney.

111. CBP and ICE's illegal electronics search and seizure policies have worked a grave injury to Mr. Anibowei's First and Fourth Amendment rights.

112. Mr. Anibowei intends to continue traveling internationally to visit his family in Nigeria and for pleasure.

113. Based on his experiences recounted above, Mr. Anibowei reasonably believes that Defendants will continue to violate his First and Fourth Amendment rights when he travels internationally in the future.

FACTS RELEVANT TO ALL CLAIMS FOR RELIEF

114. Defendants adopted the policies and practices discussed above related to searching and seizing electronic devices at the border.

115. The frequency with which border officials enforce these policies and practices against travelers is rapidly growing.

116. Mr. Anibowei has traveled across the U.S. border with his cell phone multiple times.

117. Mr. Anibowei has a credible fear that his cell phone will be searched again.

118. Mr. Anibowei is suffering the ongoing harm of the confiscation of the information on his cell phone.

119. Mr. Anibowei's phone is private personal property that agents have taken without his consent.

120. Mr. Anibowei has a reasonable expectation of privacy in the content on his cell phone, in the content he stores in the cloud that is accessible through his cell phone, in his device passwords, and in the information he holds as an information fiduciary on behalf of other people.

121. Mr. Anibowei uses his cell phone to communicate, associate, and gather and receive information privately and anonymously.

122. Mr. Anibowei uses his cell phone to store sensitive attorney work product and confidential information on behalf of his clients, some of whom are immigrants adverse to Defendants.

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

124. Mr. Anibowei feels confused, embarrassed, upset, violated, and anxious about the search and copying of his cell phone. He worries that government agents have viewed personal information taken from his phone, including photos and messages, and shared it with other government agencies. He worries about his own personal information, and also personal information from and about other people, including friends, family, clients, and professional associates.

125. 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, by promulgating or causing to be promulgated the ICE and CBP policies permitting the search of Mr. Anibowei's phone, and by directing agents to enforce those policies.

126. By the acts alleged above, Defendants have proximately caused harm to Mr. Anibowei.

127. Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of Mr. Anibowei's constitutional rights.

128. Defendants will continue to violate Mr. Anibowei's constitutional rights unless enjoined from doing so by this Court.

CLAIMS FOR RELIEF

COUNT I
FIRST AMENDMENT

129. Plaintiff re-alleges each and every allegation in paragraphs 1-128 above as if fully set forth herein.

130. Defendants violate the First Amendment by searching and seizing individuals' devices and communications containing expressive content, associational information, and privileged information, *absent a warrant supported by probable cause* that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

131. Defendants violate the First Amendment by searching and seizing individuals' devices and communications containing expressive content, associational information, and privileged information, *absent probable cause* to believe that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

132. Defendants violate the First Amendment by searching and seizing individuals' devices and communications containing expressive content, associational information, and privileged information, *absent reasonable suspicion* that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

133. Defendants have violated and will continue to violate Mr. Anibowei's First Amendment rights by searching and seizing his devices and communications containing expressive content, associational information, and privileged information, absent a warrant, probable cause, or a reasonable suspicion that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

COUNT II
FOURTH AMENDMENT
(Unlawful Search of Electronic Devices)

134. Plaintiff re-alleges each and every allegation in paragraphs 1-128 above as if fully set forth herein.

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

136. Defendants violate the Fourth Amendment by searching individuals' devices and communications containing expressive content, associational information, and privileged information, *absent probable cause* to believe that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

137. Defendants violate the Fourth Amendment by searching individuals' devices and communications containing expressive content, associational information, and privileged information, *absent reasonable suspicion* that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

138. Defendants' searches are unreasonable at their inception, and in their scope, duration, and intrusiveness.

139. Defendants have violated and will continue to violate the Fourth Amendment by searching Mr. Anibowei's electronic devices, absent a warrant, probable cause, or a reasonable suspicion that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

140. Defendants' searches of Mr. Anibowei's electronic devices are unreasonable at their inception, and in their scope, duration, and intrusiveness.

COUNT III
FOURTH AMENDMENT
(Unlawful Search of Communications)

141. Plaintiff re-alleges each and every allegation in paragraphs 1-128 above as if fully set forth herein.

142. Defendants violate the Fourth Amendment by searching individuals' emails, text messages, and other private communications, *absent a warrant supported by probable cause* that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

143. Defendants violate the Fourth Amendment by searching individuals' devices and communications containing expressive content, associational information, and privileged information, *absent probable cause* to believe that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

144. Defendants violate the Fourth Amendment by searching individuals' devices and communications containing expressive content, associational information, and privileged information, *absent reasonable suspicion* that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

145. Defendants' searches are unreasonable at their inception, and in scope, duration, and intrusiveness.

146. Defendants have violated and will continue to violate the Fourth Amendment by searching Mr. Anibowei's electronic devices, absent a warrant, probable cause, or a reasonable suspicion that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

147. Defendants' searches of Mr. Anibowei's electronic devices are unreasonable at their inception, and in their scope, duration, and intrusiveness.

COUNT IV
FOURTH AMENDMENT
(Unlawful Seizure of Devices)

148. Plaintiff re-alleges each and every allegation in paragraphs 1-128 above as if fully set forth herein.

149. Defendants violate the Fourth Amendment by seizing individuals' electronic devices for the purpose of effectuating searches of those devices after individuals leave the border, *absent a warrant, probable cause, or reasonable suspicion* that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

150. These seizures are unreasonable at their inception, and in scope, duration, and intrusiveness.

151. Defendants have violated and will continue to violate the Fourth Amendment by seizing Mr. Anibowei's electronic devices for the purpose of effectuating searches of those devices after he leaves the border, absent a warrant, probable cause, or reasonable suspicion that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

152. Defendants' seizures of Mr. Anibowei's electronic devices are unreasonable at their inception, and in their scope, duration, and intrusiveness.

COUNT V
FOURTH AMENDMENT
(Unlawful Seizure of Data)

153. Plaintiff re-alleges each and every allegation in paragraphs 1-128 above as if fully set forth herein.

154. Defendants violate the Fourth Amendment by seizing individuals' data and retaining that data, often after individuals leave the border, *absent a warrant, probable cause, or rea-*

sonable suspicion that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

155. These seizures are unreasonable at their inception, and in their scope, duration, and intrusiveness.

156. Defendants have violated and will continue to violate the Fourth Amendment by seizing Mr. Anibowei's data and retaining that data, after he leaves the border, absent a warrant, probable cause, or reasonable suspicion that the devices contain contraband or evidence of a violation of criminal, immigration, or customs laws.

COUNT VI
ADMINISTRATIVE PROCEDURE ACT, 5 U.S.C. § 706
(Agency Policies)

157. Plaintiff re-alleges each and every allegation in paragraphs 1-128 above as if fully set forth herein.

158. Each of the 2018 CBP Directive, the 2009 CBP Directive, and the 2009 ICE Directive (collectively, the "Agency Policies") is a "final agency action" subject to judicial review under the Administrative Procedure Act, 5 U.S.C. § 704.

159. The Agency Policies permit agents to conduct searches that violate the First and Fourth Amendments. The Agency Policies therefore violate the Administrative Procedure Act because they are "contrary to constitutional right, power, privilege, or immunity." 5 U.S.C. § 706(2)(B).

160. The Agency Policies further violate the Administrative Procedure Act because they are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

COUNT VII
ADMINISTRATIVE PROCEDURE ACT, 5 U.S.C. § 706
(Global Entry)

161. Plaintiff re-alleges each and every allegation in paragraphs 1-128 above as if fully set forth herein.

162. Defendants' removal of Plaintiff from the Global Entry Trusted Traveler Program is a "final agency action" subject to judicial review under the Administrative Procedure Act, 5 U.S.C. § 704.

163. Plaintiff has exhausted all of his administrative remedies and any further pursuit of administrative relief would be futile.

164. Defendants' removal of Plaintiff from the Global Entry Trusted Traveler Program violated the Administrative Procedure Act because it was "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff asks for the following relief as to all counts:

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

b. Declare that Defendants violated Plaintiff's First and Fourth Amendment rights by searching his electronic devices absent a warrant supported by probable cause that the devices contained contraband or evidence of a violation of criminal, immigration, or customs laws, and without particularly describing the information to be searched.

c. Enjoin Defendants to expunge all information gathered from, or copies made of, the contents of Plaintiff's electronic devices.

d. Enjoin enforcement of the Agency Policies against Plaintiff.

e. Enjoin enforcement of the Agency Policies.

f. Vacate the Agency Policies.

g. Award Plaintiff reasonable attorneys' fees and costs.

h. Grant such other or further relief as the Court deems proper.

Dated: March 14, 2019

Respectfully submitted,

ARNOLD & PORTER
KAYE SCHOLER LLP

By: */s/ Andrew Tutt*

Andrew Tutt (*pro hac vice*)
Robert Stanton Jones (*pro hac vice*)
Stephen K. Wirth (*pro hac vice*)
Sam Callahan (*pro hac vice*)
Graham White (*pro hac vice*)
Jayce Lane Born (*pro hac vice*)
Emily Rebecca Chertoff (*pro hac vice*)
ARNOLD & PORTER KAYE SCHOLER LLP
601 Massachusetts Ave., NW
Washington, DC 20001
(202) 942-5000
(202) 942-5999 (fax)
andrew.tutt@arnoldporter.com

Hani Mirza (State Bar No. 24083512)
TEXAS CIVIL RIGHTS PROJECT
1412 Main St., Suite 608
Dallas, Texas 75202
(972) 333-9200 ext. 171
(972) 957-7867 (fax)
hani@texascivilrightsproject.org

Natalia Cornelio*
Peter Steffensen (*pro hac vice*)
(State Bar No. 24106464)
TEXAS CIVIL RIGHTS PROJECT
405 Main Street, Suite 716
Houston, Texas 77002
(832) 767-3650
(832) 554-9981 (fax)
natalia@texascivilrightsproject.org

* Motion for pro hac vice admission forthcoming

Counsel for Plaintiff

VERIFICATION

STATE OF TEXAS)
) SS:
DALLAS COUNTY)

George Anibowei, being duly sworn, deposes and says:

I am George Anibowei, the plaintiff in this action; I have read the foregoing Verified Second Amended Complaint and know the contents thereof; except as to matters therein alleged on information and belief, I have learned of the facts alleged therein, either through my own personal knowledge or through information reported to me in the ordinary course of business; as to those matters as to which I do not have personal knowledge, I believe them to be true.

George Anibowei

Sworn to and subscribed this
12 day of March, 2019

Notary Public

VANESSA A. NARVAIZ
My Notary ID # 131302865
Expires October 3, 2021

CERTIFICATE OF SERVICE

I hereby certify that this document will be served on the Defendants in accordance with Fed. R. Civ. P. 4.

/s/ Andrew Tutt

Andrew Tutt
601 Massachusetts Ave., NW
Washington, DC 20001
(202) 942-5000
andrew.tutt@arnoldporter.com