APPENDIX

TABLE OF CONTENTS

Filed: November 19, 2025

United States Court of Appeals
for the Fifth Circuit

No. 24-11042

GEORGE ANIBOWEI,

Plaintiff–Appellant,

versus

PAMELA BONDI, *U.S. Attorney General*; UNITED STATES DEPARTMENT OF HOMELAND SECURITY; UNITED STATES CUSTOMS AND BORDER PROTECTION; UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT; KRISTI NOEM, *Secretary, U.S. Department of Homeland Security*; TROY MILLER, *Senior Official Performing the Duties of the Commissioner*, *U.S. Customs and Border Protection*; PATRICK J. LECHLEITNER, *Deputy Director and Senior Official Performing the Duties of the Director for ICE*,

Defendants–Appellees.

Appeal from the United States District Court
for the Northern District of Texas
USDC No. 3:16-CV-3495

Before ELROD, *Chief Judge*, and CLEMENT and HAYNES, *Circuit Judges.*

PER CURIAM:*

---

* This opinion is not designated for publication. *See* 5th Cir. R. 47.5.

George Anibowei, a naturalized United States citizen and attorney in Texas, appeals the district court's dismissal of his Administrative Procedure Act ("APA") claim seeking vacatur of three directives promulgated by United States Customs and Border Protection ("CBP") and United States Immigration and Customs Enforcement ("ICE") (together, "the Government").[1] In 2016, CBP officers at Dallas-Fort Worth International Airport seized Anibowei's work cell phone when he returned from an international trip and, without his consent or a warrant, copied his phone's data. Since this incident, border agents have warrantlessly searched Anibowei's cell phone at least four additional times.

Anibowei filed suit against the Government, which, ultimately, moved to dismiss Anibowei's remaining claim under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). The district court granted this motion and dismissed Anibowei's claim for lack of subject matter jurisdiction under Rule 12(b)(1), and, alternatively, for failure to state a claim on which relief can be granted under Rule 12(b)(6).

We have jurisdiction over this appeal under 28 U.S.C. § 1291. We review de novo a district court's dismissal under Rules 12(b)(1) and 12(b)(6), "taking all well-pleaded factual allegations in the complaint as true, and viewing them in the light most favorable to the plaintiff." *Gonzalez v. Blue Cross Blue Shield Ass'n*, 62 F.4th 891, 898 (5th Cir. 2023) (citation

---

[1] Specifically, CBP, Directive No. 3340-049, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION (2009); ICE, DIRECTIVE NO. 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES (2009); and CBP, Directive No. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (2018).

omitted). "We may affirm the district court's dismissal on any ground the record supports," including the alternative ground that Anibowei failed to state a claim upon which relief can be granted. *Id.* (citation omitted); *see also Cardoso v. Reno*, 216 F.3d 512, 515 (5th Cir. 2000) ("[T]his Court has long recognized that reversal is inappropriate if the ruling of the district court can be affirmed on any grounds, regardless of whether those grounds were used by the district court." (internal quotations and citation omitted)). We respectfully decline to affirm the dismissal under Rule 12(b)(1).[2]

---

[2] We have previously explained that "[w]hen a Rule 12(b)(1) motion is filed in conjunction with other Rule 12 motions, the court should consider the Rule 12(b)(1) jurisdictional attack before addressing any attack on the merits." *Wolcott v. Sebelius*, 635 F.3d 757, 762 (5th Cir. 2011) (citation omitted). We assume without deciding that the district court properly treated the Government's argument that Anibowei had "an adequate alternative remedy to APA judicial relief" as a jurisdictional inquiry and first turn to the district court's grant of the Government's Rule 12(b)(1) motion. The district court considered 5 U.S.C. § 704, which states that "final agency action for which there is no other adequate remedy in a court [is] subject to judicial review." The district court reasoned that, because Anibowei had "an adequate alternative remedy" available to him in the form of "bringing a constitutional challenge and seeking injunctive relie[f]," it did not have subject matter jurisdiction over Anibowei's APA claim. However, "[t]he 'adequate remedy' provision of § 704 is intended 'simply to avoid duplicating previously established special statutory procedures for review of agency actions.'" *Rollerson v. Brazos River Harbor Navigation Dist.*, 6 F.4th 633, 641 (5th Cir. 2021) (quoting *Darby v. Cisneros*, 509 U.S. 137, 146 (1993)). This "exception will apply only if there is clear and convincing evidence of legislative intent to create a special, alternative remedy and thereby bar APA review." *Fort Bend Cnty. v. U.S. Army Corps of Eng'rs*, 59 F.4th 180, 192 (5th Cir. 2023) (citation omitted). Neither the district court nor the

Turning to Rule 12(b)(6), Anibowei asserts that the border search exception does not apply to cell phone searches and urges us to reconsider en banc our precedent in *United States v. Castillo*, 70 F.4th 894 (5th Cir. 2023), and *Malik v. United States Department of Homeland Security*, 78 F.4th 191 (5th Cir. 2023), so that we may hold that warrants are required for most cell phone searches at the border.

However, we are bound by our rule of orderliness to follow *Castillo* and *Malik*. *See In re Bonvillian Marine Serv., Inc.*, 19 F.4th 787, 792 (5th Cir. 2021). As Anibowei explained in his reply brief (with added emphasis), "[a]ll agree that the validity of the Directives at issue in this case turns squarely *and solely* on the question whether the Fourth Amendment generally requires warrants to search cell phones at the border." *Castillo* and *Malik* answer this question in the negative and foreclose Anibowei's argument. *See Castillo*, 70 F.4th at 898; *Malik*, 78 F.4th at 200–01. Therefore, due to the rule of orderliness, we AFFIRM, on this ground, the district court's dismissal of Anibowei's complaint.

---

parties point to such "clear and convincing evidence," *id.*, and we decline to affirm the district court's dismissal of Anibowei's claim on this ground.

Filed November 22, 2024

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

GEORGE ANIBOWEI,	§	
Plaintiff,	§	
	§	
VS.	§	Civil Action No.
ALEJANDRO MAYORKAS, et al.,	§	3:16-CV-3495-D
	§	
Defendants.	§	
	§	

MEMORANDUM OPINION
AND ORDER

Defendants—including U.S. Department of Homeland Security ("DHS"), U.S. Customs and Border Protection ("CBP"), and U.S. Immigration and Customs Enforcement ("ICE") (collectively, "defendants")[1]—move to dismiss Count VI of plaintiff George Anibowei's ("Anibowei's") second amended complaint: the remaining claim that Anibowei brings under the Administrative Procedure Act ("APA"), 5 U.S.C. § 706(2)(A)-(B), seeking vacatur of three directives promulgated by CBP and ICE, and declaratory and injunctive relief against the departments and agencies and the individual

[1] The other defendants are: Secretary of Homeland Security Alejandro Mayorkas, in his official capacity; Troy A. Miller, Senior Official Performing the Duties of the Commissioner for CBP, in his official capacity; Patrick J. Lechleitner, Deputy Director and Senior Official Performing the Duties of the Director for ICE, in his official capacity; and Attorney General Merrick Garland, in his official capacity

department and agency heads in their official capacity.[2] Defendants move to dismiss Count VI for lack of subject matter jurisdiction and failure to state a claim on which relief can be granted. It appears that Anibowei is essentially conceding that he will lose if this court reaches the merits, but he is attempting to avoid dismissal for lack of jurisdiction so that the merits will be at issue on appeal. For the reasons that follow, the court grants defendants' motion and dismisses Count VI of Anibowei's second amended complaint for lack of subject matter jurisdiction. Alternatively, the court dismisses Count VI for failure to state a claim on which relief can be granted.

I

Anibowei, a lawyer, is a naturalized U.S. citizen who was born in Nigeria. He owns a small law practice where he primarily handles immigration matters. Anibowei travels several times a year, often internationally, for both work and personal reasons. In October 2016 CBP officers at the Dallas-Fort Worth International Airport seized Anibowei's work cell phone, without his consent or a search warrant, and advised Anibowei that they were going to copy the hard drive. When Anibowei protested, the officers gave him a flyer explaining their legal authority to search and seize his phone under CBP Directive No. 3349-049, Border Search of Electronic Devices Containing Information (Aug. 20, 2009) ("2009 CBP Directive"). Anibowei's work cell phone contains

[2] Anibowei initially brought seven claims for relief, including under the First and Fourth Amendments, but he voluntarily dismissed with prejudice all claims other than count VI, his APA claim, on June 17, 2024.

sensitive information about his clients and their cases, including call logs, voice mails, text messages, and an archive of Anibowei's work emails with drafts of confidential filings and other information involving removal proceedings adverse to DHS.[3]

At the time of filing his second amended complaint, CBP agents had searched Anibowei's phone at least four additional times. He intends to continue traveling internationally, but he now does so without his work phone because of the risk of further invasions of his and his clients' privacy. He continues to carry his personal phone when he travels, which also has access to his work email.

Anibowei seeks vacatur of three directives: the 2009 CBP Directive, CBP Directive No. 3340-049A, Border Search of Electronic Devices (Jan. 4, 2018) ("2018 CBP Directive"), and ICE Directive 7-6.1, Border Searches of Electronic Devices (Aug. 18, 2009) ("2009 ICE Directive") (collectively, "Directives"). He also seeks a declaration that defendants' policies and practices violate the First and Fourth Amendments by authorizing searches of electronic devices absent a warrant supported by probable cause; a declaration that they violated his First and Fourth Amendment rights by searching his devices absent a warrant supported by probable cause; an injunction ordering defendants to expunge information gathered from or copies made of the contents of his devices; an injunction against enforcement of the agency policies against himself and across the board; and reasonable attorney's fees and costs and other such relief that the court deems proper.

---

[3] CBP is a component of DHS.

The court has heard oral argument.

II

"Federal courts are courts of limited jurisdiction, and absent jurisdiction conferred by statute, lack the power to adjudicate claims." *Stockman v. Fed. Election Comm'n*, 138 F.3d 144, 151 (5th Cir. 1998). When challenging subject matter jurisdiction under Fed. R. Civ. P. 12(b)(1), a party can make a facial attack or a factual attack. *See Paterson v. Weinberger*, 644 F.2d 521, 523 (5th Cir. May 1981). If, as here, the party merely files a Rule 12(b)(1) motion, the attack is considered facial, and the court looks only at the sufficiency of the allegations in the complaint and assumes them to be true. *Id.* If the allegations are sufficient to allege jurisdiction, the court must deny the motion. *Id.* This is akin to a Rule 12(b)(6) motion in that the "pleading's allegations are presumed to be true, and '[i]f those allegations sufficiently allege a claim for recovery the complaint stands and the federal court must entertain the suit.'" *Vinmar Overseas, Ltd. v. OceanConnect, LLC*, 2012 WL 3599486, at *4 (S.D. Tex. Aug. 20, 2012) (Rosenthal, J.) (alteration in original) (quoting *Jones v. SuperMedia Inc.*, 281 F.R.D. 282, 286 (N.D. Tex. 2012) (Boyle, J.)). "The burden of proof for a Rule 12(b)(1) motion to dismiss is on the party asserting jurisdiction. Accordingly, the plaintiff constantly bears the burden of proof that jurisdiction does in fact exist." *Ramming v. United States*, 281 F.3d 158, 161 (5th Cir. 2001) (per curiam) (citations omitted).

"In deciding a Rule 12(b)(6) motion to dismiss, the court evaluates the sufficiency of plaintiffs' . . . complaint by 'accepting all well-pleaded facts as true, viewing them in the light most favorable to the plaintiff.'" *Bramlett v. Med. Protective Co. of Fort Wayne, Ind.*, 855 F.Supp.2d 615, 618 (N.D. Tex. 2012) (Fitzwater, C.J.) (internal quotation marks and alteration omitted) (quoting *In re Katrina Canal Breaches Litig.*, 495 F.3d 191, 205 (5th Cir. 2007)). To survive defendants' motion, plaintiff must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*; *see also Twombly*, 550 U.S. at 555 ("Factual allegations must be enough to raise a right to relief above the speculative level[.]"). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'shown'—'that the pleader is entitled to relief.'" *Iqbal*, 556 U.S. at 679 (quoting Rule 8(a)(2)) (alteration omitted). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678 (citation omitted).

III

The court begins with defendants' assertion under Rule 12(b)(1) that this court does not have subject matter jurisdiction over Anibowei's APA claim. Defendants contend that the court lacks jurisdiction because: (1) Anibowei's challenges to the Directives are moot; (2) his alleged injuries would not be redressed by his requested relief; (3) the Directives do not constitute final agency actions such that there is jurisdiction under the APA; and (4) Anibowei has an adequate alternative remedy to APA judicial relief, meaning there is no jurisdiction under the APA.

A

The court turns first to defendants' contention that Anibowei's claim is moot with respect to the 2009 CBP Directive and the 2009 ICE Directive because each has been superseded.[4]

1

Article III of the Constitution limits federal judicial power to cases and controversies. *United States Parole Comm'n v. Geraghty*, 445 U.S. 388, 395 (1980). A case becomes moot "when the issues presented are no longer 'live' or the parties lack a legally cognizable interest in the outcome," *id.* at 396 (quoting *Powell v. McCormack*, 395 U.S. 486, 496 (1969)), or "[i]f a dispute has been resolved or if it has evanesced because of changed circumstances, including the passage of time," *Am. Med. Ass'n v. Bowen*, 857 F.2d 267, 270 (5th Cir. 1988). A claim against an agency regulation or other directive may become moot if the agency repeals the offending pronouncement. *Spell v. Edwards*, 962 F.3d 175, 179 (5th Cir. 2020). If an agency repeals a challenged directive but then replaces it with a substantially similar one, there is no mootness because the injury remains. *Franciscan All., Inc. v. Becerra*, 47 F.4th 368, 374 (5th Cir. 2022).

---

[4] Anibowei does not contest defendants' assertion that the claim for vacatur of the 2009 CBP Directive is moot because it has been superseded by the 2018 CBP Directive.

The issue is whether the court can still order "effectual relief . . . to the prevailing party." *Knox v. Serv. Emps. Int'l Union, Local 1000*, 567 U.S. 298, 307 (2012) (citation and internal quotation marks omitted).

2

The parties do not dispute that the 2018 CBP Directive remains in effect. Additionally, the 2009 ICE Directive remains in effect except to the extent that it has been superseded by supplemental ICE guidance, *see* Ds. App. (ECF No. 125) at 33-34. The section Anibowei challenges—which allows searches and seizures of electronic devices without a warrant and probable cause—is modified by ICE Supplemental Guidance, Legal Update – Border Search of Electronic Devices (May 11, 2018) ("2018 ICE Guidance"). Ds. App. (ECF No. 125) at 33-34. The 2018 ICE Guidance replaces the policy in the 2009 ICE Directive allowing searches and seizures of electronic devices with or without individualized suspicion, *see* Ds. App. (ECF No. 125) at 24, with the requirement that agents "should no longer perform advanced border searches of electronic devices without reasonable suspicion," *id.* at 33-34. Because Anibowei challenges the policy allowing searches and seizures of devices without a warrant or probable cause, and both the original and updated versions of the policy allow for such searches and seizures, the challenge is not moot to the extent that the original policy has been replaced with a substantially similar one. *See Franciscan All., Inc.*, 47 F.4th at 374. Therefore, Count VI of Anibowei's second amended complaint should not be dismissed based on mootness.

B

The court turns next to defendants' assertion that Anibowei lacks standing because his alleged injuries would not be redressed by vacatur of the Directives.

1

"[T]he requirement that a claimant have 'standing is an essential and unchanging part of the case-or-controversy requirement of Article III.'" *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 733 (2008) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). "[T]he irreducible constitutional minimum of standing contains three elements." *Lujan*, 504 U.S. at 560. These elements are (1) an injury-in-fact that is concrete and actual or imminent, not hypothetical; (2) a fairly traceable causal link between the injury and the defendant's actions; and (3) that the injury will likely be redressed by a favorable decision. *See, e.g.*, *Bennett v. Spear*, 520 U.S. 154, 167 (1997); *Little v. KPMG LLP*, 575 F.3d 533, 540 (5th Cir. 2009).

Defendants maintain that Anibowei's alleged injury is not redressable via the requested remedies because, even if the Directives are vacated, government agents still retain the power to search electronic devices at the border without a warrant because the Directives are not the source of that authority. Rather, defendants contend, it is the "plenary authority of the Federal Government to conduct searches and inspections" at the border that authorizes these searches. Ds. Br. (ECF No. 124) at 13.

To satisfy the redressability prong of standing, the plaintiff must show a "substantial likelihood that the relief requested will redress the injury." *Vt. Agency of*

Nat. Res. v. United States ex rel. Stevens, 529 U.S. 765, 771 (2000) (internal quotation marks and citation omitted). A plaintiff must demonstrate redressability for each form of relief sought. *Friends of the Earth, Inc. v. Laidlaw Env't. Servs. (TOC), Inc.*, 528 U.S. 167, 185 (2000). The plaintiff "need not show that a favorable decision will relieve . . . *every* injury." *Larson v. Valente*, 456 U.S. 228, 243 n.15 (1982). Instead, a "substantial likelihood" that the requested relief will redress the alleged injury is enough. *Duke Power Co. v. Caroline Env't Study Grp., Inc.*, 438 U.S. 59, 79 (1978); *see also Sanchez v. R.G.L.*, 761 F.3d 495, 506 (5th Cir. 2014) (holding that a plaintiff "need only show that a favorable ruling could potentially lessen its injury").

This court frequently holds that the redressability prong is met when plaintiffs plead that agency policies are contrary to law and that their harms could be redressed by setting aside harmful guidance documents. *See, e.g.*, *Nat'l Fed'n of Indep. Bus. v. Dougherty*, 2017 WL 1194666, at *6 (N.D. Tex. Feb. 3, 2017) (Fitzwater, J.); *see also Texas v. Cardona*, 2024 WL 3658767, at *18 (N.D. Tex. Aug. 5, 2024) (O'Connor, J.) (holding that, even if defendants could enforce policies without the challenged guidance documents, a declaration that the guidance documents' interpretation was unlawful and an injunction restraining reliance on that interpretation would reduce the alleged harm).

2

Here, Anibowei pleads three redressable injuries: (1) he is forced to take precautionary measures to avoid unconstitutional border searches, such as leaving his work phone at home when he travels; (2) he is under threat that he will be subject to unconstitutional border searches in the future; and (3) he suffers an ongoing injury from the government's continued retention of the data it downloaded from his cell phone in 2016. Anibowei alleges that the requested relief of vacatur of the policies would lessen his injury by allowing him once again to carry his work phone when he travels, enabling him to travel without the threat of delay or embarrassment from unconstitutional searches, and by increasing the likelihood that the data collected from his phone would be expunged based on the recognition that the data were unlawfully obtained. Because Anibowei plausibly alleges that his injuries would likely be lessened by his requested remedies, he has adequately pleaded a redressable injury.

C

The court now considers defendants' contention that the Directives are not reviewable under the APA because they are not final agency actions.

1

"The APA allows for judicial review only of a 'final agency action[.]'" *Texas v. Equal Emp. Opportunity Comm'n*, 933 F.3d 433, 441 (5th Cir. 2019) (citing 5 U.S.C. § 704) ("*EEOC*"). Two conditions must be satisfied for an agency action to be final: (1) the action "must mark the 'consummation' of the agency's decisionmaking process," and (2) the action "must be one by which 'rights or obligations have been determined,' or from which 'legal consequences will flow.'" *Bennett*, 520 U.S. at 177-78 (citations omitted). "Courts consistently hold that an agency's guidance documents binding it and its staff to a legal position produce legal consequences or determine rights and obligations, thus meeting the second prong of *Bennett*." *EEOC*, 933 F.3d at 441. "'The primary distinction between a substantive rule'—which is, by definition, a final agency action—'and a general statement of policy . . . turns on whether an agency intends to bind *itself* to a particular legal position.'" *Id.* (quoting *Syncor Int'l Corp. v. Shalala*, 127 F.3d 90, 94 (D.C. Cir. 1997)). An action may be binding on an agency itself "if it either appears on its face to be binding[] or is applied by the agency in a way that indicates it is binding[,]" *id.* (alteration in original) (citation omitted), and, in some cases, "the mandatory language of a document alone can be sufficient to render it binding," *id.* at 422 (quoting *Gen. Elec. Co. v. Env't Prot. Agency*, 290 F.3d 377, 383 (D.C. Cir. 2002)). Mandatory language is not strictly required, however—the Supreme Court takes a "pragmatic approach." *Id.* at 441 (citation and internal quotation marks omitted). "[I]f a statement denies the [agency] discretion in the area of its coverage[,] then the statement is binding, and creates rights or obligations." *Id.* at 442 (alterations in original) (quoting *Gen. Elec. Co.*, 290 F.3d at 382).

2

Mandatory language and a pragmatic view of the Directives together indicate that these directives are final agency actions and are binding on their issuing agencies. The 2018 CBP Directive states that it exists "[t]o provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers . . . mobile phones . . . and any other communication, electronic, or digital devices subject to . . . border searches by [CBP].” Ds. App. (ECF No. 125) at 11. This directive contains binding mandatory language, stating that “[a]ll CBP Officers, Border Patrol Agents, . . . and other officials authorized by CBP to perform border searches *shall adhere to the policy described in this Directive* and any implementing policy memoranda[.]” *Id.* (emphasis added). The directive binds itself to its procedures, as is made clear by the statement in the directive that “[t]his directive *governs* border searches of electronic devices[.]” *Id.* at 12 (emphasis added).

The 2009 ICE Directive similarly states that it “provides legal guidance and establishes policy and procedures within [ICE] with regard to border search authority[,]” Ds. App. (ECF No. 125) at 23, and it states that “Special Agents are responsible for complying with the provisions of this Directive[,]” *id.* at 25. The language in these directives indicates that they are intended to be binding on the agencies themselves and their agents and officers in executing border searches of electronic devices.

Defendants point out that the Directives include disclaimers explicitly stating that they do not create any rights or privileges. *See id.* at 22, 32. But when the Directives are assessed pragmatically, it does not appear that these boilerplate statements outweigh the balance of the Directives’ language, which is clearly binding on the agency itself and those acting under its authority. By binding the agencies and their agents and officers to the interpretation of what is required for different types of searches of electronic devices at the border, these directives impact the privacy rights and privileges of individuals at the border who are subject to searches carried out under the authority and instruction of these directives.

D

Finally, the court considers whether the Directives are not reviewable under the APA on the ground that Anibowei has an adequate alternative remedy in a court for his alleged injuries.

1

The APA grants federal courts jurisdiction over "final agency action *for which there is no other adequate remedy in a court*[.]" 5 U.S.C. § 704 (emphasis added). *See also Fort Bend Cnty. v. U.S. Army Corps of Eng'rs*, 59 F.4th 180, 192 (5th Cir. 2023) (characterizing the "adequate remedy" requirement as jurisdictional). "The adequacy of the relief available need not provide an identical review that the APA would provide, so long as the alternative remedy offers the 'same genre' of relief." *Hinojosa v. Horn*, 896 F.3d 305, 310 (5th Cir. 2018) (per curiam) (citation omitted). The requirement that there be no adequate alternative remedy "entails a case-specific evaluation." *Id.* "[A] legal remedy is not inadequate for purposes of the APA because it is procedurally inconvenient for a given plaintiff, or because plaintiffs have inadvertently deprived themselves of the opportunity to pursue that remedy." *Martinez v. Pompeo*, 977 F.3d 457, 460 (5th Cir. 2020) (per curiam) (citation omitted).

2

The court holds that Anibowei has an adequate alternative remedy to his APA challenge because he could allege in a court—indeed, in this court and lawsuit—the constitutional claims that he has already brought but has voluntarily dismissed. Insofar as Anibowei seeks vacatur of the Directives to prevent being subject to warrantless searches of his electronic devices at the border, an injunction against enforcement of those policies pursuant to a constitutional challenge would similarly prevent his being subjected to such searches in the future. Therefore, bringing a constitutional challenge and seeking injunctive relied would, if successful on the merits, provide “the same genre of relief” as vacatur of the Directives pursuant to the APA. *See Hinojosa*, 896 F.3d at 310. The fact that Anibowei has raised and then voluntarily dismissed these claims does not make this remedy inadequate. *See Martinez*, 997 F.3d at 460.

E

Because Anibowei has an adequate alternative remedy, his APA claim is not fit for judicial review. The court lacks subject matter jurisdiction over this claim and therefore grants defendants’ motion to dismiss under Rule 12(b)(1).

IV

Defendants also maintain that Anibowei has failed to state a claim on which relief can be granted. They posit that the Directives do not violate the Fourth or First Amendment under the law of this circuit. The court will consider defendants’ Rule 12(b)(6) motion in the alternative.

A

To state a claim for relief under Rule 12(b)(6), a complaint’s allegations must, “when taken as true, state[] 'a claim to relief that is plausible on its face.'" *Innova Hosp. San Antonio, Ltd. P'ship v. Blue Cross & Blue Shield of Ga., Inc.*, 892 F.3d 719, 726 (5th Cir. 2018) (quoting *Twombly*, 550 U.S. at 570). The Fourth Amendment requires "that searches and seizures be reasonable[,]" and "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537-38 (1985). Historically, "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *United States vs. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

B

In the Fifth Circuit, the government does not need individualized suspicion to conduct a routine manual cell phone search at the border, and nonroutine searches require only reasonable suspicion. *See United States v. Castillo*, 70 F.4th 894, 898 (5th Cir. 2023); *Malik v. U.S. Dep't of Homeland Sec.*, 78 F.4th 191, 200 (5th Cir 2023). Anibowei "recognizes the binding force of *Castillo* and *Malik*" and that this court is bound by them. P. Resp. (ECF No. 127) at 15.[5]

---

[5] Anibowei cites *United States v. Sultanov*, 2024 WL 3520443, at *25 (E.D.N.Y. July 24, 2024), for the proposition that reasonableness under the Fourth Amendment should require probable cause and a warrant because of the First Amendment interests and considerations at stake with a search of electronic devices. Because binding Fifth Circuit precedent does not require

The 2018 CBP Directive requires reasonable suspicion or a national security concern for an advanced search of an electronic device. Ds. App. (ECF No. 125) at 15. Similarly, the 2018 ICE Guidance, which updates the requirements for advanced border searches of electronic devices, instructs agents not to perform advanced border searches of electronic devices without reasonable suspicion. *Id.* at 33-34. Accordingly, to plead a plausible claim for relief, Anibowei cannot rely on an allegation that the Directives' policies—which comply with this circuit's requirements for a border search of an electronic device to be reasonable—violate the Fourth Amendment.

C

Anibowei also alleges that the Directives violate the First Amendment because individuals "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." Compl. ¶ 123. Anibowei cites *United States v. Sultanov*, 2024 WL 3520443 (E.D.N.Y. July 24, 2024),[6] for the proposition that First Amendment considerations are relevant to the determination that a warrant and probable cause were required to search a cell phone at the border, and he cites *Zurcher v. Stanford Daily*, 436 U.S. 547 (1970), for the proposition that the warrant

a warrant and probable cause, and because *Sultanov* is not binding on this court, the court declines to follow *Sultanov*.

[6] *See supra* note 5.

requirement should be administered carefully when "presumptively protected materials are sought to be seized[.]" *Zurcher*, 436 U.S. at 564. Neither of these cases, however, suggests that it is a standalone violation of the First Amendment to search a cell phone at the border without probable cause and a warrant. Instead, both cases consider First Amendment interests to determine what is reasonable under the Fourth Amendment in their respective contexts. In *Sultanov*, which is not binding on this court, the court referred to "First Amendment considerations" in determining that the Fourth Amendment required probable cause and a warrant to search a cell phone at the border. *Sultanov*, 2024 WL3520443, at *24-25. Similarly, the Court in *Zurcher* noted that, outside of the border-search context, "prior cases do no more than insist that the courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search." *Zurcher*, 436 U.S. at 565. It did not, however, suggest that failure to do so would be a standalone violation of the First Amendment.

Absent any binding authority to the contrary, this court holds that a warrantless border search of an electronic device without probable cause does not violate the First Amendment merely because the device may contain expressive or associational content.

D

Because the Directives comply with Fifth Circuit law, Anibowei's allegations, taken as true, do not state a claim for relief that is plausible on its face.

Accordingly, the court holds in the alternative that, assuming *arguendo* that it has jurisdiction over Count VI of Anibowei's second amended complaint, Count VI does not state a claim on which relief can be granted.

* * *

Because this court lacks subject matter jurisdiction over Anibowei's APA claim, and, alternatively, because Anibowei has failed to state a claim for which relief can be granted, the court grants defendants' motion to dismiss Count VI of Anibowei's second amended complaint. The court dismisses this action without prejudice by judgment filed today.[7]

SO ORDERED.

November 22, 2024.

S/ Sidney A. Fitzwater
SIDNEY A. FITZWATER
SENIOR JUDGE

---

[7] This action is being dismissed without prejudice because the dismissal is for lack of subject matter jurisdiction. The dismissal for failure to state a claim is in the alternative and assumes *arguendo* that the court has subject matter jurisdiction.

Filed: March 20, 2026

United States Court of Appeals
for the Fifth Circuit

No. 24-11042

GEORGE ANIBOWEI,

Plaintiff–Appellant,

versus

PAMELA BONDI, *U.S. Attorney General*; UNITED STATES DEPARTMENT OF HOMELAND SECURITY; UNITED STATES CUSTOMS AND BORDER PROTECTION; UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT; KRISTI NOEM, *Secretary, U.S. Department of Homeland Security*; TROY MILLER, *Senior Official Performing the Duties of the Commissioner*, *U.S. Customs and Border Protection*; PATRICK J. LECHLEITNER, *Deputy Director and Senior Official Performing the Duties of the Director for ICE*,

Defendants–Appellees.

Appeal from the United States District Court
for the Northern District of Texas
USDC No. 3:16-CV-3495

ON PETITION FOR REHEARING EN BANC

Before ELROD, *Chief Judge*, CLEMENT, and HAYNES, *Circuit Judges.*

PER CURIAM:

Treating the petition for rehearing en banc as a petition for panel rehearing (5th CIR. R.40 I.O.P.), the petition for panel rehearing is DENIED. Because no member of the panel or judge in regular active service requested that the court be polled on rehearing en banc (FED. R. APP. P.40 and 5TH CIR. R.40), the petition for rehearing en banc is DENIED.

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
ICE Policy System

DISTRIBUTION:	**ICE**
DIRECTIVE NO.:	**7-6.1**
ISSUE DATE:	**August 18, 2009**
EFFECTIVE DATE:	**August 18, 2009**
REVIEW DATE:	**August 18, 2012**
SUPERSEDES:	**See Section 3 Below.**

DIRECTIVE TITLE: BORDER SEARCHES OF ELECTRONIC DEVICES

1. PURPOSE and SCOPE.

1.1. This Directive provides legal guidance and establishes policy and procedures within U.S. Immigration and Customs Enforcement (ICE) with regard to border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border to ensure compliance with customs, immigration, and other laws enforced by ICE. This Directive applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise.

1.2. This Directive applies to border search authority only. Nothing in this Directive limits the authority of ICE Special Agents to act pursuant to other authorities such as a warrant, a search incident to arrest, or a routine inspection of an applicant for admission.

2. **AUTHORITIES/REFERENCES.** 8 U.S.C. § 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; and the December 12, 2008, ICE Office of Investigations (OI) guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices."

3. **SUPERSEDED/CANCELLED POLICY/ SUMMARY OF CHANGES.** ICE Directive No. 7-6.0 entitled "Border Searches of Documents and Electronic Media" is hereby superseded as it relates to electronic devices. Additionally, all other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded as they relate to searches of electronic devices, with the exception of the March 5, 2007, OI guidance entitled "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry" and the December 12, 2008, OI guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media."

4. **BACKGROUND.** ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, Special Agents may review

and analyze computers, disks, hard drives, and other electronic or digital storage devices. These searches are part of ICE's long-standing practice and are essential to enforcing the law at the United States border. Searches of electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

5. DEFINITIONS. The following definitions are provided for the purposes of this Directive:

5.1. Assistance. The use of third party analytic resources such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in electronic devices or in determining the meaning, context, or value of information contained therein.

5.2. Electronic Devices. Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices.

6. POLICY.

6.1. ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth herein. Assistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate.

6.2. When U.S. Customs and Border Protection (CBP) detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.

6.3. Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems.

7. RESPONSIBILITIES.

7.1. The Directors of OI, the Office of Professional Responsibility (OPR), and the Office of International Affairs (OIA) have oversight over the implementation of the provisions of this Directive.

7.2. Special Agents in Charge (SACs) and Attachés are responsible for:

1) Implementing the provisions of this Directive and ensuring that Special Agents in their area of responsibility (AOR) receive a copy of this Directive and are familiar with its contents;
2) Ensuring that Special Agents in their AOR have completed any training programs relevant to border searches of electronic devices, including constitutional, privacy,

civil rights, and civil liberties training related to such searches, as may be required by ICE Headquarters; and

3) Maintaining appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this Directive. (See "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices" memo dated December 12, 2008.)

7.3. Attachés are responsible for ensuring coordination with their host countries, as appropriate, before conducting any such border search outside of the United States.

7.4. When ICE receives electronic devices, or copies of information therefrom, from CBP for analysis and investigation, ICE Special Agents are responsible for advising CBP of the status of any such analysis within 10 calendar days, and periodically thereafter, so that CBP records may be updated as appropriate. For example, "search ongoing"; "completed with negative results"; "returned to traveler"; or "seized as evidence of a crime."

7.5. Special Agents are responsible for complying with the provisions of this Directive, knowing the limits of ICE authority, using this authority judiciously, and ensuring comprehension and completion of any training programs relevant to border searches of electronic devices as may be required by ICE.

8. PROCEDURES.

8.1. Border Searches by ICE Special Agents.

1) Authorization to Conduct Border Search. Border searches of electronic devices must be performed by an ICE Special Agent who meets the definition of "customs officer" under 19 U.S.C. § 1401(i), or another properly authorized officer with border search authority, such as a CBP Officer or Border Patrol Agent, persons cross designated by ICE as customs officers, and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.
2) Knowledge and Presence of the Traveler. To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler. When not practicable due to law enforcement, national security, or other operational concerns, such circumstances are to be noted by the Special Agent in appropriate ICE systems. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement techniques or potentially compromise other operational concerns, the individual will not be permitted to observe the search.
3) Consent Not Needed. At no point during a border search of electronic devices is it necessary to ask the traveler for consent to search.
4) Continuation of the Border Search. At any point during a border search, electronic

devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location, including a location associated with a demand for assistance from an outside agency or entity (see Section 8.4).

5) Originals. In the event electronic devices are detained, the Special Agent should consider whether it is appropriate to copy the information therefrom and return the device. When appropriate, given the facts and circumstances of the matter, any such device should be returned to the traveler as soon as practicable. Consultation with the Office of the Chief Counsel is recommended when determining whether to retain a device in an administrative immigration proceeding. Devices will be returned to the traveler as expeditiously as possible at the conclusion of a negative border search.

8.2. Chain of Custody.

1) Detentions of electronic devices. Whenever ICE detains electronic devices, or copies of information therefrom, the Special Agent will initiate the correct chain of custody form or other appropriate documentation.

2) Seizures of electronic devices for criminal purposes. Whenever ICE seizes electronic devices, or copies of information therefrom, the Special Agent is to enter the seizure into the appropriate ICE systems. Additionally, the seizing agent must complete the correct chain of custody form or other appropriate documentation.

3) Retention of electronic devices for administrative immigration purposes. Whenever ICE retains electronic devices, or copies of information therefrom, or portions thereof, for administrative immigration purposes pursuant to 8 U.S.C. § 1357, the Special Agent is to record such retention in appropriate ICE systems and is to include the location of the retained files, a summary thereof, and the purpose for retention.
4) Notice to traveler. Whenever ICE detains, seizes, or retains original electronic devices, the Special Agent is to provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation.

8.3. Duration of Border Search.

1) Special Agents are to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search. Searches are generally to be completed within 30 calendar days of the date of detention, unless circumstances exist that warrant more time. Such circumstances must be documented in the appropriate ICE systems. Any detention exceeding 30 calendar days must be approved by a Group Supervisor or equivalent, and approved again every 15 calendar days thereafter, and the specific justification for additional time documented in the appropriate ICE systems.
2) Special Agents seeking assistance from other Federal agencies or non-Federal entities are responsible for ensuring that the

results of the assistance are received in a reasonable time (see Section 8.4(5)).

3) In determining “reasonable time,” courts have reviewed the elapsed time between the detention and the completion of the border search, taking into account any additional facts and circumstances unique to the case. As such, ICE Special Agents are to document the progress of their searches, for devices and copies of information therefrom, and should consider the following factors:
   a) The amount of information needing review;
   b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;
   c) Whether assistance was sought and the type of such assistance;
   d) Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;
   e) Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and
   f) Any unanticipated exigency that may arise.

8.4. Assistance by Other Federal Agencies and Non-Federal Entities.

1) Translation, Decryption, and Other Technical Assistance.
   a) During a border search, Special Agents may encounter information in electronic devices that presents technical difficulties, is in a foreign language, and/or encrypted. To assist ICE in conducting a border search or in determining the meaning of such information, Special Agents may demand translation, decryption, and/or technical assistance from other Federal agencies or non-Federal entities.
   b) Special Agents may demand such assistance absent individualized suspicion.
   c) Special Agents shall document such demands in appropriate ICE systems.
2) Subject Matter Assistance.
   a) During a border search, Special Agents may encounter information in electronic devices that are not in a foreign language or encrypted, or that do not require other technical assistance, in accordance with Section 8.4(1), but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by ICE. For the purpose of obtaining such subject matter expertise, Special Agents may

create and transmit a copy of such information to other Federal agencies or non-Federal entities.

b) Special Agents may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by ICE.

c) Special Agents shall document such demands in appropriate ICE systems.

3) Demand Letter. Unless otherwise governed by a Memorandum of Understanding or similar mechanism, each demand for assistance is to be in writing (e.g., letter or email), approved by a supervisor, and documented in the appropriate ICE systems. Demands are to detail the context of the search requested, ICE's legal parameters regarding the search, retention, and sharing of any information found during the assistance, and relevant timeframes, including those described in this Directive.

4) Originals. For the purpose of obtaining subject matter assistance, Special Agents may create and transmit copies of information to other Federal agencies or non-Federal entities. Original electronic devices should be transmitted only when necessary to render the demanded assistance.

5) Time for Assistance and Responses Required.

a) Assistance is to be accomplished within a reasonable period of time in order to preserve the status of the electronic devices and the integrity of the border search.

b) It is the responsibility of the Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities and to act in accord with section 8.3 of this Directive. In addition, Special Agents shall:

   i) Inform assisting agencies or entities that they are to provide results of assistance as expeditiously as possible;

   ii) Ensure that assisting agencies and entities are aware that responses to ICE must include any findings, observations, and conclusions drawn from their review that may relate to the laws enforced by ICE;

   iii) Contact the assisting agency or entity to get a status report on the demand within the first 30 calendar days;

   iv) Remain in communication with the assisting agency or entity until results are received;

   v) Document all communications and actions in appropriate ICE systems; and

   vi) Consult with a supervisor to determine appropriate action if the timeliness of results is a concern. If a demand for assistance is revoked, the Special Agent is to ensure all electronic devices are returned to ICE as expeditiously as possible.

8.5. Retention, Sharing, Safeguarding, And Destruction.

1) By ICE

a) Seizure and Retention with Probable Cause. When Special Agents determine there is probable cause of unlawful activity-based on a review of information in electronic devices or on other facts and circumstances-they may seize and retain the electronic device or copies of information therefrom, or relevant portions thereof, as authorized by law.

b) Retention of Information in ICE Systems. To the extent authorized by law, ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained. For example, information entered into TECS during the course of an investigation will be retained consistent with the policies governing TECS.

c) Sharing. Copies of information from electronic devices, or portions thereof, which are retained in accordance with this section, may be shared by ICE with Federal, state, local, and foreign law enforcement agencies in accordance with applicable law and policy. Sharing must be in compliance with the Privacy Act and applicable ICE privacy policies, such as the ICE Search, Arrest, and Seizure System of Records Notice.

d) <u>Safeguarding Data During Storage and Transmission</u>. ICE will appropriately safeguard information detained, copied, retained, or seized under this directive while in ICE custody and during transmission to an outside entity. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking originals and copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic data or physical protections (e.g., locked containers). Any suspected loss or compromise of information that contains personal data detained, copied, or seized under this directive must be reported immediately to the ICE Service Desk.

e) <u>Destruction</u>. Copies of information from electronic devices, or portions thereof, determined to be of no relevance to ICE will be destroyed in accordance with ICE policy governing the particular form of information. Such destruction must be accomplished by the responsible Special Agent within seven business days after conclusion of the border search unless circumstances require additional time, which must be approved by a supervisor and documented in appropriate ICE systems. All destructions must be accomplished no later than 21 calendar days after conclusion of the border search.

2) By Assisting Agencies

   a) Retention during Assistance. All electronic devices, whether originals or copies of information therefrom, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to ICE.

   b) Return or Destruction. At the conclusion of the requested assistance, all electronic devices and data must be returned to ICE as expeditiously as possible. In the alternative, the assisting Federal agency may certify to ICE that any copies in its possession have been destroyed or it may advise ICE in accordance with Section 8.5(2)(c). In the event that any original electronic devices were transmitted, they must not be destroyed; they are to be returned to ICE.

   c) Retention with Independent Authority. Copies may be retained by an assisting Federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information is of national security or intelligence value. In such cases, the retaining agency must advise ICE of its decision to retain certain information on its own authority. In the event that any original electronic devices were transmitted, the assisting Federal agency may make a copy of information therefrom for its retention; however, any originals must be returned to ICE.

3) By Non-Federal Entities

a) ICE may provide copies of information from electronic devices to an assisting non-Federal entity, such as a private language translation or data decryption service, only for the period of time needed by that entity to render the requested assistance.

b) Upon the completion of assistance, all copies of the information in the possession of the entity must be returned to ICE as expeditiously as possible. Any latent copies of the electronic data on the systems of the non-Federal entity must also be destroyed so that recovery of the data is impractical.

8.6. Review, Handling, and Sharing of Certain Types of Information.

1) Border Search. All electronic devices crossing U.S. borders are subject to border search; a claim of privilege or personal information does not prevent the search of a traveler's information at the border. However, the nature of certain types of information are subject to special handling by Special Agents, whether through policy or laws such as the Privacy Act and the Trade Secrets Act.

2) <u>Types of Information</u>
   a) <u>Business or Commercial Information</u>. If, in the course of a border search, Special Agents encounter business or commercial information, such information is to be treated as business confidential information. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may specifically govern or restrict handling of the information, including criminal penalties for unauthorized disclosure.
   b) <u>Legal Information</u>. Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.
   c) <u>Other Sensitive Information</u>. Other possibly sensitive information, such as medical records and work-related information carried by journalists shall be handled in accordance with all

applicable federal law and ICE policy. Although there is no Federal legal privilege pertaining to the doctor-patient relationship, the inherent nature of medical information warrants special care for such records. Questions regarding the review of these materials shall be directed to the ICE Office of the Chief Counsel and this consultation shall be noted in appropriate ICE systems.

3) Sharing. Information that is determined to be protected by law as privileged or sensitive is to be handled consistent with the laws and policies governing such information.

8.7. Measurement. ICE Headquarters will develop appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from ICE systems using data elements entered by Special Agents pursuant to this Directive.

8.8. Audit. ICE Headquarters will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

9. ATTACHMENTS. None.

10. NO PRIVATE RIGHT STATEMENT. This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees; or any other person.

Approved s/ John Morton
John Morton
Assistant Secretary
U.S. Immigration and Customs
Enforcement

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049

DATE: August 20, 2009

ORIGINATING OFFICE: FO:TO
SUPERSEDES:
REVIEW DATE: August 2012

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION

1 **PURPOSE.** To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices, encountered by U.S. Customs and Border Protection (CBP) at the border, both inbound and outbound, to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce.

These searches are part of CBP's long-standing practice and are essential to enforcing the law at the U.S. border. Searches of electronic devices help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations. Finally, searches at the border are often integral to a determination of admissibility under the immigration laws.

2 POLICY.

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air Interdiction Agents, Marine Interdiction Agents, and other employees authorized by law to perform searches at the border, the functional equivalent of the border (FEB), or the extended border shall adhere to the policy described in this Directive.

2.3 This Directive governs border search authority only. It does not limit CBP's authority to conduct other lawful searches at the border, e.g., pursuant to a warrant, consent, or incident to an arrest; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., a shipment of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede Restrictions on Importation of Seditious Matter, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede Processing Foreign Diplomatic and Consular Officials, Directive 3340-032. Diplomatic and consular officials encountered at the border, the FEB, or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), ICE Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.

3 DEFINITIONS.

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air Interdiction Agent, Marine Interdiction Agent, Internal Affairs Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Includes any devices that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

3.4 Border Search of Information. Excludes actions taken to determine if a device functions (e.g., turning an electronic device on and off), or actions taken to determine if contraband is concealed within the device itself. The definition also excludes the review of information voluntarily provided by an individual in an electronic format (for example, when an individual voluntarily shows an e-ticket on an electronic device to an Officer).

4 AUTHORITY/REFERENCES. 8 U.S.C. 1225, 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

5 PROCEDURES.

5.1 Border Searches.

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. 507).

5.1.2 In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.3 Searches of electronic devices will be documented in appropriate CBP systems of records and should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire search, or where a supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.4 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material.

5.2.1 Officers may encounter materials that appear to be legal in nature, or an individual may assert that certain information is protected by attorney-client or attorney work product privilege. Legal materials are not necessarily exempt from a border search, but they may be subject to the following special handling procedures: If an Officer suspects that the content of such a material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the Officer must seek advice from the CBP Associate/Assistant Chief Counsel before conducting a search of the material, and this consultation shall be noted in appropriate CBP systems of records. CBP counsel will coordinate with the U.S. Attorney's Office as appropriate.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel, and this consultation shall be noted in appropriate CBP systems of records.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with federal agencies that have mechanisms in place to protect appropriately such information.

5.3 Detention and Review in Continuation of Border Search of Information

5.3.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days.

5.3.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director, Patrol Agent in Charge, or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems of records.

5.3.1.2 Destruction. Except as noted in section 5.4 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.3, there is not probable cause to seize it, any copies of the information must be destroyed, and any electronic device must be returned. Upon this determination that there is no value to the information copied from the device, the copy of the information is 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 of records and which must be no later than twenty one (21) days after such determination. The destruction shall be noted in appropriate CBP systems of records.

5.3.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, and when the fact of conducting this search can be disclosed to the individual transporting the device without hampering national security or law enforcement or other operational considerations, the individual may be notified of the purpose and authority for these types of searches, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search.

5.3.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.3.2 Assistance by Other Federal Agencies.

5.3.2.1 The use of other federal agency analytical resources outside of CBP and ICE, such as translation, decryption, and subject matter expertise, may be needed to assist CBP in reviewing the information contained in electronic devices or to determine the meaning, context, or value of information contained in electronic devices.

5.3.2.2 Technical Assistance – With or Without Reasonable Suspicion. Officers may sometimes have technical difficulties in conducting the search of electronic devices such that technical assistance is needed to continue the border search. Also, in some cases Officers may encounter information in electronic devices that requires technical assistance to determine the meaning of such information, such as, for example, information that is in a foreign language and/or encrypted (including information that is password protected or otherwise not readily reviewable). In such situations, Officers may transmit electronic devices or copies of information contained therein to seek technical assistance from other federal agencies. Officers may seek such assistance with or without individualized suspicion.

5.3.2.3 Subject Matter Assistance by Other Federal Agencies – With Reasonable Suspicion. In addition to encountering information in electronic devices that is in a foreign language, encrypted, or requires technical assistance, Officers may encounter information that requires referral to subject matter experts in other federal agencies to determine the meaning, context, or value of information contained therein as it relates to the laws enforced and administered by CBP. Therefore, Officers may transmit electronic devices or copies of information contained therein to other federal agencies for the purpose of obtaining subject matter assistance when they have reasonable suspicion of activities in violation of the laws enforced by CBP. While many factors may result in reasonable suspicion, the presence of an individual on a government-operated and government-vetted terrorist watch list will be sufficient to create reasonable suspicion of activities in violation of the laws enforced by CBP.

5.3.2.4 Approvals for seeking translation, decryption, and subject matter assistance. Requests for translation, decryption, and subject matter assistance require supervisory approval and shall be properly documented and recorded in CBP systems of records.

If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.3.2.5 Electronic devices should be transmitted only when necessary to render the requested translation, decryption, or subject matter assistance. Otherwise, a copy of such information should be transmitted in lieu of the device in accord with this Directive.

5.3.2.6 When information from an electronic device is transmitted to another federal agency for translation, decryption, or subject matter assistance, the individual will be notified of this transmission unless CBP determines, in consultation with the receiving agency or other agency as appropriate, that notification would be contrary to national security or law enforcement or other operational interests. If CBP's transmittal seeks assistance regarding possible terrorism, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the transmittal or his or her presence on a watch list. When notification is made to the individual, the Officer will annotate the notification in CBP systems of records and on the Form 6051D.

5.3.3 Responses and Time for Assistance

5.3.3.1 Responses Required. Agencies receiving a request for assistance in conducting a border search are to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced by CBP.

5.3.3.2 Time for Assistance. Responses from assisting agencies are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager, responses from an assisting agency should be received within fifteen (15) days. If the assisting agency is unable to respond in that period of time, the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager may permit extensions in increments of seven (7) days.

5.3.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance being provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency to return to CBP all electronic devices that had been provided to the assisting agency, and any copies thereof, as expeditiously as possible, except as noted in 5.4.2.3. Any such revocation shall be documented in appropriate CBP systems of records. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency pursuant to the procedures outlined in this Directive.

5.3.3.4 Destruction. Except as noted in section 5.4.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the information does not exist, CBP will retain no copies of the information.

5.4 Retention and Sharing of Information Found in Border Searches

5.4.1 Retention and Sharing of Information Found in Border Searches

5.4.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents thereof, contains evidence of or is the fruit of a crime that CBP is authorized to enforce.

5.4.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. For example, information collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or ENFORCE or other systems as may be appropriate and consistent with the policies governing such systems.

5.4.1.3 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.

5.4.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is mandated by statute, Presidential Directive, or OHS policy. Consistent with 6 U.S.C. 122(d)(2) and other applicable law and policy, CBP, as a component of OHS, will promptly share any terrorism information encountered in the course of a border search with elements of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the element receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.4.1.5 Safeguarding Data During Storage and Transmission. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during transmission to another federal agency. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during transmission such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the Port Director, Patrol Agent in Charge or equivalent level manager and the CBP Office of Internal Affairs.

5.4.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.4.2 Retention by Agencies Providing Translation, Decryption, or Subject Matter Assistance

5.4.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting federal agency may be retained by that agency for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.4.2.3 below.

5.4.2.2 Return or Destruction. At the conclusion of the requested assistance, all information must be returned to CBP as expeditiously as possible, and the assisting agency must advise CBP in accordance with section 5.3.3 above. In addition, the assisting federal agency should destroy all copies of the information transferred to that agency unless section 5.4.2.3 below applies. In the event that any electronic devices are transmitted, they must not be destroyed; they are to be returned to CBP unless seized by the assisting agency based on probable cause or retained per 5.4.2.3.

5.4.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency shall assume responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so-for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.5 Reporting Requirements

5.5.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.5.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.3.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.5.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.6 Management Requirements

5.6.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.6.2 The appropriate CBP Second line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.6.3 The appropriate CBP Second line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another federal agency.

5.6.4 The Director, Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of information contained therein in order to ensure compliance with the procedures outlined in this Directive.

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S.

Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 DISCLOSURE. This Directive may be shared with the public.

10. SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008) to the extent they pertain to electronic devices.

s/ Jayson P. Ahern
Acting Commissioner
U.S. Customs and Border Protection

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049A

DATE: January 4, 2018
ORIGINATING OFFICE: FO:TO
SUPERSEDES: Directive 3340-049
REVIEW DATE: January 2021

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES

1 PURPOSE. To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. They can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws.

2 POLICY

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

2.3 This Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of this Directive, this excludes actions taken to determine if a device functions (e.g., turning a device on and off); or actions taken to determine if physical contraband is concealed within the device itself; or the review of information voluntarily provided by an individual in an electronic format (e.g., when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). This Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., an importation of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the functional equivalent of the border (FEB), or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

3 DEFINITIONS

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Special Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Any 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.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-0SC.

4 AUTHORITY/REFERENCES. 6 U.S.C. §§ 122, 202, 211; 8 U.S.C. §§ 1225, 1357, and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF605 l), Directive 5240-005.

The plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty. "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."' *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). "Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Additionally, the authority to conduct border searches extends not only to persons and merchandise entering the United States, but applies equally to those departing the country. *See, e.g.*, *United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Odutayo*, 406 F.3d 386, 391-92 (5th Cir. 2005); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995); *United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991); *United States v. Cardona*, 769 F.2d 625,629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983).

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. *See Flores-Montano*, 541 U.S. at 154 (noting that "the expectation of privacy is less at the border than it is in the interior"). Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign. *See Boumelhem*, 339 F.3d at 423.

In addition to longstanding federal court precedent recognizing the constitutional authority of the U.S. government to conduct border searches, numerous federal statutes and regulations also authorize CBP to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property, such as electronic devices. *See, e.g.*, 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a; *see also* 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer."). These authorities support CBP's enforcement and administration of federal law at the border and facilitate the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department. This includes, among other things, the responsibility to "ensure the interdiction of persons and goods illegally entering or exiting the United States"; "detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States"; "safeguard the borders of the United States to protect against the entry of dangerous goods"; "enforce and administer all immigration laws"; "deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband"; and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons." 6 U.S.C. § 211.

CBP must conduct border searches of electronic devices in accordance with statutory and regulatory authorities and applicable judicial precedent. CBP's broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

5 PROCEDURES

5.1 Border Searches

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. § 507).

5.1.2 Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

5.1.3 Basic Search. Any border search of an electronic device that is not an advanced search, as described below, may be referred to as a basic search. In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.4 Advanced Search. An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents. In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device.

Many 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.

5.1.5 Searches of electronic devices will be documented in appropriate CBP systems, and advanced searches should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire advanced search, or where supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.6 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to remain present during a search does not necessarily mean that the individual shall observe the search itself. If permitting an individual to observe the search could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material

5.2.1 Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.

5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP Associate/Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

5.2.1.3 At the completion of the CBP review, unless any materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained in coordination with the CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel office, and this consultation shall be noted in appropriate CBP systems.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel office or the CBP Privacy Officer, as appropriate.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect appropriately such information, and such information will only be shared in accordance with this Directive.

5.3 Review and Handling of Passcode-Protected or Encrypted Information

5.3.1 Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents. Passcodes or other means of access may be requested and retained as needed to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on the device that is being inspected or has been detained, seized, or retained in accordance with this Directive.

5.3.2 Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

5.3.3 If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.

5.3.4 Nothing in this Directive limits CBP's ability, with respect to any device presented in a manner that is not readily accessible for inspection, to seek technical assistance, or to use external equipment or take other reasonable measures, or in consultation with the CBP Associate/Assistant Chief Counsel office to pursue available legal remedies, to render a device in a condition that allows for inspection of the device and its contents.

5.4 Detention and Review in Continuation of Border Search of Information

5.4.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days. Devices must be presented in a manner that allows CBP to inspect their contents. Any device not presented in such a manner may be subject to exclusion, detention, seizure, or other appropriate action or disposition.

5.4.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems.

5.4.1.2 Destruction. Except as noted in section 5.5 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.4, there is no probable cause to seize the device or the information contained therein, any copies of the information held by CBP must be destroyed, and any electronic device must be returned. 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. The destruction shall be noted in appropriate CBP systems.

5.4.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, the individual subject to search will be notified of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. If the Officer or other appropriate CBP official determines that the fact of conducting this search cannot be disclosed to the individual transporting the device without impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld.

5.4.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.4.2 Assistance

Officers may request assistance that may be needed to access and search an electronic device and the information stored therein. Except with respect to assistance sought within CBP or from ICE, the following subsections of 5.4.2 govern requests for assistance.

5.4.2.1 Technical Assistance. Officers may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection. For example, Officers may encounter a device or information that is not readily accessible for inspection due to encryption or password protection. Officers may also require translation assistance to inspect information that is in a foreign language. In such situations, Officers may convey electronic devices or copies of information contained therein to seek technical assistance.

5.4.2.2 Subject Matter Assistance – With Reasonable Suspicion or National Security Concern. Officers may encounter information that requires referral to subject matter experts to determine the meaning, context, or value of information contained therein as it relates to the laws enforced or administered by CBP. Therefore, Officers may convey electronic devices or copies of information contained therein for the purpose of obtaining subject matter assistance when there is a national security concern or they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP.

5.4.2.3 Approvals for Seeking Assistance. Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.4.2.4 Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of data from the device should be conveyed in lieu of the device in accordance with this Directive.

5.4.2.5 When an electronic device or information contained therein is conveyed for assistance, the individual subject to search will be notified of the conveyance unless the Officer or other appropriate CBP official determines, in consultation with the receiving agency or other entity as appropriate, that notification would impair national security, law enforcement, officer safety, or other operational interests. If CBP seeks assistance for counterterrorism purposes, if a relevant national security-related lookout applies, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the conveyance, the existence of a relevant national security-related lookout, or his or her presence on a watch list.

When notification is made to the individual, the Officer will annotate the notification in CBP systems and on the Form 6051D.

5.4.3 Responses and Time for Assistance

5.4.3.1 Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are expected to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced or administered by CBP.

5.4.3.2 Time for Assistance. Responses from assisting agencies or entities are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager, responses should be received within fifteen (15) days. If the assisting agency or entity is unable to respond in that period of time, the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager may permit extensions in increments of seven (7) days.

5.4.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency or entity to return to CBP all electronic devices provided, and any copies thereof, as expeditiously as possible, except as noted in 5.5.2.3. Any such revocation shall be documented in appropriate CBP systems. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency or entity pursuant to the procedures outlined in this Directive.

5.4.3.4 Destruction. Except as noted in section 5.5.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the device or the information from the device does not exist, CBP will retain no copies of the information.

5.5 Retention and Sharing of Information Found in Border Searches

5.5.1 Retention and Sharing of Information Found in Border Searches

5.5.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer.

5.5.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice. For example, information collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or E3 or other systems as may be appropriate and consistent with the policies governing such systems.

5.5.1.3 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.

5.5.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is authorized by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. § 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with entities of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the entity receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.5.1.5 Safeguarding Data During Storage and Conveyance. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during conveyance. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during conveyance such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the CBP Office of Professional Responsibility and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

5.5.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.5.2 Retention by Agencies or Entities Providing Technical or Subject Matter Assistance

5.5.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting agency or entity may be retained for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.5.2.3 below.

5.5.2.2 Return or Destruction. CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible, and that the assisting agency or entity advise CBP in accordance with section 5.4.3 above. In addition, the assisting agency or entity should destroy all copies of the information conveyed unless section 5.5.2.3 below applies. In the event that any electronic devices are conveyed, they must not be destroyed; they are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.2.3.

5.5.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency assumes responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.6 Reporting Requirements

5.6.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.6.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.4.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.6.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.7 Management Requirements

5.7.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.7.2 The appropriate CBP second-line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.7.3 The appropriate CBP second-line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another agency or entity.

5.7.4 The Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of information contained therein in order to ensure compliance with the procedures outlined in this Directive.

5.7.5 Officers will ensure, in coordination with field management as appropriate, that upon receipt of any subpoena or other request for testimony or information regarding the border search of an electronic device in any litigation or proceeding, notification is made to the appropriate CBP Associate/Assistant Chief Counsel office.

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 REVIEW. This Directive shall be reviewed and updated, as necessary, at least every three years.

10 DISCLOSURE. This Directive may be shared with the public.

11 SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008), to the extent they pertain to electronic devices; CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).

s/ Kevin K. McAleenan
Acting Commissioner

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]

---

[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.

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.

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]

---

[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,

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 course of a border search, with or without

---

2017), https://venturebeat.com/2017/06/13/5-billion-people-now-have-a-mobile-phone-connection-according-to-gsma-data/.

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

---

[4] U.S. Customs and Border Protection, Border Search of Electronic Devices Containing In-formation, 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).

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 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 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.

---

[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).

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.

---

[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.

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 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

---

[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.

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).

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 combi-nation 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 essential 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.

---

[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).

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 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

---

[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.

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.

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 uninhibited 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 reasonable 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

165. 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: *<u>/s/ Andrew Tutt</u>*
Andrew Tutt

* * * * *

Counsel for Plaintiff