RECORD NUMBER: 16-4687

United States Court of Appeals

for the

Fourth Circuit

UNITED STATES OF AMERICA,

Plaintiff/Appellee,

– v. –

HAMZA KOLSUZ,

Defendant/Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA AT ALEXANDRIA

BRIEF OF *AMICI CURIAE* CAUSE OF ACTION INSTITUTE, THE COMMITTEE FOR JUSTICE AND FLOOR64, INC. IN SUPPORT OF APPELLANT HAMZA KOLSUZ

CURT LEVEY
THE COMMITTEE FOR JUSTICE
722 12th Street N.W.
4th Floor
Washington, D.C. 20005
(202) 270-7748
clevey@committeeforjustice.org

Counsel for The Committee for Justice

ERICA L. MARSHALL
CAUSE OF ACTION INSTITUTE
1875 Eye Street N.W.
Suite 800
Washington, D.C. 20006
(202) 499-4231
erica.marshall@causeofaction.org

Counsel of Record for Amici Curiae Cause of Action Institute, The Committee for Justice, and Floor64, Inc.

COUNSEL PRESS • VA – (800) 275-0668

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 16-4687 Caption: United States v. Kolsuz

Pursuant to FRAP 26.1 and Local Rule 26.1,

Cause of Action Institute
(name of party/amicus)

who is Amicus Curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☐ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: Erica J. [illegible] Date: March 20, 2017

Counsel for: Cause of Action Institute

CERTIFICATE OF SERVICE

****

I certify that on March 20, 2017 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

Erica J. [illegible]
(signature)

March 20, 2017
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 16-4687 Caption: United States v. Kolsuz

Pursuant to FRAP 26.1 and Local Rule 26.1,

The Committee for Justice
(name of party/amicus)

who is Amicus Curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☐ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: Eric J. [signature] Date: March 20, 2017

Counsel for: The Committee for Justice

CERTIFICATE OF SERVICE

****

I certify that on March 20, 2017 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

Eric J. [signature]
(signature)

March 20, 2017
(date)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 16-4687 Caption: United States v. Kolsuz

Pursuant to FRAP 26.1 and Local Rule 26.1,

Floor64, Inc.
(name of party/amicus)

who is Amicus Curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☐ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: Erin J. Date: March 20, 2017

Counsel for: Floor64, Inc.

CERTIFICATE OF SERVICE

****

I certify that on March 20, 2017 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

Erin J.
(signature)

March 20, 2017
(date)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes & Other Authorities:

AMICI CURIAE BRIEF OF CAUSE OF ACTION INSTITUTE, THE COMMITTEE FOR JUSTICE AND FLOOR64, INC. IN SUPPORT OF APPELLANT HAMZA KOLSUZ

Pursuant to Fed. R. of App. P. 29, Cause of Action Institute ("CoA Institute" or "CoA") respectfully files this *Amicus Curiae* brief in support of the position argued by Appellant Hamza Kolsuz. CoA Institute submits this brief with the consent of all parties.[1]

STATEMENT OF INTEREST

CoA is a nonprofit, nonpartisan government oversight organization that uses investigative, legal, and communications tools to educate the public on how government accountability, transparency, and the rule of law work together to protect liberty and economic opportunity. As part of this mission, CoA works to expose and prevent government and agency misuse of power by, *inter alia*, appearing as *Amicus Curiae* before this and other federal courts. *E.g.*, *McCutcheon v. Fed. Election Comm'n*, 134 S. Ct. 1434, 1460 (2014) (citing brief). CoA has a particular interest in opposing governmental overreach and curbing governmental abuses by the executive branch that infringe individual rights. CoA routinely represents clients to challenge agency action that violates the United States

[1] Counsel of Record, Erica L. Marshall, who authored this brief, formerly served as counsel to Defendant Hamza Kolsuz before the United States District Court for the Eastern District of Virginia but does not represent the Defendant on appeal; no party or party's counsel contributed money intended to fund the brief's preparation or submission; and no person other than CoA Institute contributed money intended to fund the brief's preparation or submission.

Constitution, the separation of powers doctrine, federal laws, and existing judicial precedent.

Founded in 2002, the Committee for Justice ("CFJ") is a nonprofit, nonpartisan organization dedicated to promoting the rule of law and enforcing the Constitution's limits on the federal government, including the Constitution's enumeration of federal powers and its protection of individual liberty. Central to this mission is the robust enforcement of the Bill of Rights, including the First and Fourth Amendment rights at stake in this case. CFJ advances its mission by supporting constitutionalist nominees to the federal judiciary, filing *amicus curiae* briefs in key cases, analyzing judicial decisions with respect to the rule of law, and educating government officials and the American people about the Constitution and the proper role of the courts.

Floor64 Inc. is a corporation that publishes the online news site, Techdirt.com. Techdirt's journalists regularly report on issues around technology, policy and law that involve numerous sources, whom they often need to keep confidential. Techdirt also frequently posts documents and text for analysis, and often carefully handles such documents to keep information secure and private. The site depends on the ability to protect its sources and to protect private information to continue to do its reporting.

BACKGROUND

On February 2, 2016, Defendant Hamza Kolsuz attempted to board a plane at Dulles International Airport to depart the United States bound for Istanbul, Turkey. J.A. at 89–90. A customs inspection performed by United States Department of Homeland Security ("DHS") Customs and Border Patrol ("CBP") officers revealed handgun parts contained in his checked luggage. J.A. at 89–90. Mr. Kolsuz was questioned and then arrested at the airport. J.A. at 93. Pursuant to that arrest, DHS officers seized Mr. Kolsuz's iPhone 6 Plus, a cellular mobile smartphone that Mr. Kolsuz was carrying on his person. J.A. at 93.

Following Mr. Kolsuz's arrest, on February 3, 2016, Homeland Security Special Agent ("SA") Adam Coppolo transported, among other things, Mr. Kolsuz's mobile phone to a Homeland Security office located in Sterling, Virginia. J.A. at 93. SA Coppolo then requested the assistance of Computer Forensic Agent ("CFA") Michael Del Vacchio in extracting information from Mr. Kolsuz's iPhone. J.A. at 93. From February 3, 2016 through March 3, 2016, CFA Del Vacchio completed a technology-assisted, warrantless, forensic search of the iPhone. J.A. at 93–94. Specifically, CFA Del Vacchio utilized a Cellebrite Physical Analyzer to conduct an "advanced logical file system extraction" on the phone. J.A. at 93. According to the law enforcement Report on Investigation, the purpose of the search was to find

evidence relating to violations of "Title 22 United States Code Section 2778 and Title 18 United States Code Section 554." J.A. at 94.

The forensic search ultimately generated an 896-page report setting forth the information and data contained on the mobile phone. J.A. at 94. The report details Mr. Kolsuz's internet-browsing history, text messages, "Kik" application messages, emails, previous GPS coordinates, calendar appointments dating years into the future, and contains photographs recounting Mr. Kolsuz's travels and the details of his daily life. J.A. at 94.

The United States obtained an indictment against Defendant Hamza Kolsuz on March 2, 2016, for three counts arising out of an alleged attempt to transport handgun parts from the United States to Turkey in violation of the Arms Export Control Act, 22 U.S.C. § 2778, the smuggling act, 18 U.S.C. § 554, and for conspiracy to commit those offenses, 18 U.S.C. § 371. J.A. at 14. On March 30, 2016, Mr. Kolsuz filed a Motion to Suppress Evidence obtained through the warrantless search of his smartphone. J.A. at 27. The United States District Court for the Eastern District of Virginia, Judge T.S. Ellis, III, presiding, denied Defendant's Motion to Suppress in a Memorandum Opinion dated April 29, 2016. J.A. at 190.

During a two-day bench trial, the United States introduced evidence against Mr. Kolsuz that it obtained from the warrantless search. J.A. at 223–24, 236–37.

Specifically, the United States introduced transcripts of text messages and "Kik" application messages contained on Mr. Kolsuz's mobile phone. After the trial, by order dated July 7, 2016, the District Court found Mr. Kolsuz guilty of all three counts. J.A. at 11. At the sentencing hearing held on October 7, 2016, the government dismissed Count III, and the District Court sentenced Mr. Kolsuz to thirty months on Counts I and II, to run concurrently. J.A. at 262–64. Mr. Kolsuz timely filed a Notice of Appeal on October 21, 2016.

SUMMARY OF ARGUMENT

The District Court erred in denying Mr. Kolsuz's Motion to Suppress and this Court should reverse and remand for a new trial. First, while the border search doctrine constitutes a narrow exception to the otherwise unequivocal Fourth Amendment requirement that the government obtain a warrant to conduct a search, the governmental interests that justify this narrow border search exception were not in play when the Defendant's smartphone was searched incident to his arrest, and this exception therefore cannot be used to justify the search here. The fact that Mr. Kolsuz was arrested and his phone seized at an airport—the equivalent of a border—does not change this case from one that fits squarely within *Riley v. California*, 134 S. Ct. 2473 (2014), to one that is suddenly part of a narrow exception of cases justified by the sovereign's customs enforcement interests.

The Court should see this search for what it was: a month-long, detailed, forensic search to gather evidence against Mr. Kolsuz for use in a trial on the very charges for which he was arrested. Since the search here was not actually a border search, the border search exception cannot save it.

Second, the United States essentially seeks a mechanical application of a Fourth Amendment exception even where the interests that justify the exception were not implicated in this case. The dangers of such a mechanical application are readily apparent. People traveling into and out of the United States routinely cross with smartphones or computers that contain the equivalent of "every piece of mail . . . every picture . . . [and] every book" a person has. *Id.* at 2489. These individuals include journalists, lawyers, and business travelers with confidential information typically safeguarded under American jurisprudence. Nevertheless, customs agents purport to have unfettered access to the contents of electronic devices carried by such individuals, without any reasonable suspicion or probable cause of a crime, simply by the fact that the individual wishes to leave or enter the United States. This is not the application of the border search exception that the Supreme Court had in mind when it outlined its narrow purview.

The privacy interests, Fourth Amendment, and First Amendment rights at stake are simply too high for the Court to apply a perfunctory analysis here. Accordingly, even if the Court finds that the search of the Defendant's smartphone

was a border search, it should nonetheless hold that a search of an electronic device can only properly be conducted with a warrant based on probable cause. For this reason, *amici curiae* respectfully request that the Court reverse the District Court's order denying Defendant's Motion to Dismiss.

ARGUMENT

I. The Search Was Not a Border Search, Was Not Subject to the Border Search Exception, and the Fourth Amendment Warrant Requirement Therefore Applies.

A. The Government Was Not Vindicating the Interests of the Border Search Exception When It Conducted the Search of Mr. Kolsuz's Smartphone.

The "touchstone of the Fourth Amendment is 'reasonableness.'" *Riley*, 134 S. Ct. at 2482 (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). When the government performs a warrantless search, it is *per se* unreasonable, unless the government can demonstrate that the search fits into a specific exception to the warrant requirement. *United States v. Cervantes*, 703 F.3d 1135, 1141 (9th Cir. 2012). Here, the United States seeks to justify its warrantless search under the border search doctrine, an exception to the Fourth Amendment's otherwise unequivocal warrant requirement. However, at the time of the search, from February 3, 2016, through March 3, 2016, neither Mr. Kolsuz nor his smartphone were crossing the United States border.

Mr. Kolsuz was arrested in the early morning hours of February 3, 2016, before the search of his smartphone began. As of his arrest, the smartphone was also in U.S. custody, and was not being analyzed for passage out of the country during its search. *Cf. United States v. Cotterman*, 709 F.3d 952, 956–59 (9th Cir. 2013) (CBP agents released defendant for entry into the United States but detained his laptop for a search to determine its eligibility for admission).

In fact, the United States obtained an Indictment against Mr. Kolsuz for export violations on March 2, 2016, before it even concluded the search of his smartphone on March 3, 2016. To this effect, the government Report of Investigation states very clearly that the government searched the smartphone to retrieve "evidence" related to export violations under "Title 22 United States Code Section 2778 and Title 18 United States Code Section 554." J.A. at 94 ("On March 3, 2016, SA Coppolo confirmed with CFA Del Vacchio that no other information could be obtained from the phone. . . . SA Coppolo will no longer search the report for new *evidence*. SA Coppolo will only access the report in an attempt to review the *evidence* that has already been reviewed.") (emphasis added); *see Ferguson v. City of Charleston*, 532 U.S. 67, 81–83 (2001) (holding that the scope of a warrant exception is determined, in part, by whether the generation of evidence is the primary purpose of the search).

For a search to be valid under the Fourth Amendment, it must be "'strictly tied to and justified by' the circumstances which rendered its initiation permissible."

Terry v. Ohio, 392 U.S. 1, 19 (1968) (quoting *Warden v. Hayden*, 387 U.S. 294, 310 (1967) (Fortas, J., concurring)); *see Chimel v. California*, 395 U.S. 752, 762 (1969), *abrogated on other grounds by Davis v. United States*, 564 U.S. 229 (2011); *see also Cupp v. Murphy*, 412 U.S. 291, 295 (1973). Moreover, in determining whether to grant an exception to the warrant requirement, courts must consider the facts and circumstances of each search and seizure, focusing on the reasons supporting the exception rather than on any bright-line rule of general application. *See Sibron v. New York*, 392 U.S. 40, 59 (1968); *Preston v. United States*, 376 U.S. 364, 367 (1964).

To this effect, warrant exceptions must be narrowly construed in light of their original justification. *Arizona v. Gant*, 556 U.S. 332, 343, 345–46 (2009). The border search exception recognizes the "long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country," *United States v. Ramsey*, 431 U.S. 606, 616 (1977), in order to keep out unwanted persons and effects, and to "'regulate the collection of duties and to prevent the introduction of contraband into the country.'" *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004) (citation omitted). Searches upon exit from the country also have been justified for their ability to control currency and regulate foreign commerce. *See United States v. Oriakhi*, 57 F.3d 1290, 1297 (4th Cir. 1995)

(noting the sovereign's interest in "regulating foreign commerce and, in particular, in regulating and controlling its currency").

However, the government cannot justify a warrantless search under a mechanical application of an exception, where such an application would "untether the rule from the justifications underlying" it. *Gant*, 556 U.S. at 343 (holding that the Fourth Amendment exception allowing officers to search a car incident to defendant's arrest in order to protect the officer could not be justified where defendant was already detained and officer safety was not in jeopardy); *see Knowles v. Iowa*, 525 U.S. 113, 119 (1998) (declining to extend the search-incident-to-arrest exception to a situation similar to an arrest but where "the concern for officer safety is not present to the same extent and the concern for destruction or loss of evidence is not present at all"); *see also Riley*, 134 S. Ct. at 2484 (refusing a "mechanical application" of the "search incident to arrest" exception).

Here, the only thing tethering this smartphone search to the border search doctrine at all is the fact that Mr. Kolsuz's arrest, and the seizure of his phone, occurred at an airport. However, the proximity to a border, alone, does not justify a warrantless search when that search was carried out in furtherance of general law enforcement, rather than customs and border, authority. *See Ramsey*, 431 U.S. at 616 (differentiating the "plenary customs powers" stemming from the "long-

standing right of the sovereign to protect itself" from "the more limited power to enter and search" places or objects, which requires a warrant).

At the time of the search, neither Mr. Kolsuz nor his smartphone were in the process of crossing any border. The Government was not furthering any interest in prohibiting the entry or exit of contraband, enforcing currency control, levying duties or tariffs, or excluding travelers without the property documentation to enter the country. *See Flores-Montano*, 541 U.S. at 149; *United States v. Djibo*, 151 F. Supp. 3d 297, 299 (E.D.N.Y. 2015) (suppressing evidence from defendant's cellphone that was seized after his arrest at the border, holding that, at that point, the customs agent could no longer look into the cellphone without a warrant).

B. The Government's Conduct Demonstrates that It Seized the Smartphone Pursuant to Mr. Kolsuz's Arrest, Not Pursuant to Its Border Search Authority.

While Congress "'has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country,'" *Flores-Montano*, 541 U.S. at 153 (citation omitted), no such express authority exists specifically for electronic devices. Namely, statutes provide customs officers with authority to prescribe regulations for the search of "persons and baggage," 19 U.S.C. § 1582, and the authority to "examine, inspect, and search" a "vessel or vehicle" within a customs-enforcement area. *Id.* § 1581.

But no customs statute grants customs officers any explicit authority to search electronic devices.

DHS has promulgated regulations implementing these Congressional statutory grants. *See, e.g.*, 19 C.F.R. § 162.6 (permitting the search of "persons, baggage, and merchandise" arriving in "the customs territory of the United States"); *Id.* § 162.7 (authorizing customs officers to "stop, search, and examine any vehicle, person, or beast, or search any trunk or envelope"). However, even these agency-promulgated regulations fail to expressly mention electronic devices. And none of these statutes or regulations bridge the topic of whether a social media account, or digital data stored on a cloud supported by a remote server, constitute the type of "baggage" or "merchandise" that CBP is authorized to search upon entrance into "the customs territory of the United States." *See id.* § 162.6.

Nevertheless, with neither an express statutory grant, nor any regulatory authority, DHS has essentially used the judicially-created border search exception to publish policy statements providing legal-loophole "guidance" to customs officials purporting to authorize them to conduct warrantless border searches "of information contained in documents and electronic devices." *See* U.S. Customs & Border Prot., Policy Regarding Border Search of Information (July 16, 2008), *available at* http://bit.ly/2m6tdgP; *see also* U.S. Immigration & Customs Enf't, Border Searches of Electronic Devices (Aug. 18, 2009), *available at* http://bit.ly/2neVFgf. The

government has even created a sheet that it presents to individuals at the border to justify the review of their social media accounts, email, call logs, and any other information stored on the phone. U.S. Customs & Border Prot., Inspection of Electronic Devices, Pub. No. 0204-0709, *available at* http://bit.ly/2m6htur. It states:

> You're receiving this sheet because your electronic device(s) has been detained for further examination, which may include copying. You will receive a written receipt (Form 6051-D) that details what item(s) are being detained, who at CBP will be your point of contact, and the contact information (including telephone number) you provide to facilitate the return of your property within a reasonable time upon completion of the examination.

Id.

DHS's electronic device search policies essentially turn the border search doctrine on its head and make it the *rule*, rather than the *exception*. The policy is in direct contravention of the Supreme Court's "fundamental principle of Fourth Amendment analysis that exceptions to the warrant requirement are to be narrowly construed." *New York v. Belton*, 453 U.S. 454, 464 (1981) (Brennan, J., dissenting) (citing *Arkansas v. Sanders*, 442 U.S. 753, 759–60 (1979); *Mincey v. Arizona*, 437 U.S. 385, 393–94 (1978); *Coolidge v. New Hampshire*, 403 U.S. 443, 454–55 (1971); *Vale v. Louisiana*, 399 U.S. 30, 34 (1970); *Katz v. United States*, 389 U.S. 347, 357 (1967); *Jones v. United States*, 357 U.S. 493, 499 (1958)), *abrogated on other grounds by Davis v. United States*, 564 U.S. 229 (2011). And it violates the

Fourth Amendment's purpose of "shield[ing] the citizen from unwarranted intrusions into his privacy." *Jones v. United States*, 357 U.S. 493, 498 (1958).

Moreover, DHS's policies currently allow these agencies to *share* the downloaded information with other law enforcement agencies to "assist" in their review. *See* U.S. Customs & Border Prot., Policy Regarding Border Search of Information; *see also* U.S. Immigration & Customs Enf't, Border Searches of Electronic Devices (stating that "[t]his directive provides legal guidance and establishes policy and procedures within . . . ICE . . . to search, detain, seize, retain, and *share* information contained in law electronic devices possessed by individuals at the border") (emphasis added).

Those agencies are allowed to retain the information indefinitely if they find it has "national security or intelligence value." U.S. Customs & Border Prot., Policy Regarding Border Search of Information. These other law enforcement agencies may have no customs authority whatsoever, and would not ever be entitled to obtain the information without a warrant, but are nonetheless supplied the fruits of a warrantless search. This just simply is not the type of narrow exception that the Supreme Court envisioned when it created the border search exception, and this court should find that the search of Mr. Kolsuz's phone is no more justified by the border search exception than the fishing expeditions encouraged by CBP policy. *See United States v. Kim*, 103 F. Supp. 3d 32, 46 (D.D.C. 2015) (finding the search

unconstitutional and stating that "[w]ith respect to [Mr. Kim's] ongoing activity, the search was nothing more than a fishing expedition to discover what Kim might have been up to[.]").

Notwithstanding the problematic implications of the DHS policy, this policy statement and a related publication draw a clear distinction between DHS border search authority and its other policing authority—the authority actually being exercised by the government here.[2]

If DHS had executed this search under its border search authority, the government's arguments that *Riley* does not displace the border search exception *may* carry more weight. But they fail here, where the government's assertion of border search authority came as a *post hoc* rationalization offered in Agent Coppolo's Report of Investigation, completed after Mr. Kolsuz was indicted.

[2] Congress also delegated to customs officers general policing authority. 19 U.S.C. § 1589a (stating that any "officer of the customs may . . . make an arrest without a warrant for any offense against the United States committed in the officer's presence or for a felony . . . committed outside the officer's presence"). CBP's 2008 policy statement pertaining to searches for information at the border expressly states that "[t]his policy governs border search authority only; nothing in this policy limits the authority of CBP to act pursuant to other authorities such as a warrant or a search incident to arrest." U.S. Customs & Border Prot., Policy Regarding Border Search of Information.

C. The District Court's Analysis Pertaining to Reasonable Suspicion is Inapposite as this Search Cannot Be Analyzed as a Border Search.

The District Court's Memorandum Opinion below made a cursory finding that the search did constitute a border search, and went on to spend the bulk of the decision determining whether the border search was reasonable given the highly-invasive nature of the forensic search. *United States v. Kolsuz*, 185 F. Supp. 3d 843 (E.D. Va. 2016). Ultimately, applying reasoning similar to the Ninth Circuit in *Cotterman*, the lower court found that the border search, while "non-routine," was ultimately reasonable because it was performed with reasonable suspicion. *Id*.

Since the search here cannot be justified or analyzed as a border search at all, the analysis in *Cotterman*, 709 F.3d at 952, regarding whether an invasive border search requires reasonable suspicion, and the District Court's memorandum opinion finding reasonable suspicion to justify the search, *Kolsuz*, 185 F. Supp. 3d at 843, are inapposite.[3] Moreover, *Cotterman* is not binding authority on this Court and is unpersuasive, as the government in *Cotterman* was actually analyzing Mr. Cotterman's laptop for entry into the United States after having let Mr. Cotterman pass into the country, and because the agents there had reasonable suspicion that the

[3] As noted below, even if the Court affirms the lower court's finding that the search was a border search, it contradicts existing Supreme Court authority to hold that mere reasonable suspicion could nevertheless justify such an invasive search. *Riley*, 134 S. Ct. at 2489–90 (recognizing the heightened privacy interests in smartphones).

device contained (as the agents ultimately discovered) electronic contraband in the form of child pornography (as distinguished from the search here for evidence of crime already committed). 709 F.3d at 957–59.

D. Traditional Fourth Amendment Jurisprudence Applies, Including the *Riley v. California* Warrant Requirement.

Since this search was not a border search under existing law, the reasonableness of the search must be analyzed under traditional Fourth Amendment jurisprudence. The search of Mr. Kolsuz's smartphone occurred incident to his arrest, placing it squarely within the analysis provided in *Riley v. California*.

In *Riley*, the Supreme Court unanimously established the rule that, absent exigent circumstances not relevant here, the government cannot search digital information on a cellphone seized incident to arrest without a warrant. *Riley*, 134 S. Ct. at 2495 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."). The government failed to heed this directive and cannot be allowed to use the fruits of this illegal search.

II. The Privacy Interests At Stake Outweigh the Mechanical Application of the Border Search Exception.

Even if this Court finds that the search of Mr. Kolsuz's iPhone was a border search, which it should not, the inquiry does not end there. The District Court erroneously held that the forensic search of the smartphone was justified by the

reasonable suspicion that Mr. Kolsuz had committed a crime. The district court's opinion fails to fully appreciate the magnitude of the Supreme Court's unanimous ruling that electronic devices must be entitled to the highest Fourth Amendment protections. *Id.* at 2483.

Given the privacy interests inherent in modern technology, the court should find that a warrant based on probable cause, not just reasonable suspicion, should be required to perform the type of non-routine, invasive search that the government conducted here.

A. The Privacy Interests in Electronic Devices are So High that Any Search of an Electronic Device is Non-Routine.

Courts determine whether to exempt a certain type of search from the warrant requirement "'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *Id. at* 2484 (citing *Wyoming* v. *Houghton*, 526 U. S. 295, 300 (1999)). Even assuming that the search here furthered the governmental interests underlying the border search doctrine (which it did not), the Supreme Court has recognized that smartphones contain so much information as to represent the zenith of individual privacy interests, containing "[t]he sum of an individual's private life." *Id*. at 2489. Indeed, even the lower court recognized that "the Supreme Court's decision in *Riley* appears to indicate that cell phones deserve

the highest level of Fourth Amendment protection available[.]" *Kolsuz*, 185 F. Supp. 3d at 859 (E.D. Va. 2016).

The heightened privacy interest in electronic devices has been recognized by courts around the country, with the Second Circuit noting that privacy interests "have become more susceptible to deprivation in the computer age" as digital devices contain "the quantity of information found in a person's residence, or greater." *United States v. Ganias*, 824 F.3d 199, 231 (2d Cir. 2016) (citing *Riley*, 134 S. Ct. at 2489), *cert. denied*, 137 S. Ct. 569 (2016).

Moreover, electronic devices now represent such a commonplace tool that modern business would be unable to function without them. This cannot be understated for *amici curiae* journalists and legal organizations, who rely on smartphones, tablets, and laptops more than ever in a 24-hour news and work cycle powered by the internet and other digital technology.

In an era of rapid change, "no enterprise has been more convulsed by these technologies than the business of journalism." Peter M. Shane, *The Future of Online Journalism: News, Community, and Democracy in the Digital Age*, 8 I/S: J.L. & Pol'y for the Info. Soc'y 469 (2013). Journalists rely on electronic devices to communicate with sources around the world, store research and contact information, draft and publish news articles, and film or photograph live events, and upload stories to social media. Similarly, lawyers routinely utilize laptops and smartphones

as repositories of attorney-client communications and work product documents. And businesses need such devices to perform proprietary work, transmit documents detailing trade secrets, and remotely access company information.

B. The Privacy Interests of Journalists, Lawyers, and Business Travelers in Digital Devices at the Border Warrant Consideration Here.

The courts have carefully crafted legal balancing tests that recognize the need to protect certain information, like journalist sources, attorney-client privileged information, and confidential trade secrets, by allowing the government to access such privileged information only when certain compelling justifications exist. In this regard, the current DHS "policy" purporting to allow the agency unfettered access to information at the border does not only contravene the privacy rights of individuals as defined under Fourth Amendment jurisprudence, but also disrupts other carefully-created judicial safeguards that protect the information of businesses, journalists, and lawyers' clients, from disclosure.

1. The DHS Policy Violates Judicially-Recognized First Amendment Interests.

The fundamental importance of the press to a democratic society is "recognized by specific reference to the press in the text of the [First] Amendment and by the precedents of [the Supreme] Court." *Saxbe v. Wash. Post Co.*, 417 U.S. 843, 863 (1974). The press serves this "crucial function" by providing "the means by which the people receive that free flow of information and ideas essential to

intelligent self-government." *Id.* Policies that endanger that free flow of information therefore endanger that type of self-government.

The need to guard against such policies has been recognized by statutes and regulations that not only protect the media from undue constraints but grant it certain privileges in accessing public information, such as a categorical fee reduction, 5 U.S.C. § 552(a)(4)(A)(ii)(II), and the ability to request certain records on an expedited basis. *Id.* § 552(a)(6)(E)(v)(II).

No piece of information exists in a vacuum, and journalists must often keep details, such as sources, confidential in order to fulfill their constitutional role to disseminate information to the public. The courts have recognized the press's need to maintain confidential sources and allow journalists to avoid turning over confidential information even to the courts so long as they meet a three-part test established in *Branzburg v. Hayes*, 408 U.S. 665, 739–40 (1972) (Stewart, J., dissenting), and applied by this Court. *See, e.g.*, *LaRouche v. Nat'l Broad. Co.*, 780 F.2d 1134, 1139 (4th Cir. 1986). Before it can access a journalist's information, the government must "'convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest,'" 408 U.S. at 739 (citation omitted), "demonstrate that the information sought is clearly relevant to a precisely defined subject of governmental inquiry," *id.* at 740, and

show that there is "not [a] means of obtaining the information less destructive of First Amendment liberties." *Id.*

This standard demonstrates the longstanding recognition of a unique and privileged interest in privacy for journalists. Such longstanding and detailed protections should not be rendered irrelevant because a journalist crosses a border, particularly given the importance of travel to fulfilling their duties. *See Zemel v. Rusk*, 381 U.S. 1, 28 (1965) (stating that travel by journalists is often how they obtain "information necessary to the making of informed decisions" by the public); *see also N.Y. Times Co. v. Jascalevich*, 439 U.S. 1331, 1334–35 (1978) (refusing to grant judges the unfettered right to access journalist files, even for *in camera* review, saying that "forced disclosure . . . will have a deleterious effect on the ability of the news media effectively to gather information in the public interest").

2. The DHS Policy Endangers the Attorney-Client Privilege.

The attorney-client privilege is the "oldest of the privileges for confidential communications known to the common law." *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). This privilege precludes any third party, including the government, from accessing communications between attorneys and their clients "'at all stages of actions, cases, and proceedings.'" *United States v. Zolin*, 491 U.S. 554, 565–66 (citing Fed. R. Evid. 1101(c)). Even to gain access to information *excluded* from the privilege under the crime-fraud exception, the government must present

independently admissible evidence proving that the crime fraud exception applies, *id.* at 556, or seek *in camera* review that is only available if the government demonstrates "a factual basis adequate to support a good faith belief by a reasonable person that *in camera* review of the materials may reveal evidence to establish the claim that the crime-fraud exception applies." *Id.* at 572 (internal citation omitted). This standard is meant to prevent "opponents of the privilege [from] engag[ing] in groundless fishing expeditions, with the district courts as their unwitting (and perhaps unwilling) agents." *Id.* at 571.

3. The DHS Policy Threatens Judicially-Recognized Protections for Business Information.

Finally, courts have recognized the need to protect confidential business trade secrets for over a century. *See Ruckelshaus v. Monsanto*, 467 U.S. 986, 1002–04 (1984) (recognizing that, in most states, trade secrets are treated as property and are thus protected by the Takings Clause and discussing authorities dating back to 1911). To receive such information, even pursuant to subpoena, the government bears the burden of showing a "substantial need for the testimony or material that cannot be otherwise met without undue hardship and assures that the person to whom the subpoena is addressed will be reasonably compensated." *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 684 (N.D. Cal. 2006) (applying Fed. R. Civ. P. 45(c)(3)(B), which allows a party to quash a subpoena seeking information about a trade secret, and denying the government's request that Google produce its users' search inquiries).

It is simply impossible to justify DHS's sweeping "policy" purporting to grant it unrestricted access to such information in light of these judicially-recognized protections, especially on such an amorphous and unparticularized assertion of governmental interest in enforcing customs laws.

C. The Border Search Exception Is Being Used as a Legal Loophole that Violates the Constitution and Injures American Interests.

These concerns are not merely illusory. Numerous news reports have detailed the unfortunate encounters between business travelers, journalists, and even government employees with customs agents purporting to exercise their "authority" to perform warrantless fishing expeditions at the border.

In this regard, as discussed above, DHS has used its policy on border searches, for years, as a legal loophole purporting to allow customs officers unfettered access to electronic records without so much as reasonable suspicion of any criminal activity.[4] In recent years, these searches have only grown more common, increasing fivefold in 2016. Cynthia McFadden, E.D. Cauchi, William M. Arkin, *American Citizens: U.S. Border Agents Can Search Your Cellphone*, NBC News, Mar. 13,

[4] In this regard, current CBP policy appears to contradict the state of the law in the Ninth Circuit, *see Cotterman*, 709 F.3d at 952 (holding that "exhaustive forensic searches" of electronic devices at the border may only be performed where the government has, at a minimum, reasonable suspicion of criminal activity), as well as the law set forth in a number of district court opinions finding that technology-assisted, forensic searches of electronic devices, are non-routine and thus require, at a minimum, reasonable suspicion.

2017, http://nbcnews.to/2mA0xJ2 (reporting that DHS searches of cellphones have grown fivefold in just one year, from fewer than 5,000 in 2015 to nearly 25,000 in 2016 and stating that, according to DHS officials, "five-thousand devices were searched in February [2017] alone, more than in all of 2015").

On February 14, 2017, *The New York Times* reported an incident involving Haisam Elsharkawi, an American citizen who was detained at the Los Angeles airport while traveling to Saudi Arabia. Daniel Victor, *What Are Your Rights if Border Agents Want to Search Your Phone?*, N.Y. Times, Feb. 14, http://nyti.ms/2mU6fZ1. According to the report, CBP agents "repeatedly pressured him to unlock his cellphone so that they could scroll through his contacts, photos, apps, and social media accounts." *Id*.

On January 30, 2017, Sidd Bikkannavar, an American citizen and National Aeronautics and Space Administration ("NASA") scientist, landed in Houston after vacationing in Chile. *See* Loren Grush, *A US-born NASA scientist was detained at the border until he unlocked his phone*, The Verge, Feb. 12, 2017, http://bit.ly/2nsrSRC. CBP agents pressured him to turnover his cellphone and access PIN even after Mr. Bikkannavar explained that the phone was NASA-issued and contained sensitive information about NASA's Jet Propulsion Laboratory. *Id*. When Mr. Bikkannavar finally provided the PIN, the CBP officer "left with the device and didn't return for another 30 minutes." *Id*.

Similar encounters have been reported by journalists seeking to cross into or out of the United States, even where the journalists explained that their mobile device contained confidential sources. A Canadian photojournalist, Ed Ou, was detained while attempting to enter the United States to cover a story on behalf of the Canadian Broadcast Corporation. *See* Andrea Peterson, *U.S. border agents stopped journalist from entry and took his phones*, Wash. Post, Nov. 30, 2016, http://wapo.st/2nstMBD. According to Mr. Ou, although he refused to unlock his mobile phones for CBP officers, "explaining that he had an ethical obligation to protect his reporting sources," the agents seized his electronic devices and removed them from the room where Mr. Ou was being detained, and when the phones were returned hours later, "it was clear that someone had tampered with the SIM cards and potentially made copies of data on the devices." *Id.*; *see also* Mazin Sidahmed, *Department of Homeland Security detains journalist returning from Beirut*, The Guardian, July 21, 2016, http://bit.ly/2n3U5NC (referencing an incident involving a Wall Street Journal reporter, Maria Abi-Habib, who was asked to turn over her mobile phones); Committee to Protect Journalists, Alerts, *BBC journalist questioned by US border agents, devices searched*, Feb. 1, 2017, http://bit.ly/2m6qWlO (discussing CBP's search of a BBC journalist, Ali Hamedani's, cellphone, computer and Twitter feed while he was detained in Chicago O'Hare airport).

The inevitable results of these warrantless searches have been a rise in encryption, using so-called "burner" devices, traveling with access to minimal information, or not traveling at all. *See* Andy Greenberg, *A guide to getting past customs with your digital privacy intact*, Wired, Feb. 12, 2017, http://bit.ly/2mz7Q3J). All of these are significant impediments, prompting at least two major global corporations to instruct employees simply not to travel to the United States with confidential business material. Ellen Nakashima, *Clarity Sought on Electronic Searches*, Wash. Post, Feb. 7, 2008, http://wapo.st/2nshZDl.

The privacy interests inherent in electronic devices are so high as to require a minimum of probable cause to justify their search. Any less protection will continue to chill First Amendment protections, harm business interests, and violate the Fourth Amendment rights of Americans to be free from unreasonable search and seizure.

D. A Warrant Requirement for Any Search of an Electronic Device Would Allow CBP to perform their Duties while Preserving Constitutional Safeguards.

Given the ease by which law enforcement officers can obtain warrants today, *Missouri v. McNeely*, 133 S. Ct. 1552, 1561–62 (2013), and the advanced notice that law enforcement has about many incoming and outgoing travelers from United

States airports,[5] such a requirement would have no practical effect on the ability of customs agents to enforce customs laws and keep America safe.

This is particularly true given the government's ability to detain the electronic devices (as they do now) while seeking a warrant. There would be little to no practical effect on custom agents' ability to enforce border laws, levy duties and tariffs, and prohibit the entry or exit of illegal contraband. A warrant requirement would balance the need of customs agents to search electronic devices while preserving the constitutional rights of all Americans.

[5] Under federal regulations, flights and airlines arriving from or departing to a destination outside the United States must electronically transmit the "traveler manifest information for each person on board" to CBP no less than sixty minutes prior to takeoff. *See* Fed. Aviation Admin., Advance Passenger Information System ("APIS"), *available at* http://bit.ly/2mNUgKA.

CONCLUSION

For these reasons, the Court should reverse the lower court's Order denying Mr. Kolsuz's Motion to Suppress and order a new trial.

Respectfully submitted,

Cause of Action Institute

Dated: March 20, 2017

By: /s/ Erica L. Marshall

Erica L. Marshall
Cause of Action Institute
1875 Eye Street N.W.
Suite 800
Washington, D.C. 20006
(202) 499-4231
erica.marshall@causeofaction.org

Counsel of Record for Amici Curiae Cause of Action Institute, Committee for Justice, and Floor64, Inc.

/s/ Curt Levey

Curt Levey
The Committee for Justice
722 12th Street N.W.
4th Floor
Washington, D.C. 20005
(202) 270-7748
clevey@committeeforjustice.org

Counsel for The Committee for Justice

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
Effective 12/01/2016

No. 16-4687 **Caption:** US v. Hamza Kolsuz

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT

Type-Volume Limit, Typeface Requirements, and Type-Style Requirements

Type-Volume Limit for Briefs: Appellant's Opening Brief, Appellee's Response Brief, and Appellant's Response/Reply Brief may not exceed 13,000 words or 1,300 lines. Appellee's Opening/Response Brief may not exceed 15,300 words or 1,500 lines. A Reply or Amicus Brief may not exceed 6,500 words or 650 lines. Amicus Brief in support of an Opening/Response Brief may not exceed 7,650 words. Amicus Brief filed during consideration of petition for rehearing may not exceed 2,600 words. Counsel may rely on the word or line count of the word processing program used to prepare the document. The word-processing program must be set to include headings, footnotes, and quotes in the count. Line count is used only with monospaced type. See Fed. R. App. P. 28.1(e), 29(a)(5), 32(a)(7)(B) & 32(f).

Type-Volume Limit for Other Documents if Produced Using a Computer: Petition for permission to appeal and a motion or response thereto may not exceed 5,200 words. Reply to a motion may not exceed 2,600 words. Petition for writ of mandamus or prohibition or other extraordinary writ may not exceed 7,800 words. Petition for rehearing or rehearing en banc may not exceed 3,900 words. Fed. R. App. P. 5(c)(1), 21(d), 27(d)(2), 35(b)(2) & 40(b)(1).

Typeface and Type Style Requirements: A proportionally spaced typeface (such as Times New Roman) must include serifs and must be 14-point or larger. A monospaced typeface (such as Courier New) must be 12-point or larger (at least 10½ characters per inch). Fed. R. App. P. 32(a)(5), 32(a)(6).

This brief or other document complies with type-volume limits because, excluding the parts of the document exempted by Fed. R. App. R. 32(f) (cover page, disclosure statement, table of contents, table of citations, statement regarding oral argument, signature block, certificates of counsel, addendum, attachments):

☑ this brief or other document contains 6,497 [*state number of*] words

☐ this brief uses monospaced type and contains _____ [*state number of*] lines

This brief or other document complies with the typeface and type style requirements because:

☑ this brief or other document has been prepared in a proportionally spaced typeface using
MS Word 2016 [*identify word processing program*] in
14pt Times New Roman [*identify font size and type style*]; **or**

☐ this brief or other document has been prepared in a monospaced typeface using
_____ [*identify word processing program*] in
_____ [*identify font size and type style*].

(s) Erica L. Marshall

Party Name Cause of Action Institute, et al.

Dated: 3/20/2017

CERTIFICATE OF SERVICE

I certify that on 3/20/2017 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

U. S. DEPARTMENT OF JUSTICE
Heather Nicole Alpino
600 E Street, NW Washington DC 20004
202-514-0620
heather.alpino@usdoj.gov

U. S. DEPARTMENT OF JUSTICE
Jeffrey Michael Smith
950 Pennsylvania Avenue, N.W. Room 6500 Washington DC 20530
202-532-0220
Jeffrey.Smith5@usdoj.gov

OFFICE OF THE FEDERAL PUBLIC DEFENDER
Geremy C. Kamens
1650 King Street Suite 500 Alexandria VA 22314-0000
703-600-0800
geremy_kamens@fd.org

OFFICE OF THE FEDERAL PUBLIC DEFENDER
Todd M. Richman
1650 King Street Suite 500 Alexandria VA 22314-0000
703-600-0800
Todd_Richman@fd.org

/s/ Erica L. Marshall
Signature

3/20/2017
Date