

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

GHASSAN ALASAAD, NADIA ALASAAD,
SUHAIB ALLABABIDI, SIDD BIKKANAVAR,
JÉRÉMIE DUPIN, AARON GACH, ISMAIL
ABDEL-RASOUL AKA ISMA'IL KUSHKUSH,
DIANE MAYE, ZAINAB MERCHANT,
MOHAMMED AKRAM SHIBLY, AND
MATTHEW WRIGHT,

Plaintiffs,

v.

KIRSTJEN NIELSEN, SECRETARY OF THE U.S.
DEPARTMENT OF HOMELAND SECURITY, IN
HER OFFICIAL CAPACITY; KEVIN
MCALEENAN, ACTING COMMISSIONER OF
U.S. CUSTOMS AND BORDER PROTECTION,
IN HIS OFFICIAL CAPACITY; AND THOMAS
HOMAN, ACTING DIRECTOR OF U.S.
IMMIGRATION AND CUSTOMS
ENFORCEMENT, IN HIS OFFICIAL CAPACITY,

Defendants.

No. 17 Civ. 11730 (DJC)

**BRIEF OF THE KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA
UNIVERSITY AND THE REPORTERS COMMITTEE FOR FREEDOM OF THE
PRESS AS *AMICI CURIAE* SUPPORTING PLAINTIFFS**

Jonathan M. Albano
BBO #013850
jonathan.albano@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
One Federal Street
Boston, MA 02110-1726
Telephone: (617) 341-7700
Facsimile: (617) 341-7701

Scott B. Wilkens (*pro hac vice* forthcoming)
Michael E. Stewart (*pro hac vice*
forthcoming)
JENNER & BLOCK LLP
1099 New York Ave., NW, Suite 900
Washington, DC 20001
Telephone: (202) 639-6000
Facsimile: (202) 639-6066

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
INTEREST OF AMICI CURIAE.....	1
SUMMARY OF ARGUMENT	2
ARGUMENT	3
I. Government Searches Of Electronic Devices At The Border Burden Core First Amendment Freedoms.....	3
A. Government Searches Of Electronic Devices At The Border Burden Travelers’ Freedoms Of Speech And Association.....	4
B. Government Searches Of Electronic Devices At The Border Burden Freedom Of The Press.	6
1. Suspicionless Searches Chill Reporter-Source Communications....	7
2. Journalists Are Particularly Likely To Be The Targets Of Suspicionless Border Searches.	8
II. Suspicionless Searches Of Electronic Devices At The Border Violate The First Amendment.....	10
A. The Government’s Electronic Device Searches Must Be Evaluated Independently Under The First Amendment.	11
B. Suspicionless Searches Of Electronic Devices At The Border Fail First Amendment Scrutiny.	14
III. The First Amendment Implications Of Electronic Device Searches At The Border Require Scrupulous Adherence To The Fourth Amendment Warrant Requirement.....	18
CONCLUSION.....	20

TABLE OF AUTHORITIES

CASES

<i>Baird v. State Bar of Arizona</i> , 401 U.S. 1 (1971)	15
<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	18
<i>City of Lakewood v. Plain Dealer Publishing Co.</i> , 486 U.S. 750 (1988)	17
<i>Cutting v. City of Portland</i> , 802 F.3d 79 (1st Cir. 2015)	16
<i>Entick v. Carrington</i> , 19 How. St. Tr. 1029 (C.P. 1765)	18
<i>Heller v. New York</i> , 413 U.S. 483 (1973)	12, 19
<i>Marcus v. Search Warrants</i> , 367 U.S. 717 (1961)	18
<i>McIntyre v. Ohio Elections Commission</i> , 514 U.S. 334 (1995)	15, 16
<i>NAACP v. Alabama ex rel. Patterson</i> , 357 U.S. 449 (1958)	15
<i>New York v. P.J. Video, Inc.</i> , 475 U.S. 868 (1986)	12
<i>Perry Education Ass’n v. Perry Local Educators’ Ass’n</i> , 460 U.S. 37 (1983)	16, 17
<i>In re Request from the United Kingdom Pursuant to the Treaty between the Government of the United States & the Government of the United Kingdom on Mutual Assistance in Criminal Matters in the Matter of Dolours Price</i> , 718 F.3d 13 (1st Cir. 2013)	16
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	<i>passim</i>
<i>Roaden v. Kentucky</i> , 413 U.S. 496 (1973)	12, 19
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	3, 18, 19
<i>Tabbaa v. Chertoff</i> , 509 F.3d 89 (2d Cir. 2007)	11
<i>United States v. Ickes</i> , 393 F.3d 501 (4th Cir. 2005)	12, 14
<i>United States v. Ramsey</i> , 431 U.S. 606 (1977)	<i>passim</i>
<i>United States v. Seljan</i> , 547 F.3d 993 (9th Cir. 2008)	14
<i>Ward v. Rock Against Racism</i> , 491 U.S. 781 (1989)	16
<i>Wilkes v. Wood</i> , 19 How. St. Tr. 1153 (C.P. 1763)	18
<i>Zerilli v. Smith</i> , 656 F.2d 705 (D.C. Cir. 1981)	16

Zurcher v. Stanford Daily, 436 U.S. 547 (1978)3, 18, 19

OTHER AUTHORITIES

CBP, Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049 (Aug. 20, 2009).....3

CBP, Border Search of Electronic Devices, CBP Directive No. 3340-049A (Jan. 4, 2018)3, 9

Comments of 30 Organizations and 16 Experts in Privacy and Technology, Docket No. DH6-2006-0060 (D.H.S. 2006), <http://bit.ly/2rnrh6w> 10

Complaint, *Abidor v. Napolitano*, Case No. 10–cv–04059 (E.D.N.Y. filed Sept. 7, 2010), ECF No. 19

Joseph Cox, *WSJ Reporter: Homeland Security Tried to Take My Phones at the Border*, Motherboard (July 21, 2016), <http://bit.ly/2BdVbtz>9

Brooke Crothers, *How Many Devices Can a Smartphone, Tablet Replace?* CNET (July 10, 2011 3:59 PM), <http://cnet.co/2BNK2zP>7

Michael J. de la Merced, *A World of Deal Making, Gleaned With an iPhone X*, NY Times (Dec. 27, 2017), <https://nyti.ms/2pH2oll>7

DHS, DHS Traveler Redress Inquiry Program (DHS TRIP), <https://www.dhs.gov/dhs-trip> (last visited Feb. 2, 2018).....4

Alexandra Ellerbeck, *Security Risk for Sources as U.S. Border Agents Stop and Search Journalist*, CPJ (Dec. 9, 2016), <https://perma.cc/VJ9L-HUG5>8

Gov't Obtains Wide AP Phone Records in Probe, Associated Press (May 13, 2013), <http://bit.ly/2mEtmHT>8

ICE, Border Searches of Electronic Devices, ICE Directive No. 7-6.1 (Aug. 18, 2009)....3

KFAI FOIA TRIP Complaints Border Electronics Searches, in Read Complaints About Warrantless Searches of Electronic Devices at the U.S. Border, N.Y. Times (Dec. 22, 2017), <https://www.nytimes.com/interactive/2017/12/22/us/politics/document-KFAI-FOIA-TRIP-Complaints-Border-Electronics.html>..... *passim*

Reporters Without Borders, *US-ACOS Alliance Seeks Department of Homeland Security Meeting* (Dec. 13, 2016, updated Jan. 17, 2017), <http://bit.ly/2hiN60j>9

Lindy Royce-Bartlett, *Leak Probe Has Chilled Sources, AP Exec Says*, CNN (June 19, 2013), <http://bit.ly/11NGbOH>.....8

Aaron Smith, Pew Research Center, *Record Shares of Americans Now Own Smartphones, Have Home Broadband* (Jan. 12, 2017), <http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/>4

Aaron Smith, Pew Research Center, *U.S. Smartphone Use in 2015* (Apr. 1, 2015), <http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/>.....4

Daniel J. Solove, *The First Amendment As Criminal Procedure*, 82 N.Y.U. L. Rev. 112 (2007).....15

Lana Sweeten-Shults, *Anonymous Sources Vital to Journalism*, USA Today (Feb. 27, 2017), <https://perma.cc/AV7V-Z4K8>7

U.S. Press Freedom Tracker, *BBC Journalist Questioned by US Border Agents, Devices Searched* (May 18, 2017), <http://bit.ly/2DMKctW>.....9

U.S. Press Freedom Tracker, *Photojournalist Detained at US-Canadian Border Ordered to Delete Images on Camera* (Sep. 4, 2017), <http://bit.ly/2mUjQyQ>.....9

INTEREST OF AMICI CURIAE¹

The Knight First Amendment Institute at Columbia University (“Knight Institute” or “Institute”) is a non-partisan, not-for-profit organization that works to defend the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. The Institute is particularly committed to addressing the implications of government surveillance for the freedoms of speech, association, and the press.

The Reporters Committee for Freedom of the Press was founded by leading journalists and media lawyers in 1970 when the nation’s news media faced an unprecedented wave of government subpoenas forcing reporters to name confidential sources. Today it provides pro bono legal representation, *amicus curiae* support, and other legal resources to protect First Amendment freedoms and the newsgathering rights of journalists.

¹ No counsel for a party authored this brief in whole or in part, no party or party’s counsel made a monetary contribution intended to fund the preparation or submission of this brief, and no person other than *amici* and their counsel contributed money intended to fund preparation or submission of the brief. This brief is filed pursuant to the Court’s December 27, 2017 Order (Dkt. No. 17).

SUMMARY OF ARGUMENT

Personal electronic devices have become extensions of the human mind. Individuals store on their cell phones and laptops enormous volumes of expressive materials: their private thoughts, beliefs, and associations, as well as a digital record of their whereabouts and communications with other people. Suspicionless searches of these devices at the border by the government raise constitutional questions that analog-era precedent cannot answer. Because of the scale and sensitivity of the information stored on these devices, searches of them pose a grave threat to the First Amendment freedoms of speech, of association, and of the press. This Court should hold that the First Amendment requires, at a minimum, that border agents obtain a warrant based upon probable cause before accessing the vast stores of private, expressive content on those devices.

The burden of device searches on travelers' First Amendment rights is far from "unspecified" or hypothetical, as the government argues. *See* Gov't Mem. in Support of Mot. to Dismiss (hereinafter "Gov't Mem.") at 21. Numerous complaints filed by travelers (obtained by *amicus* Knight Institute pursuant to a Freedom of Information Act request) demonstrate that border agents often scrutinize sensitive expressive and associational content that travelers store on their devices. The documents also detail the intimidation that travelers experience when border agents search their devices. Journalists are particularly vulnerable to the chilling effects of suspicionless searches, both because confidential or vulnerable sources may refuse to speak with reporters for fear that anything they say may end up in the government's hands, and because such searches can be used to retaliate against or deter reporting critical of the government.

The burdens on expression imposed by device searches demand First Amendment scrutiny. Applying the independent strictures of the First Amendment, it is clear that suspicionless searches

of electronic devices at the border are not sufficiently tailored to the government’s interests, and that the searches are therefore unconstitutional.

The government relies heavily on the “border search” doctrine in answering the plaintiffs’ First Amendment complaints, but as explained below, this reliance is misplaced for at least three reasons. First, that doctrine supplies an exception to the warrant requirement of the Fourth Amendment; it says nothing at all about the First Amendment. The First Amendment applies independently here, requiring the Court to answer the question that the Supreme Court left open in *United States v. Ramsey*, 431 U.S. 606 (1977), of whether border searches of expressive material are constitutional. Second, the applicability of the border search doctrine to electronic devices has been severely undermined by *Riley v. California*, 134 S. Ct. 2473 (2014), in which the Supreme Court made clear that analog-era precedent should not mechanically be extended to digital-age searches. Finally, even viewed solely through the lens of the Fourth Amendment, the serious First Amendment implications of device searches would nevertheless require application of the Fourth Amendment’s warrant and probable cause requirements with “scrupulous exactitude.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Stanford v. Texas*, 379 U.S. 476, 485 (1965).

ARGUMENT

I. Government Searches Of Electronic Devices At The Border Burden Core First Amendment Freedoms.

Policies promulgated by U.S. Customs and Border Protection (“CBP”) and U.S. Immigration and Customs Enforcement (“ICE”) permit border agents to search travelers’ electronic devices without any suspicion of wrongdoing.² These suspicionless intrusions directly

² ICE, Border Searches of Electronic Devices, ICE Directive No. 7-6.1 (Aug. 18, 2009); Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049 (Aug. 20, 2009). CBP recently released a revised directive, CBP, Border Search of Electronic Devices, CBP Directive No. 3340-049A (Jan. 4, 2018). The searches at issue in this case were conducted

burden travelers' freedoms of expression and association, and the freedom of the press. Travelers and journalists have described these burdens in complaints to the government and in news accounts of their experiences.

A. Government Searches Of Electronic Devices At The Border Burden Travelers' Freedoms Of Speech And Association.

Reports of travelers who have experienced suspicionless searches of their electronic devices illuminate the invasiveness of these searches and their chilling effect on the exercise of First Amendment rights. *Amicus Knight Institute* has obtained through litigation under the Freedom of Information Act, *see Knight First Amendment Inst. at Columbia Univ. v. U.S. DHS*, 1:17-cv-00548-TSC (D.D.C.), hundreds of complaints filed by individuals whose devices were searched at the border. The complaints were submitted through the U.S. Department of Homeland Security ("DHS") Traveler Redress Inquiry Program ("TRIP"),³ and they describe border agents' examinations of travelers' digitally recorded thoughts, communications, and photographs.⁴ For example, two U.S. citizens and their teenage daughters, stopped at the Houston airport when returning from a vacation to Guatemala, reported:

All our luggage was searched, all our papers were copied—including newspapers we had picked up in our travels. Our phones and electronic devices (ipad etc.) were taken, searched and all information was copied[]—all this without any explanation or

pursuant to CBP's and ICE's 2009 directives. In any event, the 2018 CBP directive offers no additional protection from "basic" or manual device searches.

³ See DHS, DHS Traveler Redress Inquiry Program (DHS TRIP), <https://www.dhs.gov/dhs-trip> (all internet sources cited last visited Feb. 2, 2018).

⁴ Over 75 percent of Americans own a smartphone, and nearly 70 percent of Americans use social media. Aaron Smith, Pew Research Center, *Record Shares of Americans Now Own Smartphones, Have Home Broadband* (Jan. 12, 2017), <http://pewrsr.ch/2igZgbJ>. A 2015 study revealed that a majority of smartphone owners used their phones to follow breaking news events, learn about events in their community, and share photos, videos, or other content about those events. Aaron Smith, Pew Research Center, *U.S. Smartphone Use in 2015* (Apr. 1, 2015), <http://pewrsr.ch/19JDwMd>.

accusation. We were advised if we refused such search, that we would be indefinitely detained.⁵

Similarly, a visa holder searched at a Denver airport reportedly received confirmation that “EIGHT persons ha[d] been handling my personal laptop computer and external hard drive” and “that all my files were copied and to be reviewed,” without being told “what is happening with my files” and “when those files will be deleted.”⁶ And a UK traveler reported that a border agent searched through “every email that I had sent and received,” as well as “personal photos of me and my family,” including “[intimate] photos with my wife.”⁷ According to the traveler, the agent was “laughing and smirking the whole time.”

Beyond these intrusions into the private content stored on travelers’ devices, the complaints also detail intrusions into travelers’ political and religious associations, and, as discussed in more detail below, newsgathering activities. For example, one traveler was stopped at a New York airport after returning from the Hajj and subjected to a search of his electronic devices that impinged upon both his political and religious affiliations. While all of the traveler’s “electronics were taken away and examined . . . without [his] consent,” he was asked “questions regarding [his] religious activity, civic engagement and political affiliation as well as charitable contributions [that] have nothing to do with [his] travel or the security of our country.” Another traveler’s complaint suggests intrusion into his religious association. The traveler, a U.S. citizen, noted that “after a lengthy interview, the officers interviewing me confessed that America needed more

⁵ *KFAI FOIA TRIP Complaints Border Electronics Searches* 33, in *Read Complaints About Warrantless Searches of Electronic Devices at the U.S. Border*, N.Y. Times (Dec. 22, 2017), <http://nyti.ms/2nAsLoL> [hereinafter *TRIP Complaints*] (Jan. 26, 2013 complaint); see also *id.* at 65 (June 12, 2015 complaint); 70 (Aug. 9, 2015 complaint); 76 (Oct. 24, 2015 complaint); 79 (Jan. 15, 2016 complaint); 93 (Sept. 25, 2016 complaint).

⁶ *TRIP Complaints* at 22 (Apr. 5, 2012 complaint).

⁷ *TRIP Complaints* at 79 (Jan. 15, 2016 complaint); see also *id.* at 58 (Jan. 16, 2015 complaint); 93 (Sept. 25, 2016 complaint).

Muslim leaders and imams like myself. However, they took my cellphone right after and downloaded all my contacts and messages.”⁸ Yet another complaint, from a U.S. citizen and freelance journalist for the *New York Times*, demonstrates intrusion into newsgathering activities and associations:

For three hours I was questioned, my notebooks and camera was [sic] taken (to make copies I assume) as was my laptop. I was asked about details of whom I met and interviewed, asked for contacts, telephone numbers, emails and I was physically searched . . . I would like this matter to be solved as soon as possible so I can continue my work as a journalist without being treated as a suspect.⁹

Many of the complaints also document a sense of intimidation in reaction to electronic device searches. Echoing sentiments expressed by numerous travelers, a U.S. citizen and professor whose family’s electronic devices were searched at a San Francisco airport wrote that “[m]y family and I feel belittled, ashamed, humiliated and disgraced when all of this happens.”¹⁰ Another U.S. citizen, who routinely endures questioning and electronic device searches upon returning to the United States from abroad, “feel[s] that ‘Welcome Back Home’ does not mean anything to me because my welcome party does not welcome with open arms, but with suspicion and paranoia.”¹¹ These first-hand accounts are illustrative of the hundreds of complaints filed by travelers whose devices were searched at the border. Such encounters inevitably burden speech and association.

B. Government Searches Of Electronic Devices At The Border Burden Freedom Of The Press.

Electronic devices are particularly critical tools for the modern-day press. For journalists on assignment, electronic devices serve as notebooks, typewriters, “cameras, video players,

⁸ *TRIP Complaints* at 24 (June 12, 2012 complaint).

⁹ *TRIP Complaints* at 94 (Oct. 18, 2016 complaint).

¹⁰ *TRIP Complaints* at 65 (June 11, 2015 complaint).

¹¹ *TRIP Complaints* at 65 (June 12, 2015 complaint); *see also id.* at 17 (Feb. 1, 2012 complaint).

rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.” *Riley*, 134 S. Ct. at 2489; *see also* Brooke Crothers, *How Many Devices Can a Smartphone, Tablet Replace?* CNET (July 10, 2011 3:59 PM);¹² Michael J. de la Merced, *A World of Deal Making, Gleaned With an iPhone X*, N.Y. Times (Dec. 27, 2017).¹³ Reporters cannot leave these devices, which are integral to their work, at home when traveling. And unfettered government access to these devices at the border threatens freedom of the press.

1. Suspicionless Searches Chill Reporter-Source Communications.

Because electronic devices are necessary to newsgathering, searches of these devices can force disclosure to the government of First Amendment-protected activity. These searches are often highly invasive, to a degree that would make reasonable journalists question whether they are really free to conduct their work. The contents of electronic devices can reveal the stories a journalist is developing, with whom she is communicating, and her specific travel plans. Disclosure of such information can expose sensitive newsgathering methods and deter potential sources from speaking to members of the media.

Suspicionless device searches may have a chilling effect on journalists’ communications with confidential sources, who are often necessary to accurate reporting. *See* Lana Sweeten-Shults, *Anonymous Sources Vital to Journalism*, USA Today (Feb. 27, 2017)¹⁴ (noting that without confidential sources, journalists “would be relying on the official side of the story, and the official side of a story isn’t always the whole side”). Some sources are willing to speak to reporters only with an assurance of confidentiality, but reporters who travel may not be able to offer that assurance when the mere act of crossing the border exposes their electronic devices to

¹² Available at <http://cnet.co/2BNK2zP>.

¹³ Available at <https://nyti.ms/2pH2oll>.

¹⁴ Available at <https://perma.cc/AV7V-Z4K8>.

suspicionless search and disclosure of their sources' identities. Similarly, suspicionless searches are especially likely to chill communications between journalists and vulnerable sources. *See, e.g.,* Alexandra Ellerbeck, *Security Risk for Sources as U.S. Border Agents Stop and Search Journalist*, CPJ (Dec. 9, 2016)¹⁵ (noting that agents at a Miami airport looked at a photojournalist's WhatsApp messages sent by a Syrian refugee source).

More broadly, government surveillance of reporters' communications is known to make sources reluctant to speak for fear of reprisal. In 2013, the Associated Press ("AP") learned that the Justice Department had seized records from twenty AP telephone lines used by more than 100 AP reporters and editors. *See Gov't Obtains Wide AP Phone Records in Probe*, Associated Press (May 13, 2013).¹⁶ AP President and CEO Gary Pruitt discussed the impact of the surveillance during a speech at the National Press Club, stating: "In some cases, government employees that we once checked in with regularly will no longer speak to us by phone and some are reluctant to meet in person." Lindy Royce-Bartlett, *Leak Probe Has Chilled Sources, AP Exec Says*, CNN (June 19, 2013).¹⁷ Suspicionless searches of electronic devices at the border can similarly deter sources from speaking with journalists, impeding the press's ability to report the news.

2. Journalists Are Particularly Likely To Be The Targets Of Suspicionless Border Searches.

Journalists are particularly vulnerable to targeted surveillance by means of suspicionless device searches, sometimes in retaliation for critical reporting. Reporters often travel to report on stories of particular interest to the United States government, which in turn may increase their likelihood of being stopped at the border and having their electronic devices searched. For

¹⁵ Available at <https://perma.cc/VJ9L-HUG5>.

¹⁶ Available at <http://bit.ly/2mEtmHT>.

¹⁷ Available at <http://bit.ly/11NGbOH>.

instance, in 2016, agents at LAX asked to search two cell phones belonging to a Wall Street Journal reporter who stated that her recent reporting had “deeply irked the US government,” and whose previous reporting sparked a Congressional investigation into U.S. military corruption. Joseph Cox, *WSJ Reporter: Homeland Security Tried to Take My Phones at the Border*, Motherboard (July 21, 2016).¹⁸ Other examples from recent years include:

- In May 2017, U.S. border agents questioned a BBC journalist at Chicago O’Hare International Airport for two hours, during which agents searched his phone and computer and read his Twitter feed.¹⁹
- Award-winning Canadian photojournalist Ed Ou said he was detained for six hours and questioned by U.S. officials at the U.S.-Canada border on October 1, 2016, while attempting to enter the United States to cover the Dakota Access Pipeline protests, and his devices were briefly confiscated.²⁰
- A photojournalist who traveled to Canada to take photographs for his work as a journalist was stopped at the border when he attempted to re-enter the United States, where a CBP agent turned on the photojournalist’s laptop computer and spent approximately 15 minutes searching its contents.²¹

CBP and ICE policies provide no substantive protections for journalists whose devices are searched. *See, e.g.*, CBP Directive No. 3340-049A § 5.2.2 (amended Jan. 4, 2018) (stating only that “work-related information carried by journalists[] shall be handled in accordance with any applicable federal law and CBP policy”). Nor do they recognize that journalists may be “flagged”

¹⁸ Available at <http://bit.ly/2BdVbtz>.

¹⁹ *See* U.S. Press Freedom Tracker, *BBC Journalist Questioned by US Border Agents, Devices Searched* (May 18, 2017), <http://bit.ly/2DMKctW>.

²⁰ *See* Reporters Without Borders, *US-ACOS Alliance Seeks Department of Homeland Security Meeting* (Dec. 13, 2016, updated Jan. 17, 2017), <http://bit.ly/2hiN60j>.

²¹ *See* Complaint, *Abidor v. Napolitano*, Case No. 10–cv–04059, ECF No. 1 ¶¶ 122–127 (E.D.N.Y. filed Sept. 7, 2010); *see also* U.S. Press Freedom Tracker, *Photojournalist Detained at US-Canadian Border Ordered to Delete Images on Camera* (Sept. 4, 2017), <http://bit.ly/2mUjQyQ> (describing a digital border search of another photojournalist who took photos while attempting to cross the U.S.-Canadian border).

for secondary screening by government officials more often than the average traveler because the nature of their work leads to travel patterns that draw additional scrutiny, such as traveling from high-risk countries, holding one-way tickets, or traveling frequently or on short notice. *See, e.g.*, Comments of 30 Organizations and 16 Experts in Privacy and Technology, Docket No. DH6-2006-0060 (D.H.S. 2006)²² (explaining that passenger profiling systems remain largely shielded from public view and stating that travel itineraries might be analyzed by CBP). These factors compound to make journalists likely targets for searches.

In short, suspicionless searches of electronic devices at the border impede the ability of journalists to gather news and communicate with sources — activities crucial to informing the public about world events.

II. Suspicionless Searches Of Electronic Devices At The Border Violate The First Amendment.

The First Amendment stands as a bulwark against the government’s suspicionless intrusion into individuals’ electronic devices, which contain enormously sensitive expressive, journalistic, and associational content. In its motion to dismiss, the government ignores the serious First Amendment concerns raised by suspicionless electronic device searches. Gov’t Mem. at 21-23.²³ The government’s argument rests on the assertion that prior decisions by other Courts of Appeals have rejected what the government calls a “First Amendment carve-out” to the border search exception. This argument fails for at least two reasons. First, the border search doctrine provides

²² Available at <http://bit.ly/2rnrh6w>.

²³ The government misleadingly calls the plaintiffs’ argument one for a “wholesale First Amendment carve-out to the border search doctrine.” Gov’t Mem. at 23. This hyperbole both misstates the argument — the plaintiffs do not suggest that any and all items are subject to First Amendment protections from search or seizure, such as is necessary to discover contraband — and assumes the conclusion that the “border search doctrine” permits suspicionless searches of electronic devices. It also incorrectly assumes that what satisfies the Fourth Amendment necessarily satisfies the First Amendment.

an exception only to the Fourth Amendment’s warrant requirement, not to the First Amendment, which independently protects against government conduct that burdens the freedoms of speech and of the press. Second, the cases cited by the government predate *Riley*, in which the Supreme Court held that a similar, analog-era exception to the warrant requirement did not extend to searches of cell phones, because of the scale and sensitivity of information those devices store. For these reasons, the Court should give the First Amendment its independent force and hold that the government’s suspicionless searches of electronic devices at the border are unconstitutional.

A. The Government’s Electronic Device Searches Must Be Evaluated Independently Under The First Amendment.

Contrary to the government’s argument, the First Amendment stands as an independent source of protection, separate and apart from the Fourth Amendment, against the search and seizure of the contents of travelers’ electronic devices at the border.²⁴ *See Tabbaa v. Chertoff*, 509 F.3d 89, 102 n.4 (2d Cir. 2007) (“[D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context.”).

Even when the Supreme Court first articulated the so-called “border search” exception to the Fourth Amendment’s warrant requirement in *United States v. Ramsey*, 431 U.S. 606 (1977), the Court recognized that searches of expressive content at the border would raise independent First Amendment concerns. *Ramsey* involved a search of incoming mail from Thailand that was suspected to contain heroin. *Id.* at 609-10. After holding the search permissible under the Fourth Amendment, the Court *separately* considered the possibility that the border search policy would chill free speech, and concluded that any such chill would be “minimal,” given that the statute at

²⁴ *Amici* agree with the plaintiffs that warrantless searches of electronic devices violate the Fourth Amendment as well.

issue prohibited the opening of envelopes absent reasonable suspicion, and given that the “[a]pplicable postal regulations flatly prohibit, under all circumstances, the reading of correspondence absent a search warrant.” *Id.* at 623-24. Under the regulations, “envelopes are opened at the border only when the customs officers have reason to believe they contain *other than correspondence*, while the *reading of any correspondence inside the envelopes is forbidden*,” absent a warrant. *Id.* at 624 (emphasis added). In other words, the Court made clear that the invasion of expressive content at the border would raise independent First Amendment concerns.

In *New York v. P.J. Video, Inc.*, 475 U.S. 868, 873 (1986), the Supreme Court again recognized the independence of First Amendment protections in the context of searches and seizures of expressive material. There, the Court explained that it had “long recognized that the seizure of films or books on the basis of their content implicates First Amendment concerns not raised by other kinds of seizures.” *Id.* While the Court held that the probable cause requirement for seizure of expressive material was *not greater* than the probable cause standard otherwise applicable to the issuance of a warrant under the Fourth Amendment, it also made clear that it was adherence to the probable cause requirement that would “protect against gross abuses” of First Amendment rights. *Id.* at 874 (quoting *Heller v. New York*, 413 U.S. 483, 492-93 (1973)).²⁵

²⁵ For this reason, the courts that have interpreted *P.J. Video* to suggest that the First Amendment provides no protections separate from the Fourth Amendment against the search and seizure of expressive material have misunderstood its holding. *See, e.g., United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005). In *P.J. Video*, the Court stated that the First Amendment does not require an even *more* stringent standard than Fourth Amendment probable cause. 475 U.S. at 874-75. But the reasoning in *P.J. Video* makes clear that the First Amendment has in numerous circumstances played an important role in protecting expressive material against seizures that might otherwise have been permissible under the Fourth Amendment. *Id.* at 873. Indeed, the Court has previously explained that other warrant “exceptions,” such as exigency, may *not* apply to expressive material under certain circumstances. *See Roaden v. Kentucky*, 413 U.S. 496, 505-06 (1973) (police may not rely on “exigency” exception to seize books or film when it would constitute a prior restraint).

Thus, when evaluating the First Amendment protections against suspicionless searches of electronic devices at the border, the Court must account for the breadth and nature of expressive content found on those devices. The Supreme Court recently recognized as much in *Riley*, where it held that the well-established “search incident to arrest” exception to the Fourth Amendment’s warrant requirement did not apply to searches of cell phones. Because the “search incident to arrest” exception and the border search exception are “similar” exceptions to the Fourth Amendment’s warrant requirement, *Ramsey*, 431 U.S. at 621, the Court’s analysis in *Riley* is particularly instructive here.

Riley’s teachings are twofold. First, the “quantitative and qualitative” differences between electronic devices and other objects that might hold expressive content necessitate rethinking the application of analog-era constitutional doctrines in new technological circumstances. The Court recognized in *Riley* that the rules set up to govern searches of physical objects do not have “much force with respect to digital content on cell phones,” reasoning that searches of cell phones invade privacy to an unprecedented extent. 134 S. Ct. at 2484. Recognizing that the two rationales for the search-incident-to-arrest exception — officer safety and preservation of evidence — were not sufficient to justify the “pervasive” threat to privacy posed by cell phone searches, the Court eschewed the Fourth Amendment framework previously applied to searches of objects on an arrestee’s person and imposed a “simple” and appropriately protective regime — requiring officers to “get a warrant.” *Id.* at 2495.

Second, the Court’s concern with warrantless searches of cell phones was inextricably intertwined with the use of those devices for expressive and associational purposes. As the Court explained, cell phones can carry “every piece of mail [owners] have received for the past several months, every picture they have taken, [and] every book or article they have read,” as well as

“picture messages, text messages, internet browsing history, a calendar, a thousand-entry phone book, and so on.” *Id.* at 2489. And cell phone searches could reveal “private interests or concerns,” such as “where a person has been” and “records of . . . transactions,” in addition to the owner’s communication history with every person she knows stretching back to the purchase of the device. *See id.* at 2490.

Riley thus underscores the error certain lower courts have made in rejecting First Amendment concerns arising from border searches of electronic devices. *See, e.g., United States v. Seljan*, 547 F.3d 993, 1011 (9th Cir. 2008) (quoting *United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005)). By assuming that searches of electronic devices were doctrinally indistinguishable from other border searches, these decisions ignored *Riley*’s teaching that analog-era precedent may not be mechanically extended to digital-age questions. The scale and sensitivity of the information stored on electronic devices, as well as their importance as means of communication, association, and newsgathering, require courts to examine whether the rationale underlying the border search doctrine justifies suspicionless searches of devices at the border. Earlier cases’ rote application of pre-*Riley* doctrine should be reevaluated post-*Riley*, taking into account the unique ability of devices to store and transmit vast quantities of First Amendment-protected expressive and journalistic material.

B. Suspicionless Searches Of Electronic Devices At The Border Fail First Amendment Scrutiny.

Applying the First Amendment’s independent guarantees in light of *Ramsey* and *Riley*, the burdens of suspicionless searches of electronic devices demand close scrutiny. The facts described in Part I, *supra*, demonstrate the First Amendment interests at stake when the government conducts suspicionless searches of electronic devices at the border. Border agents conducting those searches frequently scrutinize travelers’ private reading, private — sometimes anonymous — writings, and

private associations. Searches of journalists' electronic devices expose their confidential sources and newsgathering efforts. Because such "[g]overnment information gathering can threaten the ability to express oneself, communicate with others, explore new ideas, and join political groups," Daniel J. Solove, *The First Amendment As Criminal Procedure*, 82 N.Y.U. L. Rev. 112, 121 (2007), these searches require close scrutiny. Under any level of First Amendment scrutiny, suspicionless searches of electronic devices at the border are unconstitutional.

The Supreme Court has long recognized the First Amendment interests at stake in the forced disclosure of personal beliefs, private associations, and anonymous writings. In general, "[w]hen a State seeks to inquire about an individual's beliefs and associations a heavy burden lies upon it to show that the inquiry is necessary to protect a legitimate state interest." *Baird v. State Bar of Ariz.*, 401 U.S. 1, 6-7 (1971). And in *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), the Court held that "state action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny," regardless of "whether the beliefs sought to be advanced by association pertain to political, economic, religious, or cultural matters." *Id.* at 460-61. The Court explained that "compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [other] forms of governmental action," and therefore is typically prohibited under the First Amendment. *Id.* at 462.

Anonymous writings, too, enjoy strong First Amendment protection. The Supreme Court has held that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995). Because "identification of the author against her will" can "reveal unmistakably the content of her thoughts on a controversial issue," forced identification of a speaker can be

“particularly intrusive.” *Id.* at 355. Therefore, “exacting scrutiny” applies. *Id.* at 347 (finding forced identification of political pamphleteer unconstitutional). The First Amendment concerns with unmasking anonymous speakers are especially acute when the speakers are reporters’ confidential sources, because disclosure may jeopardize the act of publication itself. *See Zerilli v. Smith*, 656 F.2d 705, 710–11 (D.C. Cir. 1981) (“Compelling a reporter to disclose the identity of a confidential source raises obvious First Amendment problems,” and “the press’ function as a vital source of information is weakened whenever the ability of journalists to gather news is impaired.”); *cf. In re Request from the U.K. Pursuant to the Treaty between the Gov’t of the U.S. & the Gov’t of the U.K. on Mut. Assistance in Criminal Matters in the Matter of Dolours Price*, 718 F.3d 13, 23 (1st Cir. 2013) (recognizing that, in this circuit, the “leading cases regarding confidential sources” require “heightened sensitivity to First Amendment concerns”) (internal quotation marks omitted). Reporters returning from global assignments often carry with them information from confidential sources.

Regardless of whether the applicable level of scrutiny is the “closest” or most “exacting,” suspicionless searches of electronic devices fail. Even under intermediate scrutiny, the government must show that its searches are “narrowly tailored to serve a significant governmental interest,” *Cutting v. City of Portland*, 802 F.3d 79, 84 (1st Cir. 2015) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)), and that they “leave open ample alternative channels of communication.” *Perry Educ. Ass’n v. Perry Local Educators’ Ass’n*, 460 U.S. 37, 45 (1983). The government cannot do so here.

First, suspicionless searches of electronic devices at the border fail to satisfy the “narrow tailoring” requirement. Those searches are over-inclusive for the simple reason that the vast majority of suspicionless searches will reveal no information of any legitimate interest to the

government. The government has never suggested otherwise. In addition, the harm from these over-inclusive searches is not limited to those individuals who are searched; the knowledge that the content of their devices may be searched without any cause whatsoever has a likely chilling effect on the expressive activities of every traveler, who may refrain from using their devices for expressive and associational purposes for fear that their private communications will be exposed. This chilling effect is exacerbated by the nearly unfettered authority that CBP's and ICE's policies give border agents to decide whose devices to search and for what reason. *Cf. City of Lakewood v. Plain Dealer Publ'g Co.*, 486 U.S. 750, 757 (1988) (referring to the "time-tested knowledge that in the area of free expression . . . placing unbridled discretion in the hands of a government official or agency . . . may result in censorship"). Suspicionless border searches thus threaten to chill the speech of every international traveler.

Second, these searches fail to "leave open ample alternative channels of communication." *Perry Educ. Ass'n*, 460 U.S. at 45. In the modern world, there is no realistic alternative to the channels of communication that the internet and electronic devices provide, whether a potential alternative is evaluated in terms of speed, scope, breadth of audience, or ability to communicate with otherwise remote persons. *Cf. Riley*, 134 S. Ct. at 2489-90 (describing "qualitative" and "quantitative" differences in the storage, communicative capacity, and pervasiveness of cell phones compared to pre-digital objects); Part I.B, *supra* (describing journalists' dependence on electronic devices to gather and disseminate news). Government action that chills communication across these channels leaves no realistic alternative for travelers seeking to avoid such governmental intrusion.

The government offers essentially no facts to demonstrate that its suspicionless electronic device searches are appropriately tailored to a legitimate governmental interest, nor could it. Those searches are therefore inconsistent with the First Amendment.

III. The First Amendment Implications Of Electronic Device Searches At The Border Require Scrupulous Adherence To The Fourth Amendment Warrant Requirement.

The Court should also evaluate the plaintiffs' Fourth Amendment claims against the backdrop of the First Amendment interests implicated by suspicionless device searches. The history of the Fourth Amendment demonstrates that it is intertwined with the First Amendment's guarantee of a free press, and it should be interpreted to protect those interests.

The history of the Fourth Amendment is "largely a history of the conflict between the Crown and the press." *Stanford v. Texas*, 379 U.S. 476, 482 (1965). Awareness of the British Crown's use of "general warrants," which allowed government agents to search "private houses for the discovery and seizure of books and papers that might be used to convict their owner of the charge of libel," *Boyd v. United States*, 116 U.S. 616, 626 (1886), formed "part of the intellectual matrix within which our own constitutional fabric was shaped." *Marcus v. Search Warrants*, 367 U.S. 717, 729 (1961). The use of these warrants to stifle free expression was a primary concern of the pre-Revolution English courts, and one of the Founders' rationales for adopting the Fourth Amendment. *See Stanford*, 379 U.S. at 483-84 (citing *Entick v. Carrington*, 19 How. St. Tr. 1029 (C.P. 1765) and *Wilkes v. Wood*, 19 How. St. Tr. 1153 (C.P. 1763)); *Marcus*, 367 U.S. at 729; *Boyd*, 116 U.S. at 626-27.

Recognizing this historical connection between the free press and the Fourth Amendment, the Supreme Court has required adherence to the warrant and probable cause protections of the Fourth Amendment with "scrupulous exactitude" when confronted with searches and seizures of materials that "may be protected by the First Amendment." *Zurcher v. Stanford Daily*, 436 U.S.

547, 564 (1978) (quoting *Stanford*, 379 U.S. at 485). Indeed, First Amendment protections of materials to be searched or seized can change the analysis of whether an exception to the Fourth Amendment’s warrant requirement applies. That is, “[a] seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material.” *Zurcher*, 436 U.S. at 564. For that reason, the Supreme Court held that the exigency exception to the warrant requirement is inapplicable to the seizure of allegedly obscene materials when such a seizure might effectively constitute a prior restraint. *Roaden v. Kentucky*, 413 U.S. 496 (1973). The Court then extended that holding, requiring a warrant even if the seizure of such material would not constitute a prior restraint. *Heller v. New York*, 413 U.S. 483 (1973).

The border search exception to the warrant requirement should be treated no differently. The only measure sufficiently protective of the speech and associational rights of travelers, and the newsgathering activities of journalists, is to make the often confidential and sensitive contents of their electronic devices subject to search only pursuant to a warrant based on probable cause.

CONCLUSION

For the foregoing reasons, the government's motion to dismiss should be denied.

Dated: February 2, 2018

Respectfully submitted,

/s/ Jonathan M. Albano
Jonathan M. Albano
BBO #013850
jonathan.albano@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
One Federal Street
Boston, MA 02110-1726
Telephone: (617) 341-7700
Facsimile: (617) 341-7701

Scott B. Wilkens (*pro hac vice* forthcoming)
Michael E. Stewart (*pro hac vice* forthcoming)
JENNER & BLOCK LLP
1099 New York Ave., NW, Suite 900
Washington, DC 20001
Telephone: (202) 639-6000
Facsimile: (202) 639-6066

Attorneys for Amici Curiae

CERTIFICATE OF SERVICE

I, Jonathan M. Albano, hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on February 2, 2018.

Jonathan M. Albano