UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, Plaintiff, v. KURBONALI SULTANOV, Defendant.	Docket No. 1:22-cr-149 (NRM)

BRIEF OF *AMICI CURIAE* KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY AND THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

Bruce D. Brown
Gabriel Rottman
Grayson Clary
Reporters Committee for Freedom
of the Press
1156 15th St. NW, Suite 1020
Washington, D.C. 20005
T: (202) 795-9300
F: (202) 795-9310

Scott B. Wilkens
Alex Abdo
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
T: (646) 745-8500
F: (646) 661-3361
scott.wilkens@knightcolumbia.org

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

STATEMENT OF IDENTITY AND INTEREST OF AMICI CURIAE

Amici curiae are the Knight First Amendment Institute at Columbia University ("Knight Institute") and the Reporters Committee for Freedom of the Press.

Amici file this brief in support of Defendant Sultanov's motion to suppress evidence. Warrantless searches of electronic devices intrude on personal privacy and burden and chill First Amendment–protected activities, including newsgathering. As organizations that advocate for the First Amendment rights of the press and public, *amici* have a strong interest in ensuring that these searches honor constitutional limits.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

Personal electronic devices have become extensions of the human mind. Cell phones and laptops store enormous volumes of individuals' private information and expressive materials: journalists' work product, travelers' private thoughts, personal and professional associations, and digital records of their whereabouts and communications. Warrantless searches of these devices at the border raise constitutional questions that analog-era precedents cannot answer. Because of the scale and sensitivity of the information stored on these devices, government searches of them pose a grave threat to the Fourth Amendment right to privacy as well as the First Amendment freedoms of the press, speech, and association.

In this case, the government stopped the defendant, Mr. Sultanov, at JFK as he was returning from a trip abroad, and conducted a warrantless search of his cellphone in pursuit of evidence of a crime unrelated to border control—possession of child pornography. If the search had occurred in a different context, there would be no question of its unconstitutionality. But because U.S. Customs and Border Protection ("CBP") intercepted Mr. Sultanov as he was entering the country, the government argues that the search fell within the "border search" exception to the warrant requirement.

As *amici* discuss below, the questions before this Court have far-reaching implications for the newsgathering rights of journalists and the First and Fourth Amendment rights of all travelers. Journalists are particularly vulnerable to the chilling effects of electronic device 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. Documents obtained by *amicus* Knight Institute pursuant to a Freedom of Information Act request show that border personnel often use

their authority to conduct border searches as a pretext to scrutinize the sensitive expressive and associational content that travelers store on their devices.

In light of these implications, warrantless searches of electronic devices at the border violate the First and Fourth Amendments. Applying the Fourth Amendment analysis from *Riley v. California*, 573 U.S. 373 (2014), to this case, the government has only a weak interest in warrantless searches of electronic devices at the border, whereas those searches constitute a profound invasion of the expressive and privacy rights of journalists and travelers. Given this imbalance, the Fourth Amendment requires a warrant before the government can search electronic devices at the border.

The First Amendment implications of device searches should also inform the Court's Fourth Amendment analysis, because the Fourth Amendment's warrant requirement must be applied with "scrupulous exactitude" when searches burden free expression, *see Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). The First Amendment also independently regulates device searches at the border, and warrantless device searches plainly fail traditional First Amendment scrutiny. For these reasons, the Court should conclude that the search of Mr. Sultanov's device was unconstitutional.[1]

ARGUMENT

I. Government searches of electronic devices at the border intrude on Fourth Amendment privacy interests and burden First Amendment freedoms.

Policies promulgated by CBP and U.S. Immigration and Customs Enforcement ("ICE") permit border agents to search journalists' and other travelers' electronic devices without a

[1] *Amici* take no position on the defendant's Fifth Amendment argument or the applicability of the "good faith" exception to the exclusionary rule under the Fourth Amendment.

warrant, and often without any suspicion at all.[2] ICE and CBP conduct these searches frequently—in fiscal year 2021, for example, CBP conducted over 37,000 of them. *See CBP Enforcement Statistics Fiscal Year 2022 – Border Searches of Electronic Devices*, U.S. Customs & Border Prot., https://perma.cc/6P47-XA4M. And while it would be clear even absent specific evidence that these invasive searches implicate extremely sensitive information protected by the Fourth Amendment and constrict the "breathing space" that First Amendment freedoms need "to survive," *NAACP v. Button*, 371 U.S. 415, 433 (1963), the risks they pose are well-documented through news reporting, transparency litigation, and journalists' and travelers' personal accounts.

A. Government searches of electronic devices at the border burden freedom of the press.

Electronic devices are critical tools for the modern-day press. For journalists on assignment, they serve as notebooks, typewriters, "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley*, 573 U.S. at 393; *see also* Brooke Crothers, *How Many Devices Can a Smartphone, Tablet Replace?*, CNET (July 10, 2011), https://perma.cc/Z8KE-5Y8U; Michael J. de la Merced, *A World of Deal Making, Gleaned with an iPhone X*, N.Y. Times (Dec. 27, 2017), https://perma.cc/5N4W-2LN8. "[I]t is neither realistic nor reasonable to expect the average [reporter] to leave [their] digital devices at home when traveling," *United States v. Kolsuz*, 890 F.3d 133, 145 (4th Cir. 2018) (citation and internal quotation marks omitted), and unfettered government access to them threatens a free press.

1. Electronic device searches chill reporter-source communications.

Experience teaches that government surveillance that is "too permeating" will predictably intrude on the newsgathering process—exposing stories pursued, newsgathering methods

[2] *See* ICE, Directive No. 7-6.1, Border Searches of Electronic Devices (Aug. 18, 2009); CBP, Directive No. 3340-049, Border Search of Electronic Devices Containing Information (Aug. 20, 2009).

employed, and the identities of sources consulted. *United States v. Di Re*, 332 U.S. 581, 595 (1948). Device searches force reporters to disclose just such information to the government, deterring potential sources from speaking to the press and damming the free flow of information to the public.

As courts have recognized, "journalists frequently depend on informants to gather news, and confidentiality is often essential to establishing a relationship with an informant." *Zerilli v. Smith*, 656 F.2d 705, 711 (D.C. Cir. 1981); *see also* Lana Sweeten-Shults, *Anonymous Sources Vital to Journalism*, USA Today (Feb. 28, 2017), https://perma.cc/AV7V-Z4K8. Many sources are willing to speak to reporters only with that assurance of confidentiality because they reasonably fear retribution if their identities are revealed, including criminal prosecution, loss of employment, and even risk to their lives. *See Introduction to the Reporter's Privilege Compendium*, Reps. Comm. for Freedom of the Press, https://perma.cc/LQ7X-AAJA. For just that reason, the Department of Justice recently sharply restricted the ability of its employees to seize journalists' data, recognizing that past policies "fail[ed] to properly weight the important national interest in protecting journalists from compelled disclosure of information revealing their sources, sources they need to apprise the American people of the workings of their government." *Memorandum from the Attorney Gen. Regarding Use of Compulsory Process to Obtain Information From, or Records of, Members of the News Media* (July 19, 2021), https://perma.cc/428V-FX24; *see* 28 C.F.R. § 50.10 (a)(2) (regulations prohibiting the use of "compulsory legal process for the purpose of obtaining information from or records of members of the news media acting within the scope of newsgathering," with limited exceptions).[3]

[3] In response to recent examples of ICE overreach, Congress directed the agency to adopt similar guidelines, though the protocols the agency issued are less protective. *See* Gabe Rottman, *ICE Enacts New Policy Protecting Media from Legal Demands*, Lawfare (June 29, 2022), https://perma.cc/3388-MYCS.

But reporters who travel internationally cannot credibly offer sources confidentiality if the mere act of crossing the border exposes their electronic devices to search and the identities of their contacts to disclosure. *See, e.g.,* Alexandra Ellerbeck, *Security Risk for Sources as U.S. Border Agents Stop and Search Journalists*, Comm. to Protect Journalists (Dec. 9, 2016), https://perma.cc/VJ9L-HUG5. And when border agents can mine any journalist's work product at will, the press runs "the disadvantage of . . . appearing to be an investigative arm of the judicial system or a research tool of government" rather than an independent check on it, *United States v. LaRouche Campaign*, 841 F.2d 1176, 1182 (1st Cir. 1988) (internal quotation marks omitted), deterring future sources from stepping forward with sensitive information. Reporters repeatedly have described this dynamic in past controversies involving government investigations of the news media. *See, e.g.*, Jeff Zalesin, *AP Chief Points to Chilling Effect After Justice Investigation*, Reps. Comm. for Freedom of the Press (June 19, 2013), https://perma.cc/U7Z8-FPEK; *see also* Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law, and American Democracy* at 3–4 (2014), https://perma.cc/KUH6-4MVF. The warrantless search authority the United States defends here poses the same risk to the free flow of information to the public.

2. Reporters are particularly likely to be targeted for border searches.

The burden that warrantless device searches impose on newsgathering is only sharpened by the reality that journalists are at special risk of being singled out for such searches, sometimes in retaliation for critical reporting. Reporters often travel to report on stories of particular interest to the U.S. government, which naturally increases the likelihood that border agents will stop them and search their electronic devices. For instance, in 2016, agents at LAX airport asked to search two cell phones belonging to a Wall Street Journal reporter whose recent reporting had "deeply

irked the US government," and whose previous reporting had sparked a congressional investigation into corruption in the military. Joseph Cox, *WSJ Reporter: Homeland Security Tried to Take My Phones at the Border*, Motherboard (July 21, 2016), https://perma.cc/BMN9-96LW.

More recently, in early 2019, a flurry of news reports documented a clear pattern of harassment at the border of journalists covering migration issues, harassment that included device searches and detentions. *See Several Journalists Say US Border Agents Questioned Them About Migrant Coverage*, Comm. to Protect Journalists (Feb. 11, 2019), https://perma.cc/QYK3-BKSF; Ryan Devereaux, *Journalists, Lawyers, and Activists Working on the Border Face Coordinated Harassment from U.S. and Mexican Authorities*, The Intercept (Feb. 8, 2019), https://perma.cc/SR2Y-Y8KR. It was later learned that these screenings were the product of a secret database CBP maintained to monitor reporters covering issues related to migrants crossing the U.S.-Mexico border. *See* Tom Jones, Mari Payton & Bill Feather, *Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database*, NBC 7 (Jan. 10, 2020), https://perma.cc/6VPX-B67U. Screenshots of the database confirm that an "alert" was placed on these journalists' passports to flag them for secondary screening. And a federal court in this District concluded, in a suit filed by five photojournalists whose names appear in the database, that the allegations stated a violation of the reporters' First Amendment rights. *Guan v. Mayorkas*, 530 F. Supp. 3d 237 (E.D.N.Y. 2021).

Other recent examples of journalists subjected to invasive searches, including electronic device searches, illustrate how frequently journalists are targeted at the U.S. border:

- In October 2021, freelance journalist Sergio Olmos had his belongings searched in a secondary screening after declining to answer where he went to journalism school.[4]

- In April 2021, The Intercept's Ryan Devereaux and photojournalist Ash Ponders were detained after returning to the United States from covering a protest in Mexico. Ponders was strip-searched, and border officials asked to see her footage; Devereaux was told "You are not a journalist" on sharing his affiliation with The Intercept.[5]

- In June 2019, CBP officers detained independent photographer Tim Stegmaier for over four hours, searching his computer, phone, and camera, which they then seized and retained for three months.[6]

- In May 2019, CBP officers detained Rolling Stone journalist Seth Harp in Austin, Texas for four hours, questioning him about his reporting and searching his electronic devices.[7]

- In May 2017, U.S. border agents questioned a BBC journalist at Chicago O'Hare International Airport for two hours, searched his phone and computer, and read his Twitter feed.[8]

And stories have continued to emerge of broader misuse of CBP authorities to investigate members of the news media. Most recently, Yahoo News exposed "a sprawling leak investigation conducted by a secretive unit at CBP that regularly used the country's most sensitive databases to investigate the finances, travel and personal connections of journalists, congressional members

[4] *See Freelance Journalist Questioned About Journalism at Portland Airport*, U.S. Press Freedom Tracker (Oct. 18, 2021), https://perma.cc/V9K7-5GPU.

[5] *See Intercept Reporter Told "You Are Not a Journalist" When Stopped by Border Officials*, U.S. Press Freedom Tracker (Apr. 30, 2021), https://perma.cc/46N2-PV2H.

[6] *See Independent Photographer Stopped for Secondary Screening, Devices Seized*, U.S. Press Freedom Tracker (June 28, 2019), https://perma.cc/4XD7-Z6HC.

[7] Seth Harp, *I'm a Journalist But I Didn't Fully Realize the Terrible Power of U.S. Border Officials Until They Violated My Rights and Privacy*, The Intercept (June 22, 2019, 8:00 AM), https://perma.cc/6U24-2GQA; *Rolling Stone Journalist Stopped for Secondary Screening, Has Electronics Searched While Asked Invasive Questions About Reporting*, U.S. Press Freedom Tracker (May 13, 2019), https://perma.cc/RV5B-SKES.

[8] *See BBC Journalist Questioned by US Border Agents, Devices Searched*, U.S. Press Freedom Tracker (May 18, 2017), https://perma.cc/CFK5-RH5E.

and staff and other Americans not suspected of any crime." Jana Winter, *DHS to Provide Congress with Operation Whistle Pig Report Detailing Spying on Journalists, Lawmakers*, Yahoo News (Mar. 10, 2022), https://perma.cc/N57G-EMC7; *see also Reporters Committee for Freedom of the Press v. U.S. Customs and Border Protection*, Reps. Comm. for Freedom of the Press, https://perma.cc/T6N9-H9UF.

The warrantless search authority the government defends here poses an acute threat to the free press.

B. Government searches of electronic devices at the border intrude on travelers' right to privacy and freedoms of speech and association.

The chilling effect of device searches at the border extends beyond journalists' newsgathering rights. More broadly, these searches chill the First Amendment activities of ordinary travelers and intrude on their Fourth Amendment privacy rights, further inhibiting public debate and the free flow of information. Through litigation under the Freedom of Information Act, *see Knight First Amendment Inst. at Columbia Univ. v. U.S. Dep't of Homeland Sec.*, No. l:17-cv-00548-TSC (D.D.C. 2017), *amicus* Knight Institute has obtained hundreds of complaints filed by individuals whose devices were searched at the border, as well as thousands of reports documenting device searches conducted by CBP and ICE. These records describe border agents' examinations of travelers' private information, including digitally recorded thoughts, communications, and photographs.

Some of these records also detail intrusions into travelers' political and religious associations. For example, in 2016, one traveler was detained by CBP officers in the Abu Dhabi airport for three days. At the beginning of the encounter, CBP officers confiscated the traveler's devices and demanded passwords to her Facebook, Gmail, and WhatsApp accounts. Officers asked the traveler intrusive questions about her political beliefs, including "[w]hat [she] think[s] when

Americans say that Muslims are terrorists." Her devices were only returned three days later, when she boarded a new flight to the United States.[9]

Another traveler was ordered to hand over his devices and provide officers with his cell phone and computer passwords. When the traveler asked whether the officers needed a warrant, one officer replied, "This is the border. We don't need anything." The officers then searched through the traveler's text messages, contacts, and photos, asking extensive questions about certain text messages. The officers also interrogated him about his political views, any political organizations he belonged to, and whether he hated America or was part of "Antifa."[10]

Many travelers reported being subjected to questions about their religious practices. One traveler noted that "after a lengthy interview, the officers interviewing me confessed that America needed more Muslim leaders and imams like myself. However, . . . they took my cellphone right after and downloaded all my contacts and messages."[11] Another recalled that after officers confiscated her phone and demanded her password, they reviewed videos on her phone, checked her Facebook page, and interrogated her for forty-five minutes about the mosque she attended, whether she knew any victims of the Quebec mosque attack that had taken place the week before, and her opinion of President Trump's policies.[12]

---

[9] *CRCL Complaint Intake and Response (3/12/2018)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/EA4C-255Q.

[10] *CRCL Complaint Intake Form (5/27/2018)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/W7K3-2JQH.

[11] *Read Complaints About Warrantless Searches of Electronic Devices at the U.S. Border*, N.Y. Times (Dec. 22, 2017), https://perma.cc/JWC9-5ZN3 (see page 24 of the embedded document entitled "KFAI FOIA TRIP Complaints Border Electronics Searches").

[12] *CRCL Complaint Closure (07/11/2017)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/2GDA-F7G6.

Search reports completed by CBP and ICE officers show that they not only reviewed the contents of travelers' devices during border encounters, but also kept records of travelers' social media accounts. During one such search, CBP officers recorded a traveler's account handles on Instagram, Facebook, WhatsApp, Viber, Snapchat, YouTube, and Tango. The officers also made note of the traveler's answers to account security questions, his pin code, and the code to unlock his phone.[13] Other reports document the confiscation of travelers' email addresses.[14]

Some travelers were also subjected to forensic searches of their devices, which are even more intrusive than basic searches. Forensic searches generally involve prolonged confiscation of an individual's devices so that the government can download the entirety of their contents for unlimited searching.[15] *See United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013) (referring to such searches as equivalent to a "computer strip search"). Among other examples, one forensic search of a traveler's devices conducted by ICE yielded tens of thousands of chat messages, documents, photos, videos, and emails, which the government was then able to search at will.[16] Through warrantless forensic searches, border agents have downloaded travelers' geolocation data, giving the government "near perfect surveillance" into the "privacies of life."[17] *Carpenter v.*

[13] *CBP Electronic Media Report (7/26/2017)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/X5QF-V5CU.

[14] *CBP Electronic Media Report (9/03/2017)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/KVJ9-7PXR.

[15] *See also*, *e.g.*, *ICE Report of Investigation (Opened 1/12/2016, Approved 6/23/2016)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/SD6F-TFAM.

[16] *ICE Report of Investigation (Opened 1/12/2016, Approved 6/6/2016)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/D39N-EQAP; *ICE Report of Investigation (Opened 1/12/2016, Approved 6/23/2016)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/GT4D-V4JW.

[17] *ICE Report of Investigation (Opened 4/13/2012, Approved 4/19/2012)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/3R7H-HNYG; *ICE Report of Investigation (Opened 8/10/2012, Approved 10/22/2012)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/7PAT-6SPC.

United States, 138 S. Ct. 2206, 2217–18 (2018) (citations omitted). Finally, border agents have also used the threat of a forensic search to force travelers to unlock devices for a basic search.[18]

These searches inevitably burden speech and association. As in the context of government surveillance more generally, when individuals fear that their speech will be scrutinized, they will be less inclined to speak. *See, e.g.*, Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech. L.J. 117, 125 (2016) (finding a "statistically significant reduction" in Wikipedia traffic to privacy-sensitive articles after the Snowden disclosures in June 2013). When travelers know they could be subjected to warrantless searches touching on political, social, religious, or other expressive activity—activity that the First and Fourth Amendments were designed to protect from unreasonable government scrutiny—they are less likely to engage in that activity.

II. The Government's warrantless search of Mr. Sultanov's cellphone was unconstitutional.

This Court should hold that the government's warrantless search of Mr. Sultanov's cellphone violated the First and Fourth Amendments. Cellphones and laptops differ fundamentally from other objects in the scale and nature of expressive information they typically contain, and the burdens that device searches impose on individual privacy and First Amendment freedoms make them unlike the searches that historically fell within the so-called "border search" exception. In *Riley*, the Supreme Court said that equating searches of cellphones with searches of other personal items like wallets, purses, and address books is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley*, 573 U.S. at 392–93.

[18] *Letter from ACLU to DHS (5/4/2017)*, Knight First Amendment Inst. at Columbia Univ., https://perma.cc/84P6-CAFF.

These differences between electronic devices and other objects have several important implications for the defendant's suppression motion. First, they fundamentally alter the balance of interests under a traditional Fourth Amendment analysis: Cellphone searches do little to serve the government interests underlying the border search exception, but the expressive privacy interests at stake are mammoth compared to a luggage search. Second, the serious First Amendment concerns raised by searches of electronic devices affects the Fourth Amendment analysis, because the warrant requirement must be applied with "scrupulous exactitude" when searches burden First Amendment activity. *Zurcher*, 436 U.S. at 564 (quoting *Stanford*, 379 U.S. at 485). Finally, in light of travelers' and journalists' expressive and associational interests, these searches must comply with the First Amendment, which stands as an independent bulwark against the government's intrusion into individuals' electronic devices. Through any of these lenses, warrantless device searches at the border violate the Constitution.

A. Warrantless searches of electronic devices at the border violate the Fourth Amendment.

In the absence of a warrant, the search of an electronic device at the border violates the Fourth Amendment unless it "falls within a specific exception to the warrant requirement." *Riley*, 573 U.S. at 382, 402. In determining whether a traditional exception extends to the search of novel electronic devices, the "ultimate touchstone is . . . reasonableness." *Id.* at 381 (internal quotation marks omitted). In *Riley* itself, for instance, the Supreme Court held that searches of cellphones do not fall within the search-incident-to-arrest exception because such searches do not serve the government interests at stake and constitute unprecedented intrusions into personal privacy. *Id.* at 401. And in *United States v. Smith*—a case very much like this one—Judge Rakoff recently explained in great detail that "[a]pplying [the Fourth Amendment's] balancing framework to phone searches at the border yields the same result as in *Riley*." No. 22-CR-352 (JSR), 2023 WL 3358357,

at *7 (S.D.N.Y. May 11, 2023). As *Smith* demonstrates, traditional Fourth Amendment principles require a warrant here.[19]

The Fourth Amendment analysis in this case, as in *Riley* and *Smith*, requires balancing the government interests at stake against the extent of the intrusion into personal privacy. *See Riley*, 537 U.S. at 385; *Smith*, 2023 WL 3358357, at *7. The Court "should not automatically presume that a balance previously struck as to a certain kind of physical search automatically extends to a search of the data contained on a person's cell phone," and should instead "independently evaluate whether the governmental interests thought to support a warrant exception actually apply to cell phone searches, and whether the intrusion on privacy posed by a physical search is relevantly comparable to that posed by a search of cell phone data." *Smith,* 2023 WL 3358357, at *7 (citing *Riley*, 537 U.S. at 385–403).

1. Searches of electronic devices do not serve the government interest in the border search exception.

The border search exception has historically been grounded in the government's need "to regulate the collection of duties and to prevent the introduction of contraband into this country." *United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., concurring); *see also* Laura K. Donohue*, Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 Yale L.J. Forum 961, 962 (2019); *The Border Search Muddle*, 132 Harv. L. Rev. 2278, 2287 (2019). But as *Smith* explains, that interest is little served—if at all—by searching the digital equivalent of travelers' personal papers.

[19] Several courts have said that *Riley*'s analysis does not apply in the border search context, but fail to explain why, other than simply stating that the border search and search-incident-to-arrest exceptions are separate and serve different purposes. *See, e.g.*, *Alasaad v. Mayorkas*, 988 F.3d 8, 17 (1st Cir. 2021), *cert. denied sub nom. Merch. v. Mayorkas*, 141 S. Ct. 2858 (2021); *United States v. Xiang*, 67 F.4th 895, 900 (8th Cir. 2023).

For one, although the government can successfully prevent physical contraband or unauthorized people from entering the country by interdicting them at the border, it cannot do the same with the information stored on a traveler's cellphone. That information "can and very likely does exist not just on the phone device itself, but also on faraway computer servers potentially located within the country." *Smith*, 2023 WL 3358357, at *8. The government apparently fails to recognize this in arguing that so-called "digital contraband"—such as the images and videos of child pornography at issue in this case—is like physical contraband in that it can be stopped from entering the country. Dkt 22 at 19, 22-23; Dkt. 27 at 2, 4; Dkt. 30 at 3-4. While "[p]hysical contraband, once interdicted, will not enter the country, . . . digital contraband easily could and very likely already has." *Smith,* 2023 WL 3358357, at *8; *see also United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting) (noting that "digital contraband is borderless and can be accessed and viewed in the United States without ever having crossed a physical border."). And for just that reason, the government's interest in searching devices at the border is much weaker than its interest in inspecting luggage—no matter how many phones the government rifles through, it cannot meaningfully prevent data from flowing across the border. *See Smith,* 2023 WL 3358357, at *8.[20]

2. Searches of electronic devices at the border are profound intrusions upon personal privacy.

In contrast to the government's relatively weak interest in searching devices at the border, such searches constitute an extraordinary intrusion into the privacy of journalists and other travelers. Modern cellphones are fundamentally different from any other personal item that

[20] Several courts have held that searches of cellphones for digital contraband should require either no suspicion at all or only reasonable suspicion, but they, too, fail to address the "borderless" nature of digital contraband. *See*, *e.g.*, *United States v. Cano*, 934 F.3d 1002, 1014 (9th Cir. 2019).

individuals may carry with them. They are "minicomputers" that are much more than just phones; they "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley*, 573 U.S. at 393.

As a result, cellphones differ both quantitatively and qualitatively from other personal property. *Id*. Quantitatively, cell phones have an "immense storage capacity" that allows them to hold "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.*[21] That capacity has important implications for personal privacy. Users can "collect[] in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record." *Id*. at 394. And the amount users can collect of "just one type of information" can "convey far more than previously possible," such that "the sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id.* In effect, given the pervasiveness of cellphones, most Americans "keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Id.* at 395.

Qualitatively, cellphones have led to the collection of many new types of data, such as search and browsing history, location data, and the "detailed information about all aspects of a person's life" captured by the countless apps people can download to their phones, which no wallet or luggage search could previously have reached. *Id.* at 396. In short, "[a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array

[21] Notably, storage capacity has grown enormously since *Riley* was decided almost 10 years ago. At that time, the "top-selling smart phone had a standard capacity of 16 gigabytes (and [was] available with up to 64 gigabytes)." *Riley*, 573 U.S. at 394. Today, "[m]ost phones, even the budget ones, come with at least 32GB of storage," and "[h]igher-end phones … offer capacities of 256GB or more." Andrew Lanxon, *Buying a New iPhone or Android Phone? Consider These Things First*, CNET (March 24, 2023), https://perma.cc/6UXV-MJBK. The latest phones offer a storage capacity of up to one terabyte. *iPhone 15 Pro*, Apple, https://perma.cc/7HVM-M6FG; *Galaxy S23 Ultra*, Samsung, https://perma.cc/W9NQ-SPLH.

of private information never found in a home in any form—unless the phone is." *Id.* at 396–97. The expressive privacy interests at stake in device searches dwarf those implicated by a typical border search for physical contraband.

3. The balance of interests requires a warrant when the government searches electronic devices at the border.

When the government's relatively weak interest in device searches at the border is balanced against their unprecedented intrusion upon the privacy of journalists and other travelers, the result is clear. The government must obtain a warrant before searching a cellphone at the border. *See Smith,* 2023 WL 3358357, at *7 (a warrant is required because "none of the rationales supporting the border search exception justifies applying it to searches of digital information contained on a traveler's cell phone, and the magnitude of the privacy invasion . . . dwarfs that historically posed by border searches and would allow the Government to extend its border search authority well beyond the border itself"). Requiring a warrant is reasonable, in short, because "[w]ith all they contain and all they may reveal, [cellphones] hold for many Americans the privacies of life." *Riley*, 573 U.S. at 403 (internal quotation marks omitted). The government will be able to search electronic devices at the border as long as it has good enough reasons for doing so, and "recent technological advances . . . have . . . made the process of obtaining a warrant . . . more efficient." *Id.* at 401.

Rather than take seriously the balancing of interests that *Riley* requires, the government tries to take a shortcut by claiming that manual searches of cellphones at the border are "routine" and thus require no suspicion at all. The government is correct that "a suspicionless search at the border is permissible under the Fourth Amendment so long as it is considered to be routine." *Tabbaa v. Chertoff*, 509 F.3d 89, 98 (2d Cir. 2007) (internal quotation marks omitted). But the question of whether a new type of search is routine requires the very balancing of interests the

government seeks to avoid. *Id.* (noting that "[t]he determining factor" in judging whether a search is routine "is the level of intrusion into a person's privacy" (internal quotation marks omitted)); *see also United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006) ("Routine searches include those searches of outer clothing, luggage, a purse, wallet, pockets, or shoes which, unlike strip searches, do not substantially infringe on a traveler's privacy rights.").

The government also focuses on the "cursory, manual nature" of the search of Mr. Sultanov's phone, contrasting it with the more extensive search in *Smith*. *See* Dkt. 27 at 4; Dkt. 30 at 3.[22] But the searches in *Riley* and its companion case, *United States v. Wurie*, were also manual and no more detailed than the search at issue here. In *Riley*, the police conducted a brief search of the defendant's smartphone at the scene of his arrest, and a subsequent search of the phone at the police station. *Riley,* 573 U.S. at 378–79. And in *Wurie*, the police seized and later searched the defendant's less sophisticated flip phone, during which they flipped open the phone, looked at the screen, and pressed a few buttons to access the call log and look up a phone number. *Id.* at 380–81. The manual search of Mr. Sultanov's cellphone was as intrusive as, or more so than, the manual searches of the smartphone in *Riley* and the flip phone in *Wurie*.[23] The point, in either case, is that whatever voluntary restraint the government exercised, the Constitution "does not leave us at the mercy of *noblesse oblige*." *United States v. Stevens*, 559 U.S. 460, 480 (2010).

[22] In an earlier case that involved the manual search of a cellphone at the border, Judge Rakoff rejected the government's argument that it "has blanket authority to search cellphones" at the border, and held that, for the reasons stated in *Riley*, such searches require a warrant. *United States v. Booth*, 583 F.Supp.3d 545, 554 (S.D.N.Y. 2022).

[23] None of the post-*Riley* cases the government cites as permitting warrantless manual cellphone searches at the border acknowledges, much less takes account of the manual nature of the cellphone searches in *Riley*. Dkt. 22 at 19-21; Dkt. 27 at 4. One case the government cites—from this District—even mistakenly describes the searches in *Riley* as involving "download[ed] data from defendant's phone." *United States v. Oladokun*, No. 15 Cr. 559, 2016 WL 4033166, at *7 (E.D.N.Y. July 27, 2016).

4. The First Amendment implications of electronic device searches at the border require scrupulous adherence to the Fourth Amendment's warrant requirement.

The Fourth Amendment requires "scrupulous" adherence to the warrant requirement where expressive values are also at risk. *Zurcher*, 436 U.S. at 564 (quoting *Stanford*, 379 U.S. at 485); *see also United States v. Kelly*, 529 F.2d 1365, 1372 (8th Cir. 1976) ("[I]n the absence of exigent circumstances in which police must act immediately to preserve evidence of the crime, we deem the warrantless seizure of materials protected by the First Amendment to be unreasonable."). So too here, where permitting border agents to intrude on First Amendment interests without judicial oversight would have grave consequences for freedom of the press, free speech, and free association.

From the outset, the Fourth Amendment's protections have been understood as safeguards for free expression and the free press in particular. Just as "Founding-era Americans understood the freedom of the press to include the right of printers and publishers not to be compelled to disclose the authors of anonymous works," *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2390 (2021) (Thomas, J., concurring) (citation and internal quotation marks omitted), the prohibition on unreasonable searches was widely understood as a response to abusive English practices targeting dissident publishers, *see Stanford*, 379 U.S. at 482. As the Supreme Court has observed, two of the landmark cases that informed the Fourth Amendment's adoption—*Entick v. Carrington*, 19 How. St. Tr. 1029 (C.P. 1765), and *Wilkes v. Wood*, 19 How. St. Tr. 1153 (C.P. 1763)—were press cases. And whether a particular case involves the institutional press or not, the insight that a "discretionary power given to messengers to search wherever their suspicions may chance to fall" is "totally subversive of the liberty of the subject" continues to inform the best

reading of the Fourth Amendment today. *Marcus v. Search Warrants*, 367 U.S. 717, 728–29 (1961) (quoting *Wilkes*, 19 How. St. Tr. at 1167).

Recognizing that connection, 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*, 436 U.S. at 564 (quoting *Stanford*, 379 U.S. at 485). And for just that reason, "[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." *Id.* (quoting *Roaden v. Kentucky*, 413 U.S. 496, 501 (1973)). The same is true here: Whatever the merits of the border search exception in its traditional sweep, *see United States v. Aigbekaen*, 943 F.3d 713, 727 (4th Cir. 2019) (Richardson, J., concurring in the judgement) (noting that "more recent historical work" has cast doubt on its pedigree), it cannot reasonably be extended to the digital equivalent of a traveler's "papers," U.S. Const. amend. IV; *see also Smith*, 2023 WL 3358357, at *7 n.7 (noting that there is no Founding-era evidence of the application of the border search exception to "a person's papers").

The rule governing searches of these kinds must be framed with the care the Supreme Court has required where the government's discretion could, if left unregulated, be abused to tread on First Amendment interests. A warrant, and nothing short of it, is necessary to safeguard the newsgathering activities of journalists and the speech and associational rights of travelers. "No less a standard could be faithful to First Amendment freedoms." *Stanford*, 379 U.S. at 485.

B. Warrantless searches of electronic devices at the border violate the First Amendment.

1. Searches of electronic devices at the border trigger First Amendment scrutiny.

The First Amendment stands as an independent source of protection, separate and apart from the Fourth Amendment, against the search and seizure of travelers' and journalists' devices at the border. *See Tabbaa*, 509 F.3d at 101–07 (independently evaluating whether border searches at issue violated the First Amendment after concluding they did not violate the Fourth Amendment); *Alasaad*, 988 F.3d at 22 ("The First Amendment provides protections—independent of the Fourth Amendment—against the compelled disclosure of expressive information."); *see also Nieves v. Bartlett*, 139 S. Ct. 1715, 1731 (2019) (Gorsuch, J., concurring in part and dissenting in part) ("[T]he First Amendment operates independently of the Fourth and provides different protections.").

The distinction between First and Fourth Amendment protections has been clear since the Supreme Court first articulated the "border search" exception to the Fourth Amendment's warrant requirement in *United States v. Ramsey*, 431 U.S. 606 (1977). *Ramsey* involved a search of incoming international mail 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; it upheld the search only after concluding that any such chill would be "minimal," given that the statute at issue prohibited the opening of envelopes absent reasonable suspicion and that the "[a]pplicable postal regulations flatly prohibit, under all circumstances, the reading of correspondence absent a search warrant." *Id.* at 623–24 (citation omitted). In other words, the Court made clear that the inspection of expressive content at the border raises independent First Amendment concerns.

In *New York v. P.J. Video, Inc.*, 475 U.S. 868 (1986), the Court again highlighted independent 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.* at 873. The Court made 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, including where Fourth Amendment "exception[s]" like exigent circumstances would ordinarily allow law enforcement to seize material without a warrant. *Id.* at 873, 875 n.6 (discussing *Roaden v. Kentucky*, 413 U.S. 496 (1973)).[24]

More recent cases, too, highlight the Court's special concern for searches—especially warrantless ones—that burden expressive activities. Ordinarily, for instance, the Court has held that an individual has a lesser expectation of privacy in information voluntarily provided to third parties. *See Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). But in *Carpenter*, the Court rejected the extension of the third-party doctrine to cell-site location records because of "the seismic shifts in digital technology" that made possible "the exhaustive chronicle of location information casually collected by wireless carriers today," which could "provide[] an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political,

[24] Some courts have interpreted *P.J. Video* as suggesting that the First Amendment provides no independent protection against the search and seizure of expressive material because the case held that the First Amendment did not require a "higher" standard of probable cause for the seizure of allegedly obscene material. *See, e.g.*, *United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005). But those courts were incorrect to mistake the Supreme Court's narrow holding about the probable cause standard for a broad decision limiting the First Amendment's applicability to searches of expressive material.

professional, religious, and sexual associations.'" 138 S. Ct. at 2217, 2219 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

Similarly, as noted above, the Court held in *Riley* that the search incident to arrest exception to the warrant requirement did not extend to searches of cell phones, explaining that 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. 573 U.S. at 393. 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 393–94. And 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 device's purchase. *See id.* at 395–96.[25] Courts must therefore take into account the unique ability of electronic devices to store and transmit vast quantities of protected expressive and journalistic material by applying the First Amendment's requirements to device searches at the border.

[25] As is clear from these cases, "[g]overnment action can constitute a direct and substantial interference with [expressive or] associational rights even if there is no prior restraint and no clear chilling of future expressive activity." *Tabbaa*, 509 F.3d at 101–02 (attendees of Islamic conference in Toronto, Canada "suffered a significant penalty, or disability, solely by virtue of associating at the . . . Conference," because, upon trying to cross the border into the United States, "they were detained for a lengthy period of time, interrogated, fingerprinted, and photographed when others, who had not attended the conference, did not have to endure these measures").

2. Warrantless device searches do not survive any form of heightened scrutiny.

Applying the First Amendment's independent guarantees in light of these cases, it is clear that warrantless searches of electronic devices, like those at issue in this case, demand close scrutiny. Part I, *supra*, demonstrates the First Amendment interests at stake when the government conducts even basic device searches at the border. Because this kind of "[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 careful review. Under any level of First Amendment scrutiny, warrantless searches of electronic devices at the border violate the First Amendment.

The Supreme Court has long applied some form of heightened scrutiny to the forced disclosure of personal beliefs and private associations. 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 *Americans for Prosperity Foundation v. Bonta*, the Court held that compelled disclosure of association must be subjected to exacting scrutiny, "whether the beliefs sought to be advanced by association pertain to political, economic, religious or cultural matters." 141 S. Ct. at 2383 (quoting *NAACP v. Alabama ex rel. Patterson,* 357 U.S. 449, 460–61 (1958)). As the Court explained, "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." *Id.* at 2382 (quoting *NAACP*, 357 U.S. 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 to burdens on the right to anonymity. *Id.* at 347 (citation omitted) (forced identification of pamphleteer unconstitutional).

The First Amendment concerns with unmasking anonymous speakers are especially acute when those speakers are reporters' confidential sources, because their exposure threatens the ability of reporters to gather and report the news. *See Zerilli*, 656 F.2d at 710–11 ("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."). As noted above, 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," warrantless 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," *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); *cf. Gibson v. Fla. Legis. Investigation Comm.*, 372 U.S. 539, 546 (1963) (requiring legislature to "convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest" in justifying demand for organization's membership list). It cannot do so here.

First, warrantless searches of electronic devices at the border fail to satisfy the "narrow tailoring" requirement. In *Riley*, the Court rejected the government's contention that searches of cell phones incident to arrest were constitutional if officers had a reasonable suspicion that they would uncover "information relevant to the crime, the arrestee's identity, or officer safety." 573 U.S. at 399. The Court explained that the reasonable suspicion standard was not enough because such searches "would sweep in a great deal of information, and officers would not always be able to discern in advance what information would be found where." *Id.* Here, too, even if officers searched devices only when they had a reasonable suspicion that the devices contained contraband, the searches "would sweep in a great deal of information" unrelated to that interest, much of it expressive. *Id.*

While the First Circuit rejected a facial First Amendment challenge to the government's electronic device search policies in *Alasaad v. Mayorkas*, its analysis was flawed. There, the court held that the government's policies had "a plainly legitimate sweep" and "serve[d] the government's paramount interests in protecting the border." *Alasaad*, 988 F.3d at 22. But it failed to reckon with the massive amount of expressive information swept up in electronic device searches, and it failed to ask whether the searches could be narrowed or constrained while still serving the government's interests. As *Riley* made clear, courts must consider the consequences of electronic device searches on free expression, especially when obtaining a warrant is an available alternative. 573 U.S. at 401–03.

In addition, the harm from the government's policies extends far beyond those travelers whose devices have been searched. The knowledge that the content of their devices may be searched without a warrant has a chilling effect on the expressive activities of all travelers, who may refrain from using their devices for expressive and associational purposes for fear that their

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"). Warrantless electronic device searches thus threaten to chill the speech of every traveler and journalist.

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 communication channels 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*, 573 U.S. at 393 (describing "qualitative" and "quantitative" differences in the storage, communicative capacity, and pervasiveness of cell phones compared to pre-digital objects); Part I.A, supra (describing journalists' dependence on electronic devices to gather and disseminate news). The government's claim that it may search the contents of literally every device crossing the border without ever once obtaining a warrant leaves no realistic alternative for travelers or journalists hoping to safeguard the confidentiality of their communications. These searches are therefore entirely inconsistent with the requirements of the First Amendment.

CONCLUSION

For the foregoing reasons, the Court should hold that the government's search of Mr. Sultanov's cellphone violated the First and Fourth Amendments.

Dated: October 3, 2023

Respectfully submitted,

/s/ Scott B. Wilkens

Bruce D. Brown
Gabriel Rottman
Grayson Clary
Reporters Committee for Freedom
of the Press
1156 15th St. NW, Suite 1020
Washington, D.C. 20005
T: (202) 795-9300
F: (202) 795-9310

Scott B. Wilkens
Alex Abdo
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
T: (646) 745-8500
F: (646) 661-3361
scott.wilkens@knightcolumbia.org

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I, Scott B. Wilkens, do hereby certify that I have filed the foregoing Brief of Amici Curiae electronically with the Clerk of the Court for the United States District Court for the Eastern District of New York using the CM/ECF system on October 3, 2023. All participants in the case are registered CM/ECF users, and service will be accomplished by the CM/ECF system.

Dated: October 3, 2023

/s/ Scott B. Wilkens

Scott B. Wilkens
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
T: (646) 745-8500
F: (646) 661-3361
scott.wilkens@knightcolumbia.org