

United States v. Kolsuz

United States Court of Appeals for the Fourth Circuit

October 26, 2017, Argued; May 9, 2018, Decided

No. 16-4687

Reporter

890 F.3d 133 *; 2018 U.S. App. LEXIS 12147 **

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. HAMZA KOLSUZ, Defendant-Appellant.

Subsequent History: Amended: May 18, 2018.

Prior History: **[**1]** Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria. (1:16-cr-00053-TSE-1). T.S. Ellis, III, Senior District Judge.

[United States v. Kolsuz, 185 F. Supp. 3d 843, 2016 U.S. Dist. LEXIS 60538 \(E.D. Va., May 5, 2016\)](#)

Disposition: AFFIRMED.

Core Terms

border, border search, phone, searches, forensic, nonroutine, district court, cell phone, firearms, export, reasonable suspicion, digital, privacy, manual, contraband, individualized suspicion, arrest, routine, courts, airport, devices, license, probable cause, intrusive, luggage, forensic analysis, traveler, requirements, smuggle, forensic examination

Case Summary

Overview

HOLDINGS: [1]-Despite the temporal and spatial distance between the off-site forensic analysis of defendant's phone and defendant's attempted departure at the airport, the justification for the border exception to the *Fourth Amendment* warrant requirement was broad enough to reach the search of the phone; [2]-There was a direct link between the predicate for the search and the rationale for the border exception. Because the forensic search of defendant's phone was conducted in part to uncover information about an ongoing crime of illegal firearms exports, it fit within the core of the rationale underlying the border search exception; [3]-It was reasonable for the officers who conducted the forensic analysis of the phone to rely on the established and uniform body of precedent allowing warrantless border searches of digital devices that were based on at least reasonable suspicion.

Outcome

Judgment affirmed.

LexisNexis® Headnotes

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Probable Cause

Criminal Law & Procedure > Search & Seizure > Warrantless Searches > Border Searches

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

[HN1](#) [↓] **Search & Seizure, Probable Cause**

As a general rule, the *Fourth Amendment* requires that law enforcement searches be accompanied by a warrant based on probable cause. But there are exceptions, and one such exception typically covers our nation's borders. At a border — or at a border's "functional equivalent" — government agents may conduct "routine" searches and seizures of persons and property without a warrant or any individualized suspicion. The U.S. Supreme Court has described the border exception as grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country. Routine searches and seizures at the border therefore are exempted from standard *Fourth Amendment* requirements so that the government can prevent the introduction of contraband into the country and bar entry by those who would bring harm across the border, whether that be communicable diseases, narcotics, or explosives.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

Criminal Law & Procedure > Search & Seizure > Warrantless Searches > Border Searches

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

[HN2](#) [↓] **Search & Seizure, Scope of Protection**

The rationales underlying the border exception to the warrant requirement extend to exit as well as entry searches. The fundamental principles of national sovereignty that are the basis for the border search exception apply equally to government efforts to protect and monitor exports from the country as they do to efforts to control imports. Thus, with respect to exit searches, the border search exception is justified by the government's power to regulate the export of currency and other goods. And that power surely extends to controls on the exports of dangerous weapons. Even at the border, however, the government's authority is not without limits. The "ultimate touchstone" of the *Fourth Amendment* remains "reasonableness." While suspicionless border searches generally are reasonable simply by virtue of the fact that they occur at the border, the U.S. Supreme Court also has recognized a category of "nonroutine" border searches that are constitutionally reasonable only if based on individualized suspicion. Such nonroutine border searches, the Court has suggested, include highly intrusive searches that implicate especially significant dignity and privacy interests, as well as destructive searches of property and searches carried out in particularly offensive manners.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

[HN3](#) [↓] **Search & Seizure, Scope of Protection**

The *Fourth Amendment* protects property as well as privacy, and a seizure reasonable at its inception must remain reasonable in scope and duration to satisfy the *Fourth Amendment*.

Criminal Law & Procedure > ... > Standards of Review > De Novo Review > Conclusions of Law

Criminal Law & Procedure > ... > Standards of Review > Clearly Erroneous Review > Findings of Fact

Criminal Law & Procedure > ... > Standards of Review > Clearly Erroneous Review > Motions to Suppress

Criminal Law & Procedure > ... > Standards of Review > De Novo Review > Motions to Suppress

[HN4](#) [↓] **De Novo Review, Conclusions of Law**

In considering the district court's denial of a motion to suppress, the United States Court of Appeals for the Fourth Circuit reviews that court's legal conclusions de novo and its factual findings for clear error, considering the evidence in the light most favorable to the government.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

Criminal Law & Procedure > Search & Seizure > Warrantless Searches > Border Searches

[HN5](#) [↓] **Search & Seizure, Scope of Protection**

The border exception to the warrant requirement is not rendered inapplicable because a search initiated at a border ultimately is conducted at some physical or temporal remove.

Constitutional Law > ... > Fundamental

Rights > Search & Seizure > Scope of Protection

Criminal Law & Procedure > Search & Seizure > Warrantless Searches > Border Searches

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Warrantless Searches

[HN6](#) [↓] **Search & Seizure, Scope of Protection**

As a general rule, the scope of a warrant exception should be defined by its justifications. As a result, where the government interests underlying a *Fourth Amendment* exception are not implicated by a certain type of search, and where the individual's privacy interests outweigh any ancillary governmental interests, the government must obtain a warrant based on probable cause. At some point, in other words, even a search initiated at the border could become so attenuated from the rationale for the border search exception that it no longer would fall under that exception.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

Criminal Law & Procedure > Search & Seizure > Warrantless Searches > Border Searches

[HN7](#) [↓] **Search & Seizure, Scope of Protection**

The justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the border, but also the prevention and disruption of ongoing efforts to export

contraband illegally, through searches initiated at the border.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

Criminal Law & Procedure > Search & Seizure > Warrantless Searches > Border Searches

[HN8](#) [↓] **Search & Seizure, Scope of Protection**

A forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

Criminal Law & Procedure > Search & Seizure > Warrantless Searches > Border Searches

[HN9](#) [↓] **Search & Seizure, Scope of Protection**

In deciding whether a border search rises to the level of nonroutine, courts have focused primarily on how deeply it intrudes into a person's privacy. Under that approach, border searches of luggage, outer clothing, and personal effects consistently are treated as routine, while searches that are most invasive of privacy — strip searches, alimentary-canal searches, x-rays, and the like — are deemed nonroutine and permitted only with reasonable suspicion.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of

Protection

Criminal Law & Procedure > Search & Seizure > Warrantless Searches > Border Searches

[HN10](#) [↓] **Search & Seizure, Scope of Protection**

Nonroutine searches are permitted under the border exception, so long as they are accompanied by the appropriate level of individualized suspicion.

Counsel: ARGUED: Todd M. Richman, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Alexandria, Virginia, for Appellant.

Jeffrey Michael Smith, National Security Division, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee.

Esha Bhandari, AMERICAN CIVIL LIBERTIES UNION, New York, New York, for Amici American Civil Liberties Union, ACLU of Virginia, ACLU of Maryland, ACLU of North Carolina, ACLU of South Carolina, and ACLU of West Virginia.

ON BRIEF: Jeremy C. Kamens, Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Alexandria, Virginia, for Appellant.

Dana Boente, United States Attorney, Mary B. McCord, Acting Assistant Attorney General for National Security, Heather Alpino, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee.

Hope R. Amezquita, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA, Richmond, Virginia, Nathan Freed Wessler, Vera Eidelman, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, for Amici American Civil Liberties Union, ACLU of Virginia, ACLU of Maryland, **[**2]** ACLU of North Carolina,

ACLU of South Carolina, and ACLU of West Virginia.

Curt Levey, THE COMMITTEE FOR JUSTICE, Washington, D.C., Erica L. Marshall, CAUSE OF ACTION INSTITUTE, Washington, D.C., for Amici Cause of Action Institute, The Committee for Justice, and Floor64, Inc. Sophia Cope, Adam Schwartz, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, for Amici Electronic Frontier Foundation, Asian Americans Advancing Justice-Asian Law Caucus, Council on American-Islamic Relations (CAIR), CAIR California, CAIR Florida, CAIR Missouri, CAIR New York, CAIR Ohio, CAIR Dallas/Fort Worth, and The National Association of Criminal Defense Lawyers.

Michael Price, BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW, New York, New York, for Amicus Brennan Center for Justice.

Judges: Before WILKINSON, MOTZ, and HARRIS, Circuit Judges. Judge Harris wrote the opinion, in which Judge Motz joined. Judge Wilkinson wrote a separate opinion concurring in the judgment.

Opinion by: PAMELA HARRIS

Opinion

[*136] PAMELA HARRIS, Circuit Judge:

Hamza Kolsuz was detained at Washington Dulles International Airport while attempting to board a flight to Turkey because federal customs agents found firearms parts in his luggage. After arresting Kolsuz, **[**3]** the agents took possession of his smartphone and subjected it to a month-long, off-site forensic analysis, yielding a nearly 900-page report cataloguing the phone's data. The district court denied Kolsuz's motion to suppress, applying the *Fourth Amendment's* border search

exception and holding that the forensic examination was a nonroutine border search justified by reasonable suspicion. Kolsuz ultimately was convicted of attempting to smuggle firearms out of the country and an associated conspiracy charge.

Kolsuz now challenges the denial of his suppression motion. First, he argues that the forensic analysis of his phone should not have been treated as a border search at all. According to Kolsuz, once both he and his phone were in government custody, the government interest in preventing **[*137]** contraband from crossing the border was no longer implicated, so the border exception should no longer apply. Second, relying chiefly on [*Riley v. California*, 134 S. Ct. 2473, 189 L. Ed. 2d 430 \(2014\)](#) (holding that search incident to arrest exception does not apply to searches of cell phones), Kolsuz urges that the privacy interest in smartphone data is so weighty that even under the border exception, a forensic search of a phone requires more than reasonable suspicion, and instead **[**4]** may be conducted only with a warrant based on probable cause.

We agree with the district court that the forensic analysis of Kolsuz's phone is properly categorized as a border search. Despite the temporal and spatial distance between the off-site analysis of the phone and Kolsuz's attempted departure at the airport, the justification for the border exception is broad enough to reach the search in this case. We also agree with the district court that under *Riley*, the forensic examination of Kolsuz's phone must be considered a nonroutine border search, requiring some measure of individualized suspicion. What precisely that standard should be — whether reasonable suspicion is enough, as the district court concluded, or whether there must be a warrant based on probable cause, as Kolsuz suggests — is a question we need not resolve: Because

the agents who conducted the search reasonably relied on precedent holding that no warrant was required, suppression of the report would be inappropriate even if we disagreed. Accordingly, we affirm the judgment of the district court.

I.

A.

We begin with the *Fourth Amendment* principles that govern this case. [HN1](#)^[↑] As a general rule, the *Fourth Amendment* requires that law enforcement searches [**5](#) be accompanied by a warrant based on probable cause. [Arizona v. Gant, 556 U.S. 332, 338, 129 S. Ct. 1710, 173 L. Ed. 2d 485 \(2009\)](#). But there are exceptions, and one such exception typically covers our nation's borders. At a border — or at a border's "functional equivalent," like the international airport at which Kolsuz was intercepted — government agents may conduct "routine" searches and seizures of persons and property without a warrant or any individualized suspicion. [Almeida-Sanchez v. United States, 413 U.S. 266, 272-73, 93 S. Ct. 2535, 37 L. Ed. 2d 596 \(1973\)](#); [United States v. Montoya de Hernandez, 473 U.S. 531, 538, 105 S. Ct. 3304, 87 L. Ed. 2d 381 \(1985\)](#). The Supreme Court has described the border exception as "grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." [United States v. Ramsey, 431 U.S. 606, 620, 97 S. Ct. 1972, 52 L. Ed. 2d 617 \(1977\)](#); see [United States v. Flores-Montano, 541 U.S. 149, 152, 124 S. Ct. 1582, 158 L. Ed. 2d 311 \(2004\)](#) (border exception rests on government interest in "preventing the entry of unwanted persons and effects"). Routine searches and seizures at the border therefore are exempted from standard

Fourth Amendment requirements so that the government can "prevent the introduction of contraband" into the country and bar entry by those who would bring harm across the border, "whether that be communicable diseases, narcotics, or explosives." [Montoya de Hernandez, 473 U.S. at 537, 544](#).

In this case, the search in question was initiated when Kolsuz attempted to exit the country, not to enter. But we have long held that [HN2](#)^[↑] the rationales [**6](#) underlying the border exception extend to exit as well as entry searches. See [United States \[*138\] v. Oriakhi, 57 F.3d 1290, 1296-97 \(4th Cir. 1995\)](#). The "fundamental principles of national sovereignty" that are the basis for the border search exception, we have explained, apply equally to government efforts to "protect[] and monitor[] exports from the country" as they do to efforts to control imports. [Id. at 1296, 1297](#). Thus, with respect to exit searches, the border search exception is justified by the government's power to regulate the export of currency and other goods. [Id. at 1297](#). And that power surely extends to controls on the exports of dangerous weapons, like the firearms parts at issue here. See, e.g., [United States v. Boumelhem, 339 F.3d 414, 422-23 \(6th Cir. 2003\)](#) (applying border exception to exit search of shipping container believed to hold smuggled firearms).

Even at the border, however, the government's authority is not without limits. The "ultimate touchstone" of the *Fourth Amendment*, [Riley, 134 S. Ct. at 2482](#), remains "reasonableness." See [Montoya de Hernandez, 473 U.S. at 538](#). While suspicionless border searches generally are "reasonable simply by virtue of the fact that they occur at the border," [Ramsey, 431 U.S. at 616](#), the Supreme Court also has recognized a category of "nonroutine" border searches that are constitutionally reasonable only if based on individualized suspicion. See [Montoya de Hernandez, 473 U.S. at 541](#) (holding that overnight detention for [**7](#) monitored bowel

movement followed by rectal examination is "beyond the scope of a routine customs search" and permissible under the border exception only with reasonable suspicion). Such nonroutine border searches, the Court has suggested, include "highly intrusive searches" that implicate especially significant "dignity and privacy interests," as well as destructive searches of property and searches carried out in "particularly offensive" manners. [Flores-Montano, 541 U.S. at 152, 154 & n.2.](#)

B.

In January 2016, Turkish citizen Hamza Kolsuz entered the United States in Miami, Florida, on a tourist visa. By that time, Kolsuz already was well known to government authorities. In December 2012, agents had discovered 163 firearms parts in his luggage when Kolsuz checked in for a flight to Turkey at John F. Kennedy International Airport in New York. The parts were listed on the United States Munitions List ("USML"), subjecting them to export controls and a license requirement under the [Arms Export Control Act, 22 U.S.C. § 2778\(b\)\(2\)](#). See [22 C.F.R. §§ 120.2, 121.1](#) (setting out USML, and defining "defense articles and defense services" subject to control under the Act). Agents explained the licensing requirements to Kolsuz and his companions, and ultimately seized the weapons **[**8]** parts. Just one month later, in January 2013, the process more or less repeated itself: Kolsuz arrived at JFK Airport for a flight to Turkey; a search of his checked luggage revealed firearms parts; and a licensing determination disclosed that although the parts were listed on the USML, Kolsuz had not obtained the requisite export license.

When Kolsuz reentered the country on January 25, 2016, the authorities were ready for him. On February 1, 2016, Charles Reich, a Special Agent with United States Customs and Border Protection ("CBP") in New York, reached out to CBP officers on duty at Washington Dulles International Airport ("Dulles") to let them know that Kolsuz, who had been stopped before while attempting to smuggle firearms parts out of the country, would be traveling from Dulles to Turkey the following **[*139]** day. Agent Reich urged the officers to search Kolsuz's luggage for firearms parts, and followed up with an email containing additional information and a list of questions to ask Kolsuz about his associates and activities.

On February 2, 2016, Kolsuz began his return trip by checking in at Miami International Airport for a series of flights that would take him through Dulles and **[**9]** on to Turkey. When Kolsuz and his luggage reached Dulles, CBP officers Lauren Colgan and Jonathan Budd conducted an outbound customs examination of his two checked bags.¹ Once again, they found multiple firearms parts: 18 handgun barrels, 22 9mm handgun magazines, four .45 caliber handgun magazines, and one .22 caliber conversion kit. Colgan and Budd, thanks to their training, immediately recognized that the barrels and conversion kit were listed on the USML and thus could not be removed from the country without a license. And when Kolsuz was stopped on the jetway as he attempted to board his flight to Turkey, he admitted that he was in possession of firearms parts for which he did not have a federal license.

After transporting Kolsuz to a secondary inspection area, the officers conducted what would be the first of two searches of Kolsuz's

¹ Kolsuz never has suggested that this standard customs search of his checked luggage presents any constitutional problem. Nor could he: It is long established that a search of luggage taken from or bound for an overseas flight is a routine

border search that may be conducted on a suspicionless basis. See [Montoya de Hernandez, 473 U.S. at 538](#); see also, e.g., [United States v. Ezeiruaku, 936 F.2d 136, 140-41 \(3d Cir. 1991\)](#).

iPhone 6 Plus. This search — often referred to as a "manual" search — involved using the iPhone's touch screen, which was not password protected, to scroll through Kolsuz's recent calls and text messages. The officers also confirmed through a records search that Kolsuz had no export license or pending application for a license. **[**10]** After an interview with a number of CBP officers, Kolsuz was arrested.

At that point, CBP Special Agent Adam Coppolo initiated the second search of Kolsuz's phone, this one commonly known as a "forensic" search. Coppolo first transported the phone approximately four miles from Dulles to the Homeland Security Investigations office in Sterling, Virginia. There, Computer Forensic Agent Michael Del Vacchio attached the phone to a Cellebrite Physical Analyzer, which extracts data from electronic devices, and conducted an advanced logical file system extraction. The phone remained in airplane mode throughout, so the forensic examination did not reach data stored remotely — or "in the cloud" — and was instead limited to data stored on the phone itself. Even so, the data extraction process lasted for a full month, and yielded an 896-page report that included Kolsuz's personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates.

C.

Kolsuz was indicted on three counts: (i) attempting to export firearms parts on the USML without a license, in violation **[**11]** of the [Arms Export Control Act](#), [22 U.S.C. §§ 2778\(b\)](#) and (c); (ii) attempting to smuggle goods from the United States in violation of [18 U.S.C. § 554\(a\)](#); and (iii) conspiracy to commit those offenses, in violation of [18 U.S.C. § 371](#).

Before trial, Kolsuz filed a motion to suppress

the report generated by the forensic examination of his phone, arguing primarily that the border exception did not apply to the search. According to Kolsuz, a **[*140]** forensic search of a phone that occurs miles away from an airport and for a month after an attempted departure does not constitute a "border search." Moreover, Kolsuz contended, the rationales justifying the border exception were not implicated in this case, because at the time of the search there was no prospect that either he or his phone — both securely in government custody — would be crossing the border. Instead, Kolsuz argued, the forensic search should be treated as a search incident to his arrest, and under *Riley v. California*, cell phones may be searched incident to arrest only with a warrant based on probable cause.

In a comprehensively reasoned opinion, the district court denied Kolsuz's suppression motion. [United States v. Kolsuz](#), [185 F. Supp. 3d 843, 860 \(E.D. Va. 2016\)](#). The court held first that the forensic search of Kolsuz's phone was properly evaluated **[**12]** as a border search. That Kolsuz had been arrested, the district court explained, did not transform the forensic examination into a search incident to arrest or render the border exception inapplicable; both the Fourth Circuit and other courts have held that a border search may be conducted after a traveler is arrested and no longer in a position to cross the border. [Id. at 851](#) (citing [United States v. Ickes](#), [393 F.3d 501, 507 \(4th Cir. 2005\)](#)). Similarly, the court found, it is well established that a search initiated at the border may fall under the border exception even if it ultimately is conducted off-site and over a long period of time. [Id. at 851-52](#).

Now applying the border exception, the district court went on to consider whether the forensic search of Kolsuz's smartphone was a routine border search, subject to no *Fourth Amendment* requirements, or whether, as Kolsuz urged, it was a nonroutine search that required some

degree of individualized suspicion. The court acknowledged that in *Ickes*, the Fourth Circuit treated as routine a border inspection of a computer's contents, accessed manually "in the same way a typical user would" and without any "sophisticated forensic analysis." *Id. at 853* (citing *Ickes*, *393 F.3d at 502-03*). But that decision, the court determined, "does not address whether more sophisticated **[**13]** forensic searches" also may be classified as routine, *id. at 854*, particularly in light of the Supreme Court's subsequent decision in *Riley* and its emphasis on the significant privacy interests in the digital contents of phones.

The court concluded that while the manual search of Kolsuz's iPhone at the airport was a routine border search,² the off-site forensic analysis of the phone's data qualified as a nonroutine search. After *Riley*, the court found, a forensic search of a phone no longer can be analogized to an ordinary search of luggage or some other container at the border, given the breadth and sensitivity of the private information that may be uncovered. It is "difficult to conceive of a property search more invasive or intrusive than a sophisticated, digital search of a cell phone," the court concluded, which might be compared to a "body cavity search" of a phone. *Id. at 856* (quoting *United States v. Saboonchi*, *990 F. Supp. 2d 536, 569 (D. Md. 2014)*).

As a nonroutine border search, the court went on to hold, the forensic analysis of Kolsuz's phone required particularized suspicion, in the form of the familiar reasonable suspicion standard. The court rejected the more demanding requirement of a

warrant **[*141]** based on probable cause, noting that no reported case has held **[**14]** a border search to that standard. Instead, courts consistently have deemed reasonable suspicion sufficient to justify even the most intrusive of nonroutine border searches, including body cavity and alimentary canal searches. Because the government in this case had "more than reasonable suspicion" that a forensic examination of Kolsuz's phone would reveal evidence of both past and ongoing attempts to export firearms parts illegally, the court concluded, the forensic search was reasonable under the *Fourth Amendment*. *Id. at 859, 860*.

The parties consented to a bench trial, and the district court found Kolsuz guilty of all three counts against him. In finding that Kolsuz acted with the requisite willfulness, the court relied in part on messages Kolsuz exchanged with a co-conspirator, obtained from the forensic search of Kolsuz's phone.³ The court ultimately entered judgment only on the *Arms Export Control Act* and conspiracy counts against Kolsuz, dismissing the smuggling charge on the government's motion. Kolsuz was sentenced to 30 months in prison and three years of supervised release, and this timely appeal followed.

II.

Kolsuz's appeal is a narrow one, and we begin by clarifying what is and is not in front of us today. **[**15]** First, Kolsuz does not challenge the manual search of his smartphone, undertaken on-site at the airport as he tried to

²Although the district court addressed this initial search in the course of its reasoning, Kolsuz's suppression motion is limited to the subsequent forensic examination. On appeal, Kolsuz expressly disclaims any challenge to the manual search of his phone at Dulles, which in any event did not reveal information used against him at trial.

³The court also adopted an independent willful blindness

theory, under which it was "unnecessary to rely" on the messages recovered from Kolsuz's phone. J.A. 243 n.34. As the government recognizes, however, that theory does not apply to the conspiracy charge of which Kolsuz was convicted, and thus does not provide an alternative basis for affirming the district court judgment in full.

depart for Turkey. We thus have no occasion to consider application of the border exception to manual searches of electronic devices, conducted at the border and roughly contemporaneously with an attempted crossing. Cf. [United States v. Molina-Isidoro](#), [884 F.3d 287, 289 \(5th Cir. 2018\)](#) (sustaining manual search of phone at border under good-faith exception to *Fourth Amendment* exclusionary rule).

Nor does Kolsuz challenge the seizure of his phone, either initially at the airport or later at the Homeland Security Investigations office where it was forensically examined. [HN3](#) The *Fourth Amendment* protects property as well as privacy, see [Flores-Montano](#), [541 U.S. at 154](#), and a seizure reasonable at its inception must remain reasonable in scope and duration to satisfy the *Fourth Amendment*, see [Montoya de Hernandez](#), [473 U.S. at 541-42](#). But perhaps because he was in custody while the government undertook its month-long forensic analysis, Kolsuz has not asserted any impairment of a possessory interest in his phone. Accordingly, we do not address whether and under what circumstances an extended confiscation of a traveler's phone — quite apart from any search undertaken — might constitute an unreasonable seizure of property for *Fourth Amendment* purposes. Cf. [Saboonchi](#), [990 F. Supp. 2d at 569](#) (noting that forensic [**16](#) searches of digital devices may deprive individuals of their possessions for periods of days or weeks).

That leaves the question that *is* raised by this appeal: whether the forensic search of Kolsuz's phone, and the associated invasion of Kolsuz's privacy, was justified under the border search exception. [HN4](#) In considering the district court's denial of Kolsuz's motion to suppress, we review [*142](#) that court's legal conclusions de novo and its factual findings for clear error, considering the evidence in the light most favorable to the government. See [United States](#)

[v. Palmer](#), [820 F.3d 640, 648 \(4th Cir. 2016\)](#). For the reasons given below, we affirm.

A.

Kolsuz's primary argument is that the forensic analysis of his phone was not subject to the border search exception at all. Once he was arrested and his phone seized and transported miles from the airport, Kolsuz contends, the government interest that underlies the border search exception — preventing contraband from crossing a border — was no longer at issue, and the border exception was therefore inapplicable. Rather, standard *Fourth Amendment* rules governed the forensic search, and required a warrant based on probable cause because the search was incident to Kolsuz's arrest. See [Riley](#), [134 S. Ct. at 2485, 2493-94](#) (holding that the search incident exception [**17](#) does not apply to cell phones, which generally may be searched incident to arrest only with probable cause and a warrant). We cannot agree.

First, as the district court explained, [HN5](#) the border exception is not rendered inapplicable because a search initiated at a border ultimately is conducted at some physical or temporal remove. See [Kolsuz](#), [185 F. Supp. 3d at 851-52](#) ("as several courts have held, an off-site forensic search of an electronic device over a long period of time is nonetheless a border search"); see also, e.g., [United States v. Cotterman](#), [709 F.3d 952, 961-62 \(9th Cir. 2013\)](#) (en banc) (applying border exception to forensic examination of laptop computer conducted miles from and days after attempted border crossing); [Saboonchi](#), [990 F. Supp. 2d at 548-49, 561](#) (applying border exception to forensic search of cell phones conducted several hundred miles from border crossing). Indeed, after pressing this point before the district court, Kolsuz concedes it on appeal, agreeing that the location and timing of the

search in this case are consistent with the border search exception.

Nor, as the district court determined, does the fact of Kolsuz's arrest transform the examination of his phone into a search incident to arrest, triggering *Riley* and calling for a search warrant based on probable cause. In *Ickes*, our court **[**18]** applied the border search exception to approve a manual search of computer data that occurred only after the defendant had been arrested, obviating any threat of an imminent border crossing. See [393 F.3d at 503](#); see also, e.g., [United States v. Ramos, 190 F. Supp. 3d 992, 998-1000 \(S.D. Cal. 2016\)](#) (rejecting argument that arrest renders border exception inapplicable by making it impossible for defendant or contraband to cross border). Kolsuz attempts to distinguish *Ickes* on the ground that it involved an entry search rather than the exit search at issue here, but for these purposes, it makes no difference: As we have explained, where the relevant governmental interests are present, the border search exception extends equally to entry and exit searches, see [Oriakhi, 57 F.3d at 1296-97](#), and any rule carving out post-arrest searches from that doctrine would apply equally in both contexts, as well.

In its strongest form, Kolsuz's argument combines all of these factors — his arrest as he sought to depart the country, the phone in government custody miles from the border, the month-long gap between the action at the airport and the end of the search — and argues that taken together, they show that the search in this case is entirely "untethered" from any justification behind the border exception. The **[**19]** rationale **[*143]** allowing outgoing border searches, as Kolsuz describes it, is limited to intercepting contraband as it crosses the national border. Here, with the phone as well as the firearms parts seized by the government and Kolsuz under arrest, there was no contraband poised to exit the country and

thus no nexus to that rationale. When that is the case, Kolsuz argues, the border search exception does not apply, because the concerns underlying a warrant exception "define the boundaries of the exception." See [Gant, 556 U.S. at 339](#).

Kolsuz's foundational premise is correct: [HN6](#) [↑](#) As a general rule, the scope of a warrant exception should be defined by its justifications. See [Riley, 134 S. Ct. at 2484-88](#) (asking whether "application of the search incident to arrest doctrine to this particular category of effects would untether the rule from the justifications underlying the [search incident to arrest] exception"). As a result, where the government interests underlying a *Fourth Amendment* exception are not implicated by a certain type of search, and where the individual's privacy interests outweigh any ancillary governmental interests, the government must obtain a warrant based on probable cause. See *id.* At some point, in other words, even a search initiated at **[**20]** the border could become so attenuated from the rationale for the border search exception that it no longer would fall under that exception. See [Molina-Isidoro, 884 F.3d at 295-97](#) (Costa, J., concurring) (questioning whether search for evidence as opposed to contraband is consistent with justifications for border search exception).

But this is not that case. On the facts here, the link between the search of Kolsuz's phone and the interest that justifies border searches was sufficient to trigger the border exception on any account of a "nexus" requirement. Government agents forensically searched Kolsuz's phone because they had reason to believe — and good reason to believe, in the form of two suitcases filled with firearms parts — that Kolsuz was attempting to export firearms illegally and without a license. See [Kolsuz, 185 F. Supp. 3d at 859-60](#). That is a transnational offense that goes to the heart of the border

search exception, which rests in part on "the sovereign interest of protecting and monitoring exports from the country." See [Oriakhi, 57 F.3d at 1297](#); see also [Boumelhem, 339 F.3d at 423](#) (holding that exit search for firearms implicates "significant government interests" not only in controlling exports but also in national security). This is not a case, in other words, in which the government **[**21]** invokes the border exception on behalf of its generalized interest in law enforcement and combatting crime. Cf. [United States v. Vergara, 884 F.3d 1309, 1317 \(11th Cir. 2018\)](#) (Jill Pryor, J., dissenting) (relying on "general law enforcement justification" to approve evidentiary border searches would "untether the [border search exception] from its justifications"). Here, there is a direct link between the predicate for the search and the rationale for the border exception.

Moreover, as the district court explained, the agents who searched Kolsuz's phone reasonably believed that their search would reveal not only evidence of the export violation they already had detected, but also "information related to other ongoing attempts to export illegally various firearms parts." [Kolsuz, 185 F. Supp. 3d at 860](#). The government emphasizes that finding — not contested by Kolsuz — in its argument before us, and properly so. [HN7](#)[↑] The justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the border, but also the prevention and disruption of ongoing efforts to export contraband illegally, **[*144]** through searches initiated at the border. See, e.g., [Ramos, 190 F. Supp. 3d at 999](#) (approving post-arrest "investigatory" border search of cell phone for information **[**22]** about larger smuggling organization and "more contraband entering into the country at that time"); [United States v. Mendez, 240 F. Supp. 3d 1005, 1007-10 \(D. Ariz. 2017\)](#) (approving post-arrest border search of cell phone for evidence of additional

contraband entering country); cf. [United States v. Kim, 103 F. Supp. 3d 32, 44, 46, 59 \(D.D.C. 2015\)](#) (holding unreasonable forensic search of laptop at border where search was expected to reveal evidence of past but not ongoing criminal activity).

In the circumstances presented here, we agree with the government's bottom line: Because the forensic search of Kolsuz's phone was conducted at least in part to uncover information about an ongoing transnational crime — in particular, information about additional illegal firearms exports already underway, by freight or in the custody of a coconspirator, see [Kolsuz, 185 F. Supp. 3d at 860](#) — it "fits within the core of the rationale" underlying the border search exception. Brief of United States at 19-20.

B.

Most of Kolsuz's appeal is devoted to his argument against application of the border exception. But Kolsuz has a fallback position, as well: Even under the border exception, Kolsuz contends, the forensic search of his phone constituted a nonroutine border search "unsupported by the type of reasonable suspicion required to justify" such searches. Defendant's Brief **[**23]** at 31. Again, we disagree.

1.

Like the district court, we begin by considering the first premise of Kolsuz's argument: that the forensic search of his cell-phone data qualifies as a nonroutine border search, requiring some level of particularized suspicion. We agree with the district court that particularly in light of the Supreme Court's decision in [Riley, HN8](#)[↑] a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion. See [Kolsuz, 185 F. Supp. 3d at 852-58](#).

As described above, the Supreme Court has held that even at the border, individualized suspicion is necessary to justify certain "highly intrusive searches," in light of the significance of the individual "dignity and privacy interests" infringed. [Flores-Montano, 541 U.S. at 152](#). Beyond that general guidance, the Court has not delineated precisely what makes a search nonroutine. Compare [id. at 155](#) (removal and disassembly of car's gas tank does not qualify as nonroutine border search) with [Montoya de Hernandez, 473 U.S. at 541-42](#) (16-hour detention for monitored bowel movement pending rectal examination is nonroutine).⁴ But as the district court ably explains, [HN9](#)] in deciding whether a search rises to the level of nonroutine, courts have focused primarily on how deeply it intrudes into **[**24]** a person's privacy. [Kolsuz, 185 F. Supp. 3d at 853](#). Under that approach, border searches of luggage, outer clothing, and personal effects consistently are treated as routine, while searches that are most invasive of privacy — strip searches, alimentary-canal searches, x-rays, and the like — are deemed nonroutine and permitted only with reasonable suspicion. See [id. at 853 & n.14](#) (citing cases).

By that metric, even before the Supreme Court issued its 2014 decision in *Riley*, there was a convincing case for categorizing forensic searches of digital devices as nonroutine. See [Cotterman, 709 \[*145\] F.3d at 963-68](#) (holding that forensic examination of computer is nonroutine border search requiring reasonable suspicion); [Saboonchi, 990 F. Supp. 2d at 549-60](#) (same as to smartphones and flash drives). First is the matter of scale: The sheer quantity of data stored on smartphones and other digital devices dwarfs the amount of personal information that can be carried over a border - and thus subjected to a routine border search -

in luggage or a car. "The average 400-gigabyte laptop hard drive can store over 200 million pages. . . . Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage." [Cotterman, 709 F.3d at 964](#). Subjected to comprehensive **[**25]** forensic analysis, a digital device can reveal an unparalleled breadth of private information.

The uniquely sensitive nature of that information matters, as well. Smartphones and laptops "contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails," *id.*, and also may provide access to data stored remotely, [id. at 965](#).⁴ The report generated by the month-long logical file system extraction of data from Kolsuz's phone is a case in point, revealing 896 pages' worth of sensitive data including personal contacts, photographs, web browsing history, and a "history of [Kolsuz's] physical location down to precise GPS coordinates," J.A. 94 - the kind of information that, analyzed cumulatively, "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations." See [United States v. Jones, 565 U.S. 400, 415, 132 S. Ct. 945, 181 L. Ed. 2d 911 \(2012\)](#) (Sotomayor, J., concurring). And finally, while an international traveler can mitigate the intrusion occasioned by a routine luggage search by leaving behind her diaries, photographs, and other especially personal effects, the same is not true, at least **[**26]** practically speaking, when it comes to smartphones and digital devices. Portable electronic devices are ubiquitous - for many, the most reliable means of contact when abroad - and it is neither "realistic nor reasonable to

⁴The forensic search of Kolsuz's phone, which remained in airplane mode throughout, did not extend to information stored remotely ("in the cloud"), nor to residual data of files that had

been deleted by Kolsuz. [Kolsuz, 185 F. Supp. 3d at 849 & n.8](#). Like the district court, however, we decline "to distinguish an extensive forensic search of a cell phone from a very extensive forensic search of a cell phone." [id. at 857](#).

expect the average traveler to leave his digital devices at home when traveling." [Saboonchi, 990 F. Supp. 2d at 556](#).

And then came *Riley*, in which the Supreme Court confirmed every particular of that assessment. *Riley* holds that the search incident to arrest exception, which allows for automatic searches of personal effects in the possession of an arrestee, does not apply to manual searches of cell phones. [134 S. Ct. at 2493-94](#). The key to *Riley*'s reasoning is its express refusal to treat such phones as just another form of container, like the wallets, bags, address books, and diaries covered by the search incident exception. See [id. at 2488-90](#). Instead, *Riley* insists, cell phones are fundamentally different "in both a quantitative and a qualitative sense" from other objects traditionally subject to government searches. [Id. at 2489](#). And that is so, *Riley* explains, for precisely the reasons already identified by cases treating border searches of digital devices as nonroutine: the "immense storage capacity" of cell phones, putting a vastly **[**27]** larger array of information at risk of exposure, *id.*; the special sensitivity of the kinds of information that may be stored on a phone, such **[*146]** as browsing history and historical location data, [id. at 2490](#); and, finally, the "element of pervasiveness that characterizes cell phones," *id.*, making them an "insistent part of daily life," [id. at 2484](#).

After *Riley*, we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of **[*147]** individualized suspicion. See [Kolsuz, 185 F. Supp. 3d at 858](#); see also [United States v. Saboonchi, 48 F. Supp. 3d 815, 819 \(D. Md.](#)

[2014](#)) ("*Saboonchi II*") (discussing ways in which *Riley* confirms prior holding that border searches of digital devices are nonroutine). Indeed, the impact of *Riley* is plain enough that the government's brief does not seriously contest this point, focusing instead on the argument (which we next address) that nonroutine or not, the search of Kolsuz's phone was justified under the border exception.⁵ We also note that shortly after argument in this case, the Department of Homeland Security adopted a policy that treats forensic searches of digital devices as nonroutine border searches, insofar as such searches now may be conducted only with reasonable suspicion of activity that violates the customs **[**28]** laws or in cases raising national security concerns. U.S. Customs and Border Prot., CBP Directive No. 3340-049A, *Border Search of Electronic Devices* 5 (2018). That the agency has chosen to adopt these requirements, of course, does not establish that they are constitutionally mandated. Cf. [Ickes, 393 F.3d at 507](#) (distinguishing between agency practice and constitutional requirements). But it does suggest, as courts have anticipated, that the distinction between manual and forensic searches is a perfectly manageable one, see [Cotterman, 709 F.3d at 967](#) (categorizing forensic searches as nonroutine requires only "that officers make a commonsense differentiation between a manual review of files on an electronic device and application of computer software to analyze a hard drive"), and that treating forensic phone searches as nonroutine need not interfere unduly with the agency's protective mission at the border, see

⁵ The government does note that in [Ickes, 393 F.3d at 505-07](#), our court treated a search of a computer as a routine border search, requiring no individualized suspicion for the search. But as the district court explained, *Ickes* approved a manual, on-site inspection of computer contents that would be accessible to any user, and did not address the use of the sophisticated forensic

search methods at issue here. [Kolsuz, 185 F. Supp. 3d at 853-54](#); see also [Saboonchi, 990 F. Supp. 2d at 546](#) (distinguishing *Ickes* on same ground). Because *Kolsuz* does not challenge the initial manual search of his phone at Dulles, we have no occasion here to consider whether *Riley* calls into question the permissibility of suspicionless manual searches of digital devices at the border.

[Saboonchi, 990 F. Supp. 2d at 570](#).⁶

2.

That the forensic analysis of Kolsuz's phone data qualifies as a nonroutine border search does not resolve this case. [HN10](#)^(↑) Nonroutine searches are permitted under the border exception, so long as they are accompanied by the appropriate level of individualized suspicion. **[**29]** See [Montoya de Hernandez, 473 U.S. at 540-41 & n.4](#).

The district court concluded that under the border exception, the "highest level of *Fourth Amendment* protection available" is the reasonable suspicion standard, which was met in this case.⁷ [Kolsuz, 185 F. Supp. 3d at 858-59](#). As the district court explained, courts consistently have required only reasonable suspicion even when reviewing the most intrusive of nonroutine border searches and seizures - like, for instance, the one at issue in *Montoya de Hernandez*, in which the Supreme Court held that with reasonable suspicion, the government could detain a traveler thought to be smuggling contraband in her alimentary canal for 16 hours while it monitored her bowel movements and sought a court order for a rectal examination. [Id. at 852-53, 858-59](#).

Of course, certain searches conducted under

exceptions to the warrant requirement may require more than reasonable suspicion. See, e.g., [California v. Carney, 471 U.S. 386, 393-95, 105 S. Ct. 2066, 85 L. Ed. 2d 406 \(1985\)](#) (holding that automobile exception to the *Fourth Amendment* permits a warrantless search of a motor home if based on probable cause). Perhaps the same is true of some nonroutine border searches, as Kolsuz argues, but we need not resolve that question here. As the government reminds us, even if a search is judged to be constitutionally flawed in some way, its fruits need not be suppressed **[**30]** if the agents acted "in reasonable reliance on binding precedent." [Davis v. United States, 564 U.S. 229, 241, 131 S. Ct. 2419, 180 L. Ed. 2d 285 \(2011\)](#); see [United States v. Baker, 719 F.3d 313, 320-21 \(4th Cir. 2013\)](#) (describing *Davis*). In such circumstances, suppression can do little to deter police misconduct, and the "social costs" of suppression - the exclusion from trial of reliable evidence bearing on guilt or innocence - outweigh any deterrence benefits. [Davis, 564 U.S. at 237-38](#).

At the time the CBP officers conducted their forensic search of Kolsuz's phone, there was at least some case law indicating that reasonable suspicion might be required. See [Kolsuz, 185 F. Supp. 3d at 855-58](#) (discussing cases). But there was no case suggesting that even more

⁶The new policy does not use the "routine" and "nonroutine" terminology of Supreme Court case law, distinguishing instead between "basic" and "advanced" searches. But the import is the same. "Basic" searches (like those we term "manual") are examinations of an electronic device that do not entail the use of external equipment or software and may be conducted without suspicion. "Advanced" searches (like "forensic" searches) involve the connection of external equipment to a device - such as the Cellebrite Physical Analyzer used on Kolsuz's phone - in order to review, copy, or analyze its contents, and are subject to the restrictions noted above. See U.S. Customs and Border Prot., CBP Directive No. 3340-049A, *Border Search of Electronic Devices* 4-5 (2018); [Molina-Isidoro, 884 F.3d at 294 & n.2](#) (Costa, J., concurring).

⁷Kolsuz also argues that even if the search of his phone could

be justified by reasonable suspicion, what would be required is reasonable suspicion that contraband, as opposed to evidence, would be found on the device. Otherwise, according to Kolsuz, the search would be "untethered" from the constitutional justification for border searches: the interception of contraband as it crosses the border. If this argument sounds familiar, that is because it is a reformulation of Kolsuz's threshold argument against any application of the border exception to this case, addressed above. And for essentially the reasons already given, we cannot agree. The district court found - and Kolsuz does not dispute - that the agents here had reason to believe that their search of Kolsuz's phone would reveal not only evidence of past export-control violations, but also evidence of ongoing efforts to smuggle firearms over the border. [Kolsuz, 185 F. Supp. 3d at 860](#). That is enough to "tether" the search to the rationale behind the border exception.

would be necessary - for a forensic search of a phone at the border or, indeed, for *any* border search, no matter how nonroutine or invasive. And that remains the case today: Even as *Riley* has become familiar law, there are no cases requiring more than reasonable suspicion for forensic cell phone searches at the border. *But see Vergara, 884 F.3d at 1313-19* (Jill Pryor, J., dissenting) (after *Riley*, forensic search of phone is not subject to border search exception and therefore requires warrant based on probable cause).

[*148] Under these circumstances, we think it was reasonable for the CBP officers who conducted the forensic analysis of Kolsuz's phone to rely on the [**31] established and uniform body of precedent allowing warrantless border searches of digital devices that are based on at least reasonable suspicion. See *Molina-Isidoro, 884 F.3d at 293* (applying good-faith exception to warrantless manual search of phone at border). Under *Davis's* "good-faith" exception to the *Fourth Amendment* exclusionary rule, that reasonable reliance by itself is enough to bar suppression of the evidence generated by the search. See *Baker, 719 F.3d at 321*. Accordingly, we need not - and will not - reach the issue of whether more than reasonable suspicion is required for a search of this nature in affirming the judgment of the district court. See *Molina-Isidoro, 884 F.3d at 294* (Costa, J., concurring) (reliance on good-faith exception particularly appropriate in area of rapid legal and technological change).

III.

For the reasons given above, the judgment of the district court is

AFFIRMED

Concur by: WILKINSON

Concur

WILKINSON, Circuit Judge, concurring in the judgment:

I thank the majority for its thoughtful opinion. While I agree with much of what is said, my point of departure is quite basic. The majority appears to leave the legislative and executive branches shivering in the cold. Those branches have a critical role to play in defining the standards for a border search, and they are much [**32] better equipped than we are to appreciate both the privacy interests at stake and the magnitude of the practical risks involved.

The standard of reasonableness in the particular context of a border search should be principally a legislative question, not a judicial one. Congress should decide that standard. Courts should apply it. This is a separation of powers approach that makes use of the respective capabilities of all three branches of government, not just one.

The infirmity of a constitutional rule in the unique context of a border search is clear. Such a rule claims for courts the sole prerogative to set standards in an area where legislative inquiry would be invaluable and where the executive maintains a strong sovereign interest. Diminishing the other two branches flirts with real-life dangers. The whole enterprise calls for the greatest caution and circumspection, not premature declarations of constitutional rules.

If individualized suspicion is to be required in order to conduct what the majority asserts is a "nonroutine border search," Maj. Op. at 4, then Congress must say so. And in all events, there was plainly reasonable suspicion to conduct the search here. The majority [**33] should have stopped right there. Assuming without deciding that reasonable suspicion was even required, it is present here in triplicate.

Instead my colleagues wander from what Article

Ill indisputably envisions as the core role of courts: simply to decide a case or controversy. The majority turns prescriptive, but the pronouncement here is too abstract and floats too far above the realities at the border.

Lethal capabilities are advancing at a rapid pace. Detection of destructive devices is becoming more difficult. Nation states, terrorist bands, and individual arms merchants see profit and prestige and power in joining the arms race. Might we wish to hear in a manner more probing than appellate briefs and oral argument exactly what are the dimensions of the [*149] threats we face? What makes us think the elective branches would downgrade the significant privacy interests the majority rightly identifies? Might the other two branches, if given a fair chance, have something to say? And do not Articles I and II, which set forth the legislative and executive roles in matters of grave international import, give them the right to say it? Who are we to propound the idea that democratic bodies, where [**34] *Fourth Amendment* reasonableness is concerned, have nothing to contribute?

Alarmist? Hyperbolic? Perhaps. But if we so limit the role of our coordinate branches with a constitutional ruling, how shall we ever know?

I.

The majority fairly recounts the facts here, and they are straightforward and incriminating. Before his arrest at Dulles airport, Customs and Border Protection (CBP) agents had twice stopped Kolsuz, a Turkish national, at JFK airport for carrying contraband firearms parts proscribed by statute. See [22 U.S.C. § 2778](#). On both occasions, Kolsuz failed to produce the license required to export those parts. Both times, CBP agents informed Kolsuz that he needed a license to export those items.

Kolsuz reentered the United States on January 25, 2016, on a tourist visa. He again purchased

numerous gun parts. Law enforcement officials who were familiar with Kolsuz's previous attempts to export contraband firearms asked CBP to search Kolsuz's bags when he tried to return to Turkey. When Kolsuz arrived at Dulles, CBP searched his bags. The inspection revealed eighteen handgun barrels, twenty-two 9 mm handgun magazines, four .45 caliber handgun magazines, and one .22 caliber Glock conversion kit. All of these firearms [**35] parts are restricted items on the U.S. Munitions List. At no time did Kolsuz have permission to export them. Based on Kolsuz's previous attempts to bring firearm parts out of the country, CBP had ample reason to suspect that Kolsuz might again try to export firearms.

Following the search of Kolsuz's bags, CBP officers interrogated Kolsuz and performed a cursory inspection of his iPhone. At the end of the interrogation, Kolsuz was arrested and his iPhone seized. At that point, his iPhone was transported to Sterling, Virginia, where federal law enforcement conducted an "advanced logical file system extraction" of the iPhone. This extraction, as the majority notes, generated an 896-page report on the information contained in the phone.

II.

This was plainly a border search. See Maj. Op. at 18. Assuming reasonable suspicion of Kolsuz's criminal activity is somehow required, it clearly existed here. We need go no further. Rather than deciding the case on solid and suitably limited grounds, the majority goes on to prescribe a constitutional standard whose rationale would label a great many cell phone searches undertaken at the border as "nonroutine" and forbidden absent prior individualized [**36] suspicion.

While the majority purports not to reach the question of the justification required for the manual search of Kolsuz's cell phone at Dulles airport, see Maj. Op. at 22 n.5, the rhetorical

thrust of its opinion as concerns cell phones and smartphones may be read by many courts to require individualized suspicion for border searches of all cell phones period. Or if the majority intends a less sweeping standard, the slipperiness of the distinction between intrusive and less intrusive cell phone searches and between those that are routine and those that are nonroutine will [*150] lead, I fear, to difficulties in application down the road. While the majority's constitutional venture may be correct, it also may well not be. Again, we are not the ones to set the standard.

We are, each of us, in over our heads. We have no idea of the dangers we are courting. JFK and Dulles are quintessential border posts. See [*Almeida-Sanchez v. United States*, 413 U.S. 266, 273, 93 S. Ct. 2535, 37 L. Ed. 2d 596 \(1973\)](#). Thousands of international travelers go through them every day. Yet the majority hardly grapples with how law enforcement is expected to ascertain individualized suspicion when dealing with such numbers. The privacy interest, while weighty, is the only side of a precarious balance [**37] that seems to concern the majority, and this in the application of the *Fourth Amendment*, which articulates reasonableness and hence balance as a standard. See [*Katz v. United States*, 389 U.S. 347, 360, 88 S. Ct. 507, 19 L. Ed. 2d 576 \(1967\)](#).

One would hope that rather than charging unnecessarily ahead, the majority would recognize the need for congressional input, which the enunciation of constitutional standards makes more difficult. Constitutional standards are preemptive. They sweep all other pieces off the board. Judicially promulgated constitutional standards say essentially, "That's that. The Constitution is the highest law, and the judiciary shall be its sole guardian."

Empirical questions lie at the heart of the tension between privacy and security interests at the border. How many people travel through

international airports every day? What screening techniques and investigative resources does government have available? What materials are being smuggled in and out, and by whom? What practical obstacles exist to individualized findings? What, in other words, is the magnitude of danger courted by progressive step-ups of search requirements?

The limited glimpse from a single case does no more than beg the question: What is the reality of it all? This is why any *Fourth Amendment* standard is [**38] best designed here through the more adaptable legislative process and the wider lens of legislative hearings. See [*Riley v. California*, 134 S. Ct. 2473, 2497-98, 189 L. Ed. 2d 430 \(2014\)](#) (Alito, J., concurring in the judgment) ("Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."). For "[a]s new technologies continue to appear in the marketplace and outpace existing surveillance law, the primary job of evaluating their impact on privacy rights and of updating the law must remain with the branch of government designed to make such policy choices, the legislature." [*In re Askin*, 47 F.3d 100, 106 \(4th Cir. 1995\)](#).

The majority contends that the "Department of Homeland Security adopted a policy that treats forensic searches of digital devices as nonroutine border searches." Maj. Op. at 22. I think the document is more complex than this, but in all events, it proves my point—that in this narrow area agency policy born of actual and ongoing experience is more adaptable than a freeze-frame constitutional ruling.

Courts too often assume Congress is desensitized to the need for privacy protections. This does lawmakers a disservice. Congress has long sought to strike [**39] a balance between privacy and security in the context of digital searches. See, e.g., *USA Freedom Act of*

2015, *Pub. L. No. 114-23, 129 Stat. 268* (limiting government surveillance of telephone records); [18 U.S.C. §§ 2510-22 \(2012\)](#) (limiting the government's ability to monitor electronic communications); **[*151]** Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, [115 Mich. L. Rev. 1117, 1120 \(2017\)](#) (observing "the recent enactment of more and stronger statutory privacy laws" by federal and state legislatures in the past five years). And, though of course not directly relevant in the context of a federal border search, states have historically also protected *Fourth Amendment* privacy rights. See Kerr, [115 Mich. L. Rev. at 1120](#) (documenting state statutes limiting the use of digital searches).

It is sometimes said in non-border search cases that the judiciary does no more than provide "a floor" which Congress can exceed at its discretion. See, e.g., [Kelsey v. Cty. of Schoharie, 567 F.3d 54, 64 \(2d Cir. 2009\)](#); [Graves v. Mahoning Cty., 821 F.3d 772, 778 \(6th Cir. 2016\)](#). But the so-called floor in this case is not some innocuous minimum, but a hugely consequential policy judgment that certain categories of border searches will require individualized suspicion. The fact that Congress has not thus far seen fit to adopt a court's preferred standard gives us no license to act preemptively with an unnecessary constitutional disquisition. **[**40]** The dangers of this notion are underscored by the majority's reservation here of the question whether probable cause or a warrant may be required for some unspecified categories of border searches in the future. See *Maj. Op.* at 24-25. This does not sound like any sort of "floor" at all.

The dangers of judicial standard-setting in an area as sensitive as border searches is thus apparent. Here the legislative process would be informed by numerous representatives of the executive branch, who can lend their practical insights and experience to the inquiry. The executive's role has always been thought

especially important in an area such as border searches, where it has long been held to have a uniquely sovereign interest. The border search exception to the *Fourth Amendment's* warrant requirement is based on the "longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." [United States v. Ramsey, 431 U.S. 606, 616, 97 S. Ct. 1972, 52 L. Ed. 2d 617 \(1977\)](#). As the Supreme Court has explained, "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." See [United States v. Flores-Montano, 541 U.S. 149, 152, 124 S. Ct. 1582, 158 L. Ed. 2d 311 \(2004\)](#). That interest is so powerful that border searches "are reasonable simply by virtue of the fact **[**41]** that they occur at the border." [Ramsey, 431 U.S. at 616](#).

The role of courts is thus not to blanket the field of border searches by preempting constitutionally the contributions that the other two branches of our government are constitutionally empowered and uniquely positioned to make. *Marbury v. Madison* did of course say that it is "emphatically the province and duty of the judicial department to say what the law is." [5 U.S. \(1 Cranch\) 137, 177, 2 L. Ed. 60 \(1803\)](#). But that is a very different proposition from holding that constitutional interpretation must be solely a judicial function. Indeed "the general architecture of [the Constitution] would seem to imply a basic coequality among the three departments. . . . [I]t nowhere explicitly raises the Court above coordinate legislative and executive departments." Akhil Reed Amar, *Architecture*, [77 Ind. L.J. 671, 692-93 \(2002\)](#). This is not a new idea. James Madison wrote that "none of [the three branches of government] ought to possess, directly or indirectly, an overruling influence over the others in the administration of their respective powers." *The Federalist* No. 48 (James Madison). But it is precisely

that [*152] "overruling influence" the majority asserts in its unnecessary constitutional exercise today.

III.

The general search that all [**42] of us must undergo at airports attests to the difficulties of ensuring airborne security through individualized suspicion. Our new world has brought inconvenience and intrusions on an indiscriminate basis, which none of us welcome, but which most of us undergo in the interest of assuring a larger common good. Our old world of relative security and relative privacy, if indeed it ever existed, is now gone with the wind. It is painful to dream of retrieving what is ours no longer.

The Supreme Court has often noted how technology endangers privacy. As it observed in *Riley*, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." [134 S. Ct. at 2488-89](#). But *Riley* involved the warrantless search of a cell phone following an ordinary roadside arrest after a traffic violation. The defendant was not at the border. The setting here is far different from *Riley*.

Nor does the privacy interest recognized in *Riley* begin to answer the question of *who* should strike the balance between privacy and security at the border of the country, the point most freighted with security threats and the point at which a nation asserts and affirms [**43] its very right to nationhood.

Porous borders are uniquely tempting to those intent upon inflicting the vivid horrors of mass casualties. Then too, there is the danger of highly classified technical information being smuggled out of this country only to go into the hands of foreign nations who do not wish us well and who seek to build their armaments to an ever more perilous state.

It is no secret that rapid technological advances have enhanced the ability of criminal syndicates and terrorist networks to execute transnational schemes through the coordination now made possible by instantaneous communications. To give criminal enterprises the advantage of technological advancements and at the same time impair access of law enforcement to those same developments risks recalibrating the *Fourth Amendment* balance in a manner that does not comport with reasonableness. Cell phones may prove essential to revealing the scope of a conspiracy; who is involved; what weapons and devices the conspirators possess; what the purpose and plans and timing of the plotted criminal acts may be; and where indeed those who would carry out these acts may be located.

But to stop there is to halve the equation. The majority is right [**44] to emphasize that searches of cell phones and the like can reveal a trove of data unconnected to any criminal offense. The intrusion upon personal privacy is undoubtedly severe. One may of course say that international travelers are on notice that border inspections may be uniquely intrusive, and that travelers can prepare for that prospect by not taking a full load of personal data abroad, where additional dangers of theft and inadvertent loss may also await. But the fact that we can pack our digital suitcase with the same care that we pack personal belongings in traditional luggage still does not nullify the reality that these sorts of searches look into our lives in a way that is deeply uncomfortable, especially when government itself becomes the agent of intrusion. But the ultimate question here is not whether there is a balance to be struck between what are highly significant privacy and security interests. It is [*153] what branch of government is best suited to make that determination. In this case, where there is a longstanding historical practice in border searches of deferring to the legislative and executive branches, the majority should have

shown a modest measure of restraint **[**45]** simply by deciding the case. Our role in this narrow area is more the application of standards than the creation of them. In reaching to formulate a constitutional rule, the majority has turned the whole thing on its head.

We are ruling in a vacuum. We are building a doctrinal house without foundation. The majority opinion provides little context or background or real-life picture of Dulles Airport. It leaves little role for the legislative branch. At what point the domestic conveniences of cell phone use should ripen into transnational entitlements is primarily for the political branches to determine. The elected branches are also best able to gauge at what point the creeping constitutionalization of border searches reflects the cultural habits and practices of an elite group of transnational Americans at the risk of endangerment that knows no class bounds.

It is ill advised to ignore the role of the political branches in addressing a phenomenon that may fall short of the formal warfare contemplated in Articles I and II, but still retains major features of international conflict. To reach beyond the Article III function is to court grave dangers which we may perceive as remote and hypothetical **[**46]** until one day, very suddenly, they are not. Not that any one case or any one appellate court will likely bring down havoc on our heads. In our shielded circumstances, we may never know or be apprised of many effects of our decisions. Still it is uncomfortable to guess. I have nothing but respect for my friends in the majority. But taken cumulatively, rulings slowly constitutionalizing border searches are taking chances with the safety and lives of our fellow Americans. And this, as a judge, I cannot do.