Journal of Air Law and Commerce

Volume 84 | Issue 1 Article 6

2019

Flying in the Face of Suspicionless Cell Phone Searches: Fourth Circuit Grants Airline Passengers Heightened Protection From Searches by Customs Officers

Andrea deLorimier
Southern Methodist University, Dedman School of Law

FLYING IN THE FACE OF SUSPICIONLESS CELL PHONE SEARCHES: FOURTH CIRCUIT GRANTS AIRLINE PASSENGERS HEIGHTENED PROTECTION FROM SEARCHES BY CUSTOMS OFFICERS

ANDREA DELORIMIER*

I. INTRODUCTION

INTERNATIONAL TRAVELERS ARE aware that airport customs officers may search their personal property.[1] However, most travelers do not know that officers have the power to mine every piece of data stored in their cell phones, even if there is no reason to suspect the passenger of criminal activity.[2] Given that many Americans believe cell phone searches implicate privacy rights "comparable to that of strip searches and body cavity searches,"[3] it is imperative that travelers' cell phones be granted heightened Fourth Amendment protections. The Fourth Circuit mirrored this sentiment in *United States v. Kolsuz*.[4]

In *Kolsuz*, the court held that a forensic examination of a cell phone at the airport must be categorized as a nonroutine border search and can only be conducted upon a showing of reasonable suspicion.[5] The court did not reach the question of whether the search required more than reasonable suspicion, such as a warrant based on probable cause, because the officers were acting in reasonable reliance on established law.[6] This casenote argues that the Fourth Circuit's classification of a forensic

* J.D. Candidate, SMU Dedman School of Law, May 2020; B.A., Texas A&M University, May 2017. I would like to thank the SMU Law Review Association for this opportunity and my parents for their encouragement and support.

[1] United States v. Cotterman, 709 F.3d 952, 967 (9th Cir. 2013).

[2] *Id.*

[3] Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1167 (2014).

[4] 890 F.3d 133, 146 (4th Cir. 2018).

[5] *Id.* at 146–47.

[6] *Id.* at 147.

border search as nonroutine was a step in the right direction.[7] However, given the serious privacy interests at stake, the court should have taken the opportunity to resolve the question of whether a forensic border search requires customs officers to have more than reasonable suspicion. The answer to this question is "accordingly simple—get a warrant."[8]

II. FACTUAL BACKGROUND

On February 2, 2016, Turkish citizen Hamza Kolsuz arrived at Dulles International Airport in Virginia for a flight to Turkey.[9] Customs officers examined his checked luggage and discovered he was carrying unregistered firearm parts in violation of federal law.[10] The officers brought Kolsuz to a secondary inspection area where they conducted a "manual" search of his iPhone 6, which consisted of browsing his recent calls and text messages.[11] After completing the manual search, officers transported Kolsuz's phone from the airport to the Homeland Security Investigations office (located four miles away) where an agent conducted a "forensic" search of the phone's data.[12] This search lasted for a full month and resulted in an 896-page report of 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."[13]

Kolsuz was indicted on three counts: attempting to export firearms without a license, attempting to smuggle goods from the United States, and conspiracy to commit these offenses.[14] Kolsuz moved to suppress the report generated by the forensic search of his phone, arguing that the forensic search constituted a nonroutine border search and required a warrant based on probable cause.[15]

---

[7] *See id.* at 146.

[8] Riley v. California, 573 U.S. 373, 403 (2014).

[9] *Kolsuz*, 890 F.3d at 139.

[10] *Id.*

[11] *Id.*

[12] A forensic search consists of attaching the cell phone to a "Cellebrite Physical Analyzer," which extracts data from the device. *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.* at 139–40.

The district court agreed with Kolsuz that the forensic search must be classified as nonroutine.[16] However, the court rejected a warrant requirement, stating that no court to date had required a warrant for nonroutine border searches and that even the most invasive nonroutine border searches have been justified on a reasonable suspicion standard.[17] The court convicted Kolsuz of all three counts.[18]

III. LEGAL BACKGROUND

The Fourth Amendment typically requires law enforcement officials to obtain warrants based on probable cause prior to searching individuals' private possessions.[19] However, at the border—or the border's functional equivalents, such as international airports—officers can conduct routine searches without "any requirement of reasonable suspicion, probable cause, or warrant."[20] Although routine border searches require no level of suspicion, the Supreme Court, through a series of cases involving airport security, recognized a category of highly intrusive "nonroutine" searches that are permitted only if accompanied by individualized suspicion.[21] In order to determine whether a border search qualifies as nonroutine, the Supreme Court implemented a balancing test: weighing a search's "intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests."[22] For example, highly invasive searches of the person, searches that are carried out in a "particularly offensive" manner, and searches that are destructive to personal property are more likely to be considered nonroutine and require a level of suspicion prior to searching.[23]

Courts initially demonstrated a reluctance to classify forensic searches of digital devices as nonroutine. In *United States v. Cotterman*, however, the Ninth Circuit held that a forensic search at

---

[16] *Id.* at 140.

[17] *Id.* at 140–41

[18] *Id.* at 141.

[19] *See* Arizona v. Gant, 556 U.S. 332, 338 (2009).

[20] United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

[21] *Kolsuz*, 890 F.3d at 138.

[22] *Montoya de Hernandez*, 473 U.S. at 537 (citing United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983)).

[23] United States v. Flores-Montano, 541 U.S. 149, 154 n.2, 155–56 (2004) (stating that there may be searches so "destructive" to personal property as to justify a level of suspicion); *see Montoya de Hernandez*, 473 U.S. at 541 (holding that officials at the border must have individualized suspicion in order to conduct a search of an airline passenger suspected of smuggling drugs in her alimentary canal).

an airport was nonroutine and required customs officers to have reasonable suspicion of criminal wrongdoing prior to conducting the search.[24] In coming to this conclusion, the court drew on the sheer quantity of information in cell phones as well as the "uniquely sensitive" nature of that information.[25] Then, in *United States v. Saboonchi*, the District Court of Maryland echoed this analysis, adding that the pervasiveness of cell phones in society renders it neither "realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling."[26]

In response to the increasing sophistication and omnipresence of digital devices, the Supreme Court issued its decision in *Riley v. California*.[27] In *Riley*, the Court held that a manual search of a cell phone seized incident to an arrest (another Fourth Amendment exception) requires a warrant based on probable cause.[28] As a general premise, the Court held that cell phones "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[29] The Court noted cell phones' immense storage capacity, overwhelming presence in society, and ability to contain many distinct types of personal information.[30] This decision forced lower courts to determine how the Supreme Court's updated stance on digital privacy would apply to the other Fourth Amendment exceptions, such as the border search exception.

The Eleventh Circuit was the first federal circuit court to consider "whether a warrant is required to conduct a forensic search of a cell phone at the border post-*Riley*."[31] In *United States v. Vergara*, the Eleventh Circuit refused to use *Riley* to inform its privacy analysis and refuted the idea that border searches should ever require a warrant or probable cause.[32] The dissent, on the other hand, looked to the Supreme Court's privacy con-

---

[24] United States v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013).

[25] *Id.* at 964, 966.

[26] United States v. Saboonchi, 990 F. Supp. 2d 536, 556 (D. Md. 2014) (mem. op.).

[27] *See* Riley v. California, 573 U.S. 373, 401 (2014).

[28] *Id.* at 2485.

[29] *Id.* at 2488–89.

[30] *Id.* at 2489–90.

[31] Aisha J. Dennis, *Riling Up the Border Search Doctrine: Litigating Searches of Digital Content at Our Ports of Entry*, THE CHAMPION 40, 44 (Mar. 2018).

[32] United States v. Vergara, 884 F.3d 1309, 1311 (11th Cir. 2018), *cert. denied*, 139 S. Ct. 70 (2018).

siderations in *Riley* to support its argument that a warrant should be required.[33]

IV. ANALYSIS

A. Forensic Searches of Cell Phones are Nonroutine Border Searches Requiring Reasonable Suspicion

In *United States v. Kolsuz*, the Fourth Circuit held that the forensic search of an international traveler's cell phone "must be treated as a nonroutine border search" accompanied by a showing of individualized suspicion.[34] In classifying the search as nonroutine, the court relied primarily on the holdings of various cases that lend support to this conclusion and the Supreme Court's confirmation of these cases' reasoning in *Riley*.

Judge Harris began the opinion by stating that the question of whether a border search is nonroutine should be informed by "how deeply it intrudes into a person's privacy."[35] With this principle as a guideline, the court noted that multiple courts have already constructed strong cases for construing forensic searches of digital devices as nonroutine.[36] Specifically, Judge Harris found the reasoning of *Cotterman* and *Saboonchi* compelling, agreeing with these courts that the "unparalleled breadth" and "uniquely sensitive nature" of cell phones' information, coupled with their pervasiveness, lend support to the idea that a forensic border search cannot be considered routine.[37] Turning to the case at hand, the court found that the forensic search of Kolsuz's phone—resulting in a 896-page report of Kolsuz's personal information—was a "case in point" as to how invasive forensic searches can be.[38]

The Fourth Circuit did not reach the question of whether anything more than reasonable suspicion is required for a forensic search of a cell phone.[39] Applying the good-faith exception to the Fourth Amendment exclusionary rule, the court ruled that the officers who conducted the forensic analysis of Kolsuz's phone were relying "on the established and uniform body of

---

[33] *Id.* at 1317 (Pryor, J., dissenting).

[34] United States v. Kolsuz, 890 F.3d 133, 146 (4th Cir. 2018).

[35] *Id.* at 144.

[36] *Id.* at 145–46.

[37] *Id.* at 145.

[38] *Id.*

[39] *Id.* at 148.

precedent allowing warrantless border searches of digital devices that are based on at least reasonable suspicion."[40]

B. Why the Fourth Circuit Did Not Go Far Enough

The Fourth Circuit properly held that customs officers must have reasonable suspicion prior to conducting a forensic border search of an airline passenger's cell phone.[41] However, given that the unique "quantitative" and "qualitative" characteristics of cell phones led the Supreme Court to require a warrant prior to conducting searches of cell phones seized incident to arrest, it is peculiar that the Fourth Circuit failed to reach the same conclusion in terms of forensic searches of cell phones at international airports.[42] The court should have seized the opportunity to bring its argument to its logical conclusion: due to the weighty privacy concerns at stake during air travel, customs officers must obtain a warrant based on probable cause prior to conducting a forensic search of a passenger's cell phone.

Critics of a warrant requirement believe the government's interest in protecting the international border is too strong to be trumped by individual privacy concerns.[43] For example, shortly after *Kolsuz* was decided, the Eleventh Circuit held that customs officers do not need any level of suspicion prior to forensically searching an airline passenger's cell phone.[44] In creating this circuit split, the court stated that it was "unpersuaded that a traveler's privacy interest should be given greater weight than the 'paramount interest [of the sovereign] in protecting . . . its territorial integrity.'"[45]

Although the government undoubtedly has an interest in airport security,[46] a passenger's privacy interests during international travel are just as strong, if not stronger. Even though *Riley*'s analysis of digital privacy rights applies similarly to forensic searches of a cell phone at international airports, there are multiple reasons why forensic border searches implicate privacy rights beyond those enumerated by the Supreme Court. First,

---

[40] *Id.*

[41] *Id.* at 145.

[42] *Id.* at 144.

[43] *See* United States v. Touset, 890 F.3d 1227, 1235 (11th Cir. 2018).

[44] *Id.* at 1234.

[45] *Id.* at 1235 (quoting United States v. Flores-Montano, 541 U.S. 149, 153 (2004)).

[46] *Id.*

cell phones are a practical necessity for air travel.[47] Cell phones not only serve as an airline passenger's most reliable means of communication with loved ones while abroad but also have the capacity to hold an array of crucial travel information, such as mobile boarding passes, hotel reservations, and travel itineraries. Because cell phones are essential to international flights, travelers are virtually guaranteed to be carrying their cell phones if they are subjected to a more invasive search while going through customs.

Second, it is important to highlight the stark differences between manual and forensic searches.[48] *Riley*'s holding pertained to manual searches, meaning the officers at issue simply scrolled through the phone's digital content.[49] On the other hand, a customs officer conducting a forensic search is "capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites."[50] The Supreme Court contemplated similar privacy concerns in its discussion of cloud computing, noting that digital privacy is further compromised when a search extends beyond data stored on the physical device itself.[51] Although forensically searching a phone's deleted material differs from searching material stored in the cloud, both scenarios involve searches in which the owner of the device does not intend to have the searched data stored on the device. The implication of this is that an airline traveler who deletes sensitive information from his phone in anticipation of a search at the airport is nonetheless at risk of being subjected to a highly invasive digital search by customs officials. It is likely that the Supreme Court would hold that this level of privacy invasion is "like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[52]

Notwithstanding the significant privacy justifications, a warrant requirement is also a more workable standard than that of reasonable suspicion. A reasonable suspicion standard requires customs officers, prior to conducting the search, to point to "a particularized and objective basis for suspecting the particular

---

[47] *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 556–58 (D. Md. 2014) (mem. op.).

[48] *See* United States v. Vergara, 884 F.3d 1309, 1315 (11th Cir. 2018), *cert. denied*, 139 S. Ct. 70 (2018).

[49] *Id.* at 1316.

[50] United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013).

[51] *See* Riley v. California, 573 U.S. 373, 397 (2014).

[52] *Id.*

person stopped of criminal activity."[53] Accordingly, even though *Kolsuz* offers some protection to the 30,200 international travelers[54] who had their cell phones searched by customs officers last year, airline passengers are still at the mercy of officers who decide whether to probe a cell phone on a discretionary basis. On the other hand, a warrant requirement would remove the threat of officer discretion by requiring them to receive permission prior to conducting a forensic search.[55] Requiring a warrant would not only protect passengers but also shield customs officers from the risk of carrying out a search that later litigation declares unreasonable.[56]

Given the substantial digital privacy concerns that are unique to air travel, the majority's willingness to defer to *Riley*'s privacy analysis, and the workability of the warrant requirement, the Fourth Circuit failed to take its argument to the logical conclusion. Although an individualized suspicion standard is a step in the right direction, the court missed an opportunity to hold that a warrant is required prior to conducting a forensic border search of a cell phone. Thus, until the Supreme Court rules on the matter, the status of international airline travelers' digital privacy is up in the air because of this circuit split.

---

[53] United States v. Cortez, 449 U.S. 411, 417–18 (1981) (setting out the definition of the reasonable suspicion standard).

[54] *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. CUSTOMS AND BORDER PROT. (Jan. 5, 2018) https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and (last modified Jan. 9, 2018) [https://perma.cc/NMD5-6942]. This is a nearly 60% increase over the number of such travelers in 2016. *Id.*

[55] *See* Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1638–39 (2012).

[56] *See id.* at 1641–42.