Travel Tip

Expect warrantless digital device searches at the border.

BY PIERRE GROSDIDIER

As unsettling as they are, warrantless border searches of digital devices are legal. It is well established that the sovereign's interest in territorial integrity reaches its zenith at the border.[1] Accordingly, the "border search" exception to the Fourth Amendment's privacy protections dispenses U.S. Customs and Border Protection, or CBP, officers from securing probable cause-based warrants for border searches, either inbound or outbound.[2]

The border search exception applies equally to digital devices, which the CBP regards as luggage. The key issues as to these devices are the level of the search, i.e., basic versus forensic, and the level of suspicion of illicit activity required for each, i.e., none or a reasonable level of suspicion. The U.S. Supreme Court has defined reasonable suspicion as "a particularized and objective basis for suspecting the particular person stopped of criminal activity," an analysis that must consider "the totality of the circumstances."[3] No court has held that reasonable suspicion is required for a basic search, which means that CBP officers are free to manually rummage through a traveler's cellphone or computer.[4] Federal appellate courts are split regarding the level of suspicion required for forensic searches.

In *United States v. Kolsuz*, CBP officers detained departing traveler Hamza Kolsuz after finding unauthorized firearm parts in his suitcases.[5] The CBP seized and forensically searched his phone. Kolsuz was ultimately convicted and appealed the district court's denial of his motion to exclude the evidence collected from his iPhone. Invoking the Supreme Court's landmark *California v. Riley* decision, and the fact that the forensic search took a month at a place "miles away from [the] airport" after his arrest, Kolsuz argued that the grounds for the border search exception no longer applied and that the search required "a warrant based on probable cause."[6] In *Riley*, the U.S. Supreme Court held that the Fourth Amendment's ban on unreasonable searches meant that warrantless searches of cellphones seized during an arrest were unconstitutional, absent exigent circumstances.[7]

The 4th Circuit Court of Appeals disagreed with Kolsuz, holding that the delayed, off-site forensic search remained a border search because of its nexus to the contraband firearm parts. The court held that, because of its invasiveness and considering *Riley*, the forensic search qualified as a "nonroutine border search, requiring some measure of individualized suspicion."[8] But the court also held that CBP officers reasonably relied on the assumption that the reasonable suspicion standard justified their search of Kolsuz's iPhone. The court, therefore, did not have to decide whether the search required more than reasonable suspicion to affirm Kolsuz's conviction.

The 9th Circuit Court of Appeals reached a similar result in *United States v. Cotterman*, a case involving allegations of child pornography.[9] Using privacy arguments like those later invoked by the Supreme Court in *Riley*, *Cotterman* held that a forensic border search required reasonable suspicion.[10]

But recently, in *United States v. Touset*, the 11th Circuit Court of Appeals held that forensic border searches did not require reasonable suspicion.[11] Karl Touset's digital devices were seized when he entered the country based on the suspicion that he was allegedly involved in child pornography. Forensic searches found illicit pictures on four devices. Touset pleaded guilty but reserved the right to appeal the trial court's denial of his motion to suppress the forensically collected evidence. The court of appeals affirmed. It noted that the Supreme Court "never required reasonable suspicion for a search of property at the border, however non-routine and intrusive," and saw no reason to hold otherwise. The court also saw no reason to treat digital devices differently from physical luggage. It found unpersuasive the reasoning in *Kolsuz* and *Cotterman* because it had already held in *United States v. Vergara* that *Riley* did not apply to border searches.[12] In the alternative, the court affirmed because border agents had reasonable suspicion to forensically search Touset's digital devices.

These three decisions lend judicial support to the CBP's 2018 Border Search of Electronic Devices Directive, which authorizes digital device searches at the border.[13] Searches are limited to information on the device and may not be used to access remotely stored information, like banking records not downloaded. CBP officers may perform basic device searches with or without suspicion. Advanced searches performed by accessing devices electronically require reasonable suspicion of illicit activity. **TBJ**

This article was originally published in the September 2018 edition of Circuits *and has been edited and reprinted with permission.*

Notes

1. *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).
2. *United States v. Ramsey*, 431 U.S. 606, 619 (1977); *United States v. Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018).
3. *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (citing *United States v. Cortez*, 449 U.S. 411, 417–18 (1981)).
4. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985); *Cotterman*, 709 F.3d at 960–61.
5. *Kolsuz*, 890 F.3d at 136.
6. *Id.* at 140, 142 (citing *California v. Riley*, 134 S. Ct. 2473 (2014)).
7. *Riley*, 134 S. Ct. at 2494–95. *Riley* involved domestic arrests.
8. *Kolsuz*, 890 F.3d at 137, 144–45.
9. *Cotterman*, 709 F.3d at 957.
10. *Id.* at 968.
11. 890 F.3d 1227, at 1232–33 (11th Cir. 2018).
12. *Id.* at 1234 (citing *United States v. Vergara*, 884 F.3d 1309, 1312 (11th Cir. 2018)).
13. CBP Directive No. 3340-049A, *Border Search of Electronic Devices* (Jan. 4, 2018).

PIERRE GROSDIDIER

is counsel to Haynes and Boone's business litigation practice group in Houston. He divides his practice between construction litigation and construction contract drafting. Grosdidier belongs to the first group of attorneys certified in construction law by the Texas Board of Legal Specialization in 2017. His practice also includes data privacy, unauthorized computer access, and media and entertainment issues and litigation. Prior to practicing law, Grosdidier worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. Grosdidier is a member of the State Bar of Texas, an AAA panelist, a registered P.E. in Texas (inactive), the State Bar of Texas Computer & Technology Section webmaster, and Circuits *co-editor for 2018-2019.*