Connecticut Law Tribune
MAY 24, 2017 ctlawtribune.com An ALM Publication

Fourth Amendment Exception Allows Customs to Search Personal Devices

By JOE MARTINI AND JAMES GLASSER, WIGGIN AND DANA

Bradley International Airport now boasts direct service to Dublin, Ireland, Edinburgh, Scotland, and various destinations in Canada. Those entering and leaving the United States through Bradley and other international airports and border crossings should be aware of an important exception to the Fourth Amendment warrant requirement and the corresponding broad authority vested in U.S. Customs and Border Patrol (CBP) agents.

CBP agents can search cellphones, laptops and other electronic devices of those entering or leaving the country, regardless of citizenship and despite the vast quantities of extremely personal information stored on those devices. And CBP agents are searching more devices now than ever. Citing data provided by border patrol, the New York Times recently reported searches of electronic devices had quintupled from about 5,000 in 2015 to 25,000 in 2016.

Although the "border search exception" to the Fourth Amendment's warrant requirement is long-standing and well-recognized, recent advances in technology have raised new and significant privacy concerns. Unlike a short time ago when business travelers packed a few files relevant to their trip, almost all travelers now bring along a laptop, iPad or smartphone with the equivalent of several overflowing file cabinets of documents and data. An examination of any one of these devices could reveal more about a person's life than a search of every room of his or her home—and all without a warrant. Fourth Amendment jurisprudence has traditionally shifted to adapt to new technologies, as when the Supreme Court held in Kyllo v. United States , 533 U.S. 27 (2001), and United States v. Jones , 565 U.S. 400 (2012), that the use of thermal imaging devices and a GPS tracking devices, respectively, constitute a search and require a warrant. In keeping with the evolving interpretation of the Fourth Amendment, the historically broad scope of the border search doctrine, as applied to the warrantless searches of electronic devices, has rightly been called into question by judges and advocates. It is also subject to reassessment by virtue of the Supreme Court's recent decision in *Riley v. California*.

In *Riley*, a unanimous court held that "a warrant is generally required" before searching information stored on a cellphone seized during an arrest. 134 S. Ct. 2473, 2493 (2014). The court reasoned that cellphone data "differ[s] in both a quantitative and a qualitative sense" from other physical items, and a search for data "would typically expose to the government far more than the most exhaustive search of a house." Id. at 2389, 2495. Although there may be instances where law enforcement officers may search cellphones without a warrant in exigent circumstances, the Supreme Court left open the question of whether other exceptions to the Fourth Amendment's warrant requirement—such as the border search exception—continue to apply to electronic data.


Joseph Martini, a partner at Wiggin and Dana, New Haven, Conn.

Earlier guidance from the Supreme Court established that under the border search exception, only "routine" border searches are per se reasonable, whereas "non-routine" border searches must rest on some degree of particularized suspicion. Whether a border search is "routine" has been linked to the intrusiveness of the search. Before the court's decision in *Riley*, one appellate court held that a forensic examination of a laptop computer at the border implicates a greater privacy interest than a routine border search, and therefore requires reasonable suspicion. *United States v. Cotterman , 709 F.3d 952, 962-64 (9th Cir. 2014) (en banc). After Riley, courts have reached differing conclusions on whether and to what extent Riley's rationale applies to border searches of electronic devices, often*

focusing on whether a forensic search of a phone's data is intrusive enough to qualify as "non-routine."

Two of these cases, still working their way through the federal court system and currently pending before the Fourth and Eleventh Circuit Courts of Appeals, may serve to clarify the law on warrantless searches of cellphones at the border. In *United States v. Vergara*, Case 8:16-cr-00021-JDW-MAP, Dkt. No. 34 (April 8, 2016), a U.S. citizen was stopped by Customs when disembarking from a cruise ship at the Port of Tampa. After rifling through Vergara's phone, an agent came on a video that he thought constituted child pornography. Homeland Security seized the phone and conducted a forensic examination, the results of which revealed that the phone did, in fact, contain child pornography. Vergara moved to suppress the contents of his cellphone, and the district court denied his request, holding that the manual, "cursory" search conducted by the Customs agent was a "routine" border search that did not require a warrant or even reasonable suspicion. The court also found that the manual search was "constitutionally distinguishable from the more intrusive forensic search conducted at the direction" of Homeland Security, and therefore followed the Ninth Circuit's pre-*Riley* decision in *Cotterman* holding that a forensic examination at the border implicates a greater personal privacy interest than a manual search and therefore requires reasonable suspicion. The district court nevertheless concluded that information learned from the cursory, routine search provided the agents with reasonable suspicion sufficient to conduct the nonroutine, forensic search, and that a warrant based on probable cause was not required.

If the Eleventh Circuit affirms the district court's order, it will be the first appellate court post-*Riley* to hold that reasonable suspicion is required for a forensic examination. Less likely, the Eleventh Circuit might overrule the district court's order, and, as urged by Vergara, become the first court to require a warrant for a border search of a cellphone or electronic device.

A similar case, *United States v. Kolsuz*, Case No. 1:16-CR-53, 2016 WL 2658156 (E.D. Va. May 5, 2016), is pending before the Fourth Circuit. Kolsuz, a Turkish citizen, moved to suppress information obtained from two searches of his cellphone—an initial search of recent calls and text messages conducted at the airport, and a forensic search conducted later at the offices of Homeland Security. As in *Vergara*, the district court held that the manual search was routine and did not require any level of individualized suspicion, and the forensic search was a nonroutine border search justified by "more than reasonable suspicion." *Kolsuz*, 2016 WL 2658156, at *10. The Fourth Circuit might be less likely to disturb the lower court's order in the light of its own pre-*Riley* case upholding the constitutionality of a forensic search of a computer and disks at the Canadian border. See U.S. v. Ickes , 393 F.3d 501 (4th Cir. 2005). Nonetheless, *Kolsuz* has the potential to clarify existing border search law or at least tee up the issue for Supreme Court consideration.

In a concurring opinion in *Riley*, Justice Samuel Alito indicated that he would rather the issue be settled outside of the courts, and urged lawmakers to enact legislation regulating searches of cellphones and electronic devices. Writing that "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment," Alito pointed to the regulation of electronic surveillance as an instructive example of just such legislation from the relatively recent past. *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring). On April 4, Republican and Democratic lawmakers in the House and Senate introduced a bipartisan bill that would require a warrant before federal agents could search citizens' phones, laptops and other electronic devices at points of entry to the United States. Despite significant media coverage of the increasing number of cellphone searches at the border, it is unclear whether support for this bill will be drowned out by the new administration's tough talk on border security.

As Justice Learned Hand observed almost a century ago, it is "a totally different thing to search a man's pockets and use against them what they contain, from ransacking his house for everything which may incriminate him." *United States v. Kirschenblatt , 16 F.3d 202, 203 (2d Cir. 1926). If his pockets contain a smartphone, that is no longer true. Every major advancement in technology calls for a new balancing of security and privacy interests, and with cellphone border searches increasing exponentially, judges or legislators must move quickly to strike the right balance.*

Even in this uncertain environment, there are practical steps that can be taken to limit exposure to forensic searches of electronic devices at the border. Companies and individuals should consider using a "travel only" laptop or phone when traveling internationally, as well as marking and segregating privileged documents or documents that contain trade secret or other confidential or sensitive materials. Employees should also be trained and educated on their rights and the proper response if subject to a forensic search. For instance, employees should be instructed that if an agent asks for their consent to search any devices, they are not obligated to provide consent and may refuse consent. Employees should also understand that they have no obligation to assist CBP agents by, for example, providing passwords for locked devices. ■

Andrew Giering of Wiggin and Dana assisted in the preparation of the article.