THE
NATIONAL LAW REVIEW

IoT Update: Federal Appeals Courts Split on Forensic Searches of Devices Seized at Border

COVINGTON

Article By
Katharine Goodloe
Covington & Burling LLP
Inside TechMedia

- Communications, Media & Internet
- Global
- Immigration

- 4th Circuit (incl. bankruptcy)
- 11th Circuit (incl. bankruptcy)

Thursday, May 31, 2018

Two federal appellate courts are taking sharply different views on whether—and why—government agents must have some amount of suspicion to conduct forensic searches of electronic devices seized at the border.

The Fourth Circuit on May 9, 2018, held that government agents must have reasonable suspicion to conduct forensic searches of cell phones seized at the border. It said that decision was based on the Supreme Court's recognition in *Riley v. California* that phones contain information with a "uniquely sensitive nature." The Fourth Circuit and Ninth Circuit are the only two federal appellate courts to require reasonable suspicion for forensic border searches.

In contrast, the Eleventh Circuit on May 23, 2018, rejected that position—and held that no suspicion is required for forensic border searches of electronic devices. According to the Eleventh Circuit, even after *Riley*, "it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects."

The decisions evince a split in how far courts are willing to apply *Riley*, including whether that decision has any bearing on border searches, which are a narrow

exception to the Fourth Amendment's warrant requirement.

Fourth Circuit: *Riley* Applies to Border Searches

In *United States v. Kolsuz*, the Fourth Circuit analyzed the reasonableness of a forensic search of the cell phone of a Turkish national traveling out of Dulles International Airport who was detained after agents located unlicensed firearms in his luggage.

Kolsuz's phone was seized at the airport and driven to an off-site facility, where agents used an extraction program that took "a full month, and yielded an 896-page report" about the phone's contents, according to the court. That report 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, the court said. Notably, the phone remained in airplane mode during the extraction, so that the forensic program obtained only data stored on the phone itself and not data stored remotely in the cloud.

The Fourth Circuit held this was a "border" search, even though it was conducted several miles from the airport after Kolsuz was in custody. Because the government invoked the border exception in investigating the "transnational offense" of firearms trafficking, the court held there was a "direct link" to the border search rationale, unlike cases in which the government seeks to invoke the border exception "on behalf of its generalized interest in law enforcement and combatting crime."

The court next addressed the level of suspicion required to conduct a forensic search of an electronic device seized at the border. It held that "[a]fter *Riley*, . . . a forensic search of a digital phone must be treated as nonroutine border search, requiring some form of individualized suspicion." According to the Fourth Circuit, 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 dairies covered by the search incident [to arrest] exception." Given that refusal, the court held that "cell phones are fundamentally different . . . from other objects subject to government searches."

Eleventh Circuit: *Riley* Does Not Apply to Border Searches

In *United States v. Touset*, the Eleventh Circuit rejected this reasoning. *Touset* involved the forensic search of two laptops, two hard drives, and two tablets seized at the border after a U.S. citizen arrived at Atlanta's Hartsfield-Jackson International Airport. The forensic searches revealed child pornography on two laptops and the two hard drives—although the court does not explain how those forensic searches were conducted.

According to the Eleventh Circuit, "the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border." That is because the Supreme Court has afforded greater protection to persons than to property and does not distinguish between searches of "different types of property," the court said. It held there was "no reason why the Fourth Amendment would require

suspicion for a forensic search of electronic device when it imposes no such requirement for a search of other personal property."

To reach that conclusion, the Eleventh Circuit relied on its March 2018 decision in *United States v. Vergara*, which held that *Riley* does not apply to border searches because that decision was limited to the search-incident-to-arrest doctrine. (*Vergara* did not address the issue of what level of suspicion was required, because the defendant in that case only argued a warrant was needed—and the court held it was not.) It also distinguished *Riley* by finding that the rationales supporting the border exception still had force when applied to digital information—unlike the rationales supporting the search-incident-to-arrest exception.

Indeed, the Eleventh Circuit suggested that "if we were to require reasonable suspicion for searches of electronic devices, we would create special protection for the property most often used to store and disseminate child pornography." It found "no reason" to "create a special rule that will benefit offenders who now conceal contraband in a new type of property."

Effect Unclear Given CBP Guidance

The practical implications of these cases are not yet clear—particularly because U.S. Customs and Border Protection in January issued guidance requiring reasonable suspicion for forensic searches of electronic devices seized at the border. Given that guidance (summarized in our prior post), it is possible that agents may conduct fewer forensic searches without reasonable suspicion, reducing the frequency with which this issue is litigated. Still, because the guidance contains an exception allowing for suspicionless forensic searches in cases of "national security concern," the issue may arise more frequently in that particular context.