CARLTON FIELDS

U.S. Supreme Court: Warrant Generally Required to Search Information on a Cell Phone, Even Incident to Arrest

July 17, 2014

The United States Supreme Court has ruled that police officers must generally secure a warrant before searching through the contents of a cell phone of a person they arrest.[1] *This decision will have important implications for telecommunications providers, possibly by affecting the number of subpoenas they receive for phone records, and for users who have confidential information on their smart phones. Due to this case, individuals arguably have greater expectations of privacy in the content on their phones.* The case, *Riley v. California*, involved two individuals convicted of crimes (unrelated to those for which they were initially arrested) after police examined information on their cell phones. The government argued that the warrantless search was constitutional under an exception to the usual requirement that officers obtain a warrant.[2] The exception allows officers to search individuals when they arrest them. The Court rejected that argument and focused on the fact that the justifications for such searches – officer safety and preventing the destruction of evidence – are far less applicable to searches of digital information.[3] The Court's opinion recognized that cell phones contain a huge volume of information likely to be intensely personal (raising significant privacy concerns), and unlikely to harm officers (lowering the government's interest in invading that privacy).[4] Given these differences the Court concluded that "a warrant is generally required before [searching a cell phone], even when a cell phone is seized incident to arrest."[5] However, the Court concluded by noting that a different exception to the warrant requirement, one that allows warrantless searches in exigent circumstances, still applies to the contents of cell phones.[6] Thus, if a particular situation requires the police to search a cell phone to "assist persons who are seriously injured or are threatened with imminent injury" or to help out in another emergency, then the police need not obtain a warrant to do so.[7] The implications of the Supreme Court's decision are resounding. Notably, the logic of this case likely also applies to searches of tablets, laptops, and other electronic devices that contain a large amount of potentially personal data.[8] *Riley* will also undoubtedly have a significant effect on common law enforcement practices. Law enforcement

officers can no longer routinely troll through information on cell phones using the excuse that they are merely searching an individual they just arrested. Law enforcement may attempt to justify more cell phone searches under the exigent circumstances exception, which remains available on a case-by-case basis. Also, it may make more requests to cell providers directly using subpoenas and court orders issued under the Stored Communications Act.[9] The *Riley* ruling continues a trend of recent cases that address search and seizure issues in our increasingly digital era[10]. And it highlights the need to update telecommunication laws to keep up with the rapidly evolving pace of technological development (after all, the Federal Communications Act just celebrated its 80th birthday).[11] Indeed, several bills that aim to do just that are pending in Congress,[12] and major changes are expected in the near future at both the national[13] and state[14] level. The House Energy and Commerce Committee is also soliciting feedback from the public and telecom industry on a series of white papers being written in preparation for a major Federal Communications Act overhaul.[15] All signs suggest that *Riley* is just the first of several major changes to come. Our telecommunications and white collar and government investigation groups continue to track these significant developments. We stand ready to assist and advise our clients as privacy law issues continue to evolve.

---

[1] *Riley v. California*, Nos. 13-132 & 13-212, 2014 WL 2864483, at *9 (U.S. June 25, 2014).

[2] *Id.* at *9-12.

[3] *Id.*

[4] *Id.*

[5] *Id.* at *19.

[6] *Id.*

[7] *Id.*

[8] In fact, one commentator has suggested that "[t]he most important takeaway from [*Riley*] is that Digital is Different." Jennifer Granick, SCOTUS & Cell Phone Searches: Digital is Different, Just Security (June 25, 2014, 4:11 PM), http://justsecurity.org/12219/scotus-cell-phone-searches-digital/.

[9] *See* 18 U.S.C. § 2703 (laying out the subpoena procedure).

[10] *See* e.g. *United States v. Jones*, 132 S. Ct. 945, 565 U.S. __ (2012) (law enforcement's warrantless attachment of GPS tracking device to defendant's vehicle violated Fourth Amendment); *United States v. Quartavious Davis*, Case No. 12-12928 (11th Cir. June 11, 2014) (law enforcement's warrantless obtaining of stored cell site location data violated defendant's Fourth Amendment reasonable expectation of privacy, though good faith exception

applied in this instance). We discussed the *Davis* case in a recent article for the *Daily Business Review*, available online at http://bit.ly/1ruGrwY (paywall).

[11] *See* Greg Walden, At 80 Years Old, It's Time for a Tune-Up, Energy & Com. Committee (June 19, 2014), http://energycommerce.house.gov/press-release/80-years-old-it%E2%80%99s-time-tune (noting that the law just celebrated its 80th birthday).

[12] *See* the Electronic Communications Privacy Act Amendments of 2013, S. 607, 113th Cong., available at http://www.gpo.gov/fdsys/pkg/BILLS-113s607is/pdf/BILLS-113s607is.pdf (seeking to update the Electronic Communications Privacy Act), the Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong., available at http://www.gpo.gov/fdsys/pkg/BILLS-113hr983ih/pdf/BILLS-113hr983ih.pdf (proposing the amendment of the criminal statutes to require warrants when obtaining electronic communications and requiring law enforcement agencies to notify subscribers of the warrant).

[13] *See* Brendan Sasso, House to Re-Write Foundational Communications Law, The Hill (Dec. 3, 2013), http://thehill.com/policy/technology/191954-house-to-re-write-foundational-communications-law (reporting that an effort to modernize the outdated Act, last updated in 1996, is underway); Julian Hattem, Thune Sets Stage for Senate Communications Law Overhaul, The Hill (June 25, 2014), http://thehill.com/policy/technology/210543-thune-sets-stage-for-senate-communications-law-overhaul (reporting that the Senate is also expected to overhaul the aging law).

[14] *See* Peter Marcus, New Legislative Take on Old Telecommunications Laws: Bipartisan Package Draws Ire of AARP, The Colorado Statesman (Mar. 28, 2014), http://www.coloradostatesman.com/content/994743-new-legislative-take-old-telecommunications-laws (reporting that nearly a half dozen bills have been introduced in the state legislature to update the State's communications laws).

[15] *See* energy & Com. Committee: #CommActUpdate, http://energycommerce.house.gov/commactupdate (last visited July 3, 2014) (providing updates and information about the revision process).

Related Practices

Cybersecurity and Privacy
Technology
Telecommunications
White Collar Crime & Government Investigations

Related Industries

Technology
Telecommunications