Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Riley Cellphone Search Rule Is Slowly Sweeping The Nation

Law360, New York (September 26, 2014, 10:08 AM ET) --

Carrie Sarhangi

In June, the U.S. Supreme Court issued the landmark Riley v. California opinion, which held that police officers cannot review the contents of a cellphone incident to an arrest absent a search warrant or exigent circumstances. Commentators opined that this bright-line rule would clear up the murky waters created by courts less decisive or intrepid and now, just three months later, the patience of our nation's courts in tolerating warrantless cellphone searches has already waned.

In late August, a New York state trial court suppressed photographs seized from the cellphone of a court observer during the 2012 high-profile sexual assault matter involving Satmar spiritual counselor, Nechemia Weberman. People v. Weissman, No. 2012KN002159, (N.Y. Crim. Ct. Aug. 26, 2014). During the course of the Weberman trial, the presiding judge admonished those in the gallery to refrain from using their cellphones. Despite the judge's explicit direction, the defendant removed his cellphone from his pocket and took photographs of others in attendance at the trial, including the female complainant while she testified.

When defendant Weissman attempted to exit the courtroom, he was stopped by an officer who seized his phone, scrolled through two to three photographs, and then identified the pictures that the defendant took while in the courtroom. While the court conceded that the officer's initial investigation was reasonable, in part, because "the courthouse is an environment where persons have diminished expectations of privacy," it also held that the officer was not permitted to physically seize the phone and view its contents without a warrant. The judge found the search was too expansive in nature and highlighted the officer's viewing of two to three pictures prior to finding the relevant photos as prohibited under Riley. People v. Weissman.

The Pennsylvania Superior Court, too, has applied the Riley rule, thereby affirming their intent to protect citizens' expectation of privacy when it comes to the treasure troves of data found on our cellphones. In July, the Superior Court affirmed the lower court's suppression of photographs found on a cellphone, relying on Riley in finding the seizure "undoubtedly unconstitutional." Commonwealth v. Stem, 96 A.3d 407, 413 (Pa. Super. Ct. 2014).

There, although the cellphone was seized incident to arrest, the police turned on the phone, searched

the cellphone data, and proactively accessed the phone's picture application prior to obtaining a warrant. Although the police officer only viewed a single photo that he believed to be child pornography prior to applying for a search warrant, the court suppressed all 17 photos containing child pornography, unmistakably designating them fruit of the poisonous tree. Commonwealth v. Stem, 96 A.3d at 414.

If the Riley rule is slowly sweeping the nation as Weissman, supra and Stem, supra, indicate, then the question becomes: Just how far do Fourth Amendment protections apply when it comes to the data created on and by our cellphones?

Sure, now your tweets, texts and Facebook posts are protected from warrantless searches, but what about the historical cell-site data that originates from your mobile? Historical cell-site data is a record of a wireless subscriber's calls, including the antenna towers utilized to carry the call to or from the subscriber, and can be used to extrapolate the location of the cellphone user at the time and date of the call. This precious information is routinely captured and maintained by third-party telecommunications companies, i.e., Verizon Communications Inc., AT&T Inc., Sprint Nextel Corp., etc., and if accessed, can "reconstruct someone's specific movements down to the minute, not only around town, but also within a particular building." Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing United States v. Jones, 132 S. Ct. 945, 957 (2012)).

And contrary to the more stringent requirements associated with obtaining a search warrant — a showing of probable cause — federal law only requires a showing of "reasonable grounds" to obtain Verizon's roadmap to where you bought your coffee yesterday and where you met with your client last week. See Stored Communications Act, 18 U.S.C.A. § 2703 (requiring a showing of "reasonable grounds to believe that the … records sought are relevant and material to an ongoing criminal investigation" before a judicial authority to obtain a court order).

Although there seem to be inroads to declaring the SCA unconstitutional, the issue has yet to be teed up before the post-Riley Supreme Court. See, i.e., United States v. Davis, 754 F.3d 1205, 1215 (11th Cir. 2014) (finding that cell-site location data is within a subscriber's reasonable expectation of privacy and that the procurement of such data without a warrant is a violation of the Fourth Amendment); In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317–19 (3d Cir. 2010) (requiring the government to pursue a search warrant and establish probable cause to obtain cell-site records rather than issuing an order pursuant to the SCA); In re Application of United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (denying the government's request for an order under 18 U.S.C.A. § 2703, but holding that orders obtained pursuant to the SCA for historical cell-site information are not categorically unconstitutional).

For the first time, the Riley court's holding and a wireless subscriber's privacy interests in his or her historical cell data came to a head in United States v. Guerrero, No. 13-50376, (5th Cir. Sept. 11, 2014). Echoing Chief Justice John Roberts' theme in Riley that the Fourth Amendment needs to be reconsidered in light of today's ever-changing technological world, the Guerrero defendant argued that the Fifth Circuit should protect his historical cell-site information for privacy-related reasons similar to the Supreme Court's protection of the defendant's cellphone data in Riley.

The Fifth Circuit rejected Guerrero's argument, finding that the two cases involved distinct legal questions: The Riley defendant's issue was whether the search incident to arrest exception overcame the privacy interest for the contents of an arrestee's cellphone and Guerrero's issue was whether a cellphone owner has a reasonable expectation of privacy in information held by a third-party wireless service provider.

Perhaps the most interesting part of the Fifth Circuit's opinion was not its ruling, but its less-than-subtle suggestion that post-Riley, the Supreme Court needs to close the gap between technology and citizens' privacy interests and reconsider the third party doctrine in the context of historical cell site data. United States v. Guerrero.

Until then though, rest assured that you can tweet, text and Facebook to your heart's content knowing that the Fourth Amendment's protections apply to the data created on your cellphone, but be forewarned that the data created by your cellphone is just a court order away.

—By K. Carrie Sarhangi, Montgomery McCracken Walker & Rhoads LLP

Carrie Sarhangi is an associate in Montgomery McCracken's Philadelphia office and an editor of the firm's White Collar Alert blog. Previously, she served as an assistant district attorney with the Major Crimes Division of the Philadelphia District Attorney's office.