CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 159 years

TUESDAY, AUGUST 12, 2014

Chicago Daily Law Bulletin®

Volume 160, No. 158

Court protects privacy in ruling on warrantless searches of cellphones

Every now and then The Nine agree on something. Among the unanimous rulings the U.S. Supreme Court issued in the final stretch this year was Riley v. California, which held that law enforcement officials may not make a warrantless search of a person's cellphone incident to an otherwise lawful arrest.

(Justice Samuel A. Alito Jr. wrote separately but concurred in the judgment. So The Nine mostly agreed, at least.) While some commentators lauded the ruling as a "sweeping" vindication of privacy rights in the digital age, others took a more blasé tone, calling the decision constitutionally sound and protective of individual liberties, but declining to lionize the justices as digital pioneers for grasping that smartphones are fundamentally different from, say, the contents of someone's wallet or glove compartment.

The specific appeals before the court in Riley came from criminal prosecutions in California and Massachusetts. In the California state court case, the petitioner was stopped for driving with expired registration tags, and upon arrest, the police discovered that the man's license had been suspended. A search of the vehicle yielded firearms, and the police seized the petitioner's smartphone and accessed information on the phone (pictures and messages).

Various references led the police to surmise gang affiliations, which ultimately resulted in the petitioner's prosecution and conviction on three counts, including attempted murder, involving a previous assault. Although the petitioner tried to suppress the cellphone-derived evidence, the state courts allowed the evidence, and the conviction was affirmed on appeal.

In the Massachusetts case, the cellphone information was less directly incriminating, but it led police to identify the defendant's "house," where the police conducted (with a warrant) a search that uncovered crack cocaine. While the federal court rejected the defendant's motion to suppress, the 1st U.S. Circuit Court of Appeals overturned the conviction on the basis that the cellphone search was illegal and the proceeding investigations therefore "fruit of the poisonous tree."

Writing for the court, Chief Justice John G. Roberts Jr. began by recounting the jurisprudence on searches incident to a lawful arrest. Roberts focused on two chief concerns underpinning the historical allowance for police to search the contents of a vehicle incident to a lawful arrest: officer safety and evidence preservation.

The court concluded that neither concern — other than in the most extraordinary cases — justified the warrantless search of data on an arrestee's cellphone. An officer can check a phone to make sure that, for example, there's not a razor blade hidden between the phone and its case (probably not much of an ongoing threat, in light of the court's ruling) and can also secure the phone and then obtain a warrant to later search its contents.

Reviewing all the data stored on a phone, including browser history and a user's apps, may very well reveal more about the user than a search of that person's house.

Although the federal government (appealing the 1st Circuit decision) and the state of California argued that technology allowing phones to be scrubbed remotely posed a significant evidence-destruction threat, the court treated this argument fairly dismissively.

The record failed to support a conclusion that remote scrubbing was prevalent or that real-time searches were necessary to preserve evidence. And to the extent the threat is real, the court wasn't convinced that permitting warrantless searches would address the problem so as to justify the privacy intrusion.

While not exactly characterizing the government's concerns as red herrings, Roberts demonstrated some impatience at the notion that a cellphone search was indistinguishable from more traditional — that is, physical — searches: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."

From a broader privacy perspective, the core of the opinion lies in the court's statements concerning the particular qualities of cellphones and their immense data storage capabilities. Roberts recognized that even the term "cellphone" doesn't capture the essence of smartphones — that they are, essentially, handheld computers — and that the "sum of an individual's private life can be reconstructed" by looking at a phone's digitally stored contents.

He noted not only the capacity of smartphones, but their pervasiveness and their wide-ranging uses. Reviewing all the data stored on a phone, including browser history and a user's apps, may very well reveal more about the user than a search of that person's house. (Unless, as Roberts added, the phone is in the house.)

With perhaps broader implications, the court also discussed the particular problems raised by cloud computing. A cellphone user often would not know which materials are stored on their devices and which are stored remotely, "in the cloud." And what may be stored locally on one device may be stored remotely on another.

Although the government conceded that it had no claim to warrantless searches of materials accessed remotely, the court was unsatisfied by the government's suggestions for addressing the problem. Roberts directed a zinger at the proposal that law enforcement agencies "develop protocols to address" cloud computing: "Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols."

With language this rousing (and amusing), it's actually not so surprising that some labeled the opinion as "sweeping." The court also rejected a variety of limiting principles, such as the suggestion that the searches be permitted but only insofar as they obtained material that could have been obtained through a pre-digital search. Indeed, Roberts expressed what may be viewed as a fair skepticism toward how law enforcement officers might manipulate these supposed restrictions in practice.

While privacy "comes at a cost," the court regarded the exigent circumstances exception as sufficient to provide law enforcement authorities with the opportunity to conduct cell phone searches in truly extreme situations, such as the hypotheticals of "a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cellphone." In general, the court admonished, the message is clear: Get a warrant.

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a partner in Loeb & Loeb's Chicago office. She focuses on matters involving the convergence of advertising and promotions, emerging media, technology and privacy law as well as intellectual property law. She can be reached on nmcginn@loeb.com.