Litigation Alert: Supreme Court Defends Expectation of Privacy In Cell Phone Data

JUNE 26, 2014

Fenwick
FENWICK & WEST LLP

The Supreme Court, in a unanimous decision, limited the ability of law enforcement to search cell phones while making arrests, requiring police to obtain a search warrant before examining the data contained in an arrestee's device. *Riley v. California*, 573 U.S. ___ (2014). For David Riley and Brima Wurie, the appellants and defendants in two jointly decided cases, the ruling means that the data collected from their respective cell phones and evidence derived from that data should have been suppressed before trial. While much of Chief Justice John Robert's opinion centers upon Fourth Amendment precedent, it also implicates distinctive privacy related characteristics of cell phone data and cloud computing.

The opinion reflects the Court's view that individuals have substantial privacy interests in information stored on their cell phones, at least in the context of government searches. This reasonable expectation of privacy stems from the Court's finding that "modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse" because of both the quantity and types of data people store on mobile devices. Slip op. at 17.

The quantitative aspect of the Court's analysis focuses upon the immense storage capacity of mobile phones. The opinion explains that a cell phone's distinctive ability to store "millions of pages of text, thousands of pictures, or hundreds of videos" leads to three privacy related consequences: the ability to combine distinct types of information, the capability to convey vast amounts of data, and the potential to reveal data that can date back for years. Slip op. at 18. In fact, the decision indicates that the "cache of sensitive personal information" on a cell phone would often expose "far more than the most exhaustive search of a house." Slip op. at 19, 20.

Of even greater potential significance for future privacy cases, the Court also found that the qualitative differences in the data stored on cell phones as compared to physical records serve as a basis for device owners' privacy expectations. Unlike physical records, cell phone data reveals private interests, movements, concerns, and hobbies:

> "An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. *See United States v. Jones*, 565 U. S. ___, ___ (2012) (SOTOMAYOR, J., concurring) (slip op., at 3) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."). Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life."
>
> Slip op. at 19, 20.

This language, while dicta, suggests that individuals have constitutionally protected privacy interests in each of these categories of information, at least for purposes of a government search of their personal devices. What remains to be seen is whether the Court and lower courts tasked with following *Riley* will apply this reasoning to government requests for similar data that is stored by third parties, such as phone companies, ISPs and other online service providers. The opinion gives those providers legal ammunition to insist on a warrant before turning over such records. The opinion also leaves open the question of whether businesses that make commercial use of data stored on or generated by users' mobile devices without their

consent face civil tort liability for common law invasion of privacy.

Riley was also the Court's first foray into the privacy issues of cloud computing. As an additional basis for requiring law enforcement to obtain a warrant before searching a cell phone, the Court cited the fact that many forms of data that appear to be stored on a phone are actually stored on a server in the cloud: "[C]ell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference." Slip op. at 21. This suggests that a majority of the Court would find that individuals may have a constitutionally protected expectation of privacy to data they store on remote servers, at least in the context of government searches. This dicta gives cloud service providers a strong legal foothold to require law enforcement seeking the contents of subscribers' online storage accounts to obtain a warrant, even though the Stored Communications Act can be read to require only a subpoena with notice or a court order. The opinion also likely bolsters the cause of privacy advocates and service providers who have been pushing Congress to amend the Electronic Communications Privacy Act to require law enforcement to obtain a warrant for all stored online content. Although the impact of *Riley* beyond cell phone searches by law enforcement remains to be seen, the case is likely to be heavily cited in both civil and criminal privacy cases for years to come.

For more information please contact:

Tyler G. Newby, Partner
415.875.2495; *tnewby@fenwick.com*

Zachary Lerner, Summer Associate,
Harvard Law School, Class of 2015
650.335.7545; *zlerner@fenwick.com*