A Timely Analysis of Legal Developments

ASAP®

July 10, 2014

Five Lessons for Employers from *California v. Riley*

By Phillip Gordon

In the waning days of its current term, the U.S. Supreme Court ruled unanimously in *California v. Riley* that police officers generally violate the Fourth Amendment's prohibition against unreasonable searches by conducting a warrantless search of a smartphone seized incident to an arrest. The ruling turned largely on the Supreme Court's interpretation of a long-established exception to the Fourth Amendment's warrant requirement. Although the Fourth Amendment and the relevant exception will rarely apply to private employers, the high court's decision remains highly relevant for private employers whose workplace searches, like police searches, increasingly encounter personal smartphones, whether as part of a bring your own device program or not, and other mobile devices.

The Supreme Court's decision provides five key takeaways for private employers that we discuss below. At the end of this article, we supplement those takeaways with recommendations for workplace searches of employees' personal smartphones and other mobile devices. Employers should note that the high court's decision does not affect their ability to search company-owned mobile devices. Because they own those devices, employers can establish as a condition of use that employees waive any expectation of privacy in information— whether business or personal— stored on the device.

Private Employers Must Treat Smartphones Differently From Other Personal Property When Conducting a Workplace Search

In the words of the Supreme Court, "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." Those heightened privacy concerns derive from the quantity of data that can be stored on the device and the nature of that information. Taken together, those attributes permit searches of a personal smartphone to reveal to private employers far more about an employee than searches of any other type of personal property that might be brought to the workplace.

The massive memory of smartphones is well known. As the Supreme Court pointed out, the standard, 16 gigabytes memory of today's top-selling smartphone "translates to millions of pages of text, thousands of pictures or hundreds of videos." The Supreme Court emphasized that it is not just the sheer quantity of data that distinguishes a smartphone from other personal property. Several other aspects of smartphone data storage can make a search of the device highly invasive.

First, the distinct types of information stored on a smartphone "reveal much more in combination than any isolated record." Second, smartphones often contain months', if not years', worth of information, dating back to the device's purchase and even earlier. Third, Internet browser history can reveal "an individual's interests and concerns." Fourth, "historic location information ... can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." Finally, the Supreme Court noted that the "average smartphone user has installed 33 apps, which together can form a revealing montage of the user's life."

The Supreme Court highlighted the potential intrusiveness of a smartphone search by comparing it to the search of a house, the sanctum sanctorum for Fourth Amendment purposes. The high court concluded in the following language that a smartphone search can be far more invasive:

> Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

This same analogy can be used with equal force against a private employer who has searched an employee's personal smartphone without taking the steps recommended below to mitigate risk.

Courts Will Likely Apply the Same Privacy Standards to all Mobile Devices

While the Supreme Court's ruling focused on smartphones, private employers likely will confront a variety of mobile devices when conducting workplace searches, ranging from flip phones to tablets to laptops. The high court's ruling suggests that private employers should not expect courts to be receptive to arguments trying to differentiate among these devices based on their technical capabilities.

To illustrate the point, the Supreme Court issued its ruling in companion cases, one involving a flip phone and another involving a smartphone. The high court made no distinction in its analysis between the two devices because all mobile phones have fundamentally similar storage capacity and capability. It noted that, "Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, thousand-entry phone book and so on."

Private Employers can Still Search Employees' Personal Smartphones

While the Supreme Court recognized that individuals' privacy interests in their smartphones are "weighty," its ruling specifically rejected the notion that those interests immunize smartphones from a search by law enforcement. As stated by the Court, "Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to an arrest."

A private employer, of course, is not required to obtain a warrant to establish the reasonableness of a search of an employee's personal smartphone. However, the types of factors that courts will consider in deciding whether to issue a warrant to search a smartphone can inform an employer's decision whether its own smartphone search is reasonable.

These factors include the strength of the employer's suspicion that the smartphone contains evidence of unlawful conduct or policy violations; the time, place and manner of the search; and the nature and scope of the search. Employers should strongly consider evaluating these factors before searching an employee's personal smartphone because under common law, an invasion of privacy generally is actionable only if the intrusion would be highly offensive to a reasonable person. That element of the tort turns on a balancing of the employee's "weighty" privacy interests against the employer's legitimate business interests and the method by which the employer sought to accomplish those interests.

Searching an Employee's Smartphone Without Consent Could Potentially Trigger Liability Under State and Federal Computer Trespass Laws

All 50 states have outlawed computer trespass and the federal Computer Fraud and Abuse Act also criminalizes computer trespass. Several of the state laws and the CFAA supplement their criminal sanctions with civil remedies. Most of these laws were enacted long before smartphones entered the marketplace. Consequently, they almost uniformly define a fundamental element of the crime as unauthorized access to someone else's computer without addressing the question whether a smartphone is a computer for purposes of the statute.

The Supreme Court's decision did not specifically address state computer trespass laws or the CFAA. However, the Court did note, in dicta, that the "term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." While this dicta is not controlling precedent, courts applying computer trespass laws could rely on it to conclude that those laws apply to smartphones.

Beware: Smartphones are a Gateway to 'the Cloud'

The Supreme Court's decision identifies yet another reason for distinguishing smartphone searches from searches of other personal property (i.e., "a cell phone [can be] used to locate data elsewhere at the tap of a finger"). More to the point, "cloud computing" allows "Internet-connected devices to display data stored on remote servers rather than on the device itself." Notably, even the U.S. conceded in its brief that law enforcement cannot rely on the exception to the warrant rule for searches incident to an arrest to justify a search of data in the cloud that is accessible through a suspect's smartphone.

Similarly, private employers who search an employee's smartphone must beware of accessing information stored in an employee's cloud accounts, for example, by clicking on an app that permits direct access to an online storage account, such as Dropbox, or to a web-based email account, such as Hotmail. Information stored in such accounts may be protected not only by state computer trespass laws and the CFAA but also by the federal Stored Communications Act, another computer trespass law that provides for both criminal penalties and civil damages. The SCA generally prohibits unauthorized access to electronic communications in electronic storage at an electronic communications service. While the SCA's application to cloud computing remains somewhat unsettled, an adverse ruling on an SCA claim could expose an employer to substantial liability.

Recommendations for Employers

In light of the Supreme Court's recent decision in Riley, private employers should consider taking the following steps before searching an employee's personal smartphone and when conducting the search:

1. Recognize that searches of employees' personal smartphones and other mobile devices are high-risk endeavors that should be undertaken only in consultation with legal counsel.
2. Do not reflexively rely on workplace search policies applicable to searches of backpacks, briefcases and even cars when searching an employee's personal smartphone.
3. Whenever feasible, request and obtain consent in writing before searching an employee's smartphone. Confirm that the scope of the consent is consistent with the intended scope of the search and limit the search to the scope of the consent.
4. Before searching an employee's smartphone without consent, consult with counsel concerning the potential application of state computer trespass laws or the CFAA. If the smartphone can be searched without violating these laws, structure the search in a way that a court likely would deem reasonable in the event of an invasion of privacy claim.

Take steps to avoid accessing information stored in cloud accounts, for example, by placing the device in airplane mode or by not opening apps. Keep in mind that even these steps might not prevent an employer's unauthorized access to information stored in the cloud because, for example, an employee might synchronize a personal email account with a work email account, allowing those personal emails to be downloaded before the phone is set to airplane mode and without tapping any apps.

Phillip Gordon, Co-Chair of Littler's Privacy and Background Check Practice Group, is a Shareholder in the firm's Denver office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, or Mr. Gordon at pgordon@littler.com.