REPRINTED FROM:
App Developer Magazine
July 2014
Source: http://appdevelopermagazine.com

ALPERT BARR & GRANT
A Professional Law Corporation

Riley vs. California: A "Revoltin' Development" or Recognition of the Importance of Digital Privacy?

By Adam D.H. Grant

On June 25, 2014, the United States Supreme Court issued its opinion in David Riley vs. California 573 U.S. ___ (2014) which addressed the question of whether the police properly searched Riley's mobile phone as part of a traffic violation stop. The officer accessed information on the phone and noticed the repeated use of a term associated with a street gang.

At the police station two hours later, a detective specializing in gangs further examined the phone's digital contents. Based in part on the photos and videos the detective found, the stated charged Riley in connection with a shooting that occurred several weeks earlier and sought an enhanced sentence based on Riley's gang membership. Riley moved to suppress all evidence that the police obtained from his cell phone. The trial court denied the motion and convicted Riley. The Court of Appeal affirmed the denial and the conviction. However, the Supreme Court reversed the judgment and remanded the case to the trial court.

What does all this mean? It reminds me of the popular radio comedy, "The Life of Riley." Chester Riley worked at a fictitious aircraft plant in California, but the show primarily involved Riley's antics at home. Riley's regular use of malapropisms and awkward interventions in minor problem lead to the radio show being one of the most popular during the 1940's. Riley's stock answer to every turn of fate became a widely used phrase, "what a revoltin' development this is!" Fast forward 75 years and things seem to have progress from "revoltin" to downright wonderful in the area of mobile phone digital privacy. In this ruling, David Riley likely uttered Chester Riley's oft quoted phrase when he learned of his conviction and of the Court of Appeals' affirmation. Yet when David read the decision, I am sure he felt elated and not "revoltin."

After digital privacy experts read the decision, I am sure they will feel just like David. The decision includes an extensive discussion of privacy rights associated with the data stored on everyone's mobile phone. Justice Robert observed that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Further, in rejecting the United States assertion that searching data stored on a cell phone is materially indistinguishable from searches of a person's physical items, Justice Robert retorted, "[t]hat is like saying a ride on a horseback is materially indistinguishable from a flight to the moon." The court particularly noted the immense storage capacity of the most common phone equates to far more than anyone ever stores in their own home.

As this case involved the police officer's ability to conduct a warrantless search incident to a traffic stop, the court tracked the three key cases involved in such searches. In Chimel vs. California (1969) 395 U.S. 742, when analyzing a warrantless search of a home, the court laid down the groundwork for the current search incident to arrest doctrine. The court concluded that "[w]hen an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapon that the latter might seek to use in order to resist arrest or effect escape."

Four years later in United States vs. Robinson (1973) 414 U.S. 218, the court turned its attention to a warrantless search of the arrestee's person. In concluding the search was reasonable, the court explained that, "[t]he authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect."

Finally, the court in Arizona vs. Gant (2009) 556 U.S. 332, recognized the Chimel concerns for officer safety and evidence preservation underline the search incident to the arrest exception. However, the court allowed a warrantless search of a vehicle's passenger compartment "when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."

Using this trilogy of cases as the backdrop, the court made some interesting observations. First, it declared that the data stored on a cell phone "cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. I assume the court was not advised of certain mobile app's ability to immediately issue a "panic" alert to pre-determined recipient's emails via text as to the location of the person and his/her immediate need. One could certainly imaging such an app being used to broadcast to other criminals the arrestee's exact location and a message indicating he was being detained by police. Clearly such information could be used to intercept the arrest or harm the arresting officers.

The court further opined that once the police offers secured a cell phone, "there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone. I would further assume that the judges did not hear about blue tooth enabled apps that wipe all data from a phone when they lose blue tooth connection with a blue tooth enabled hardware "tethered" to the phone.

However, the court recognized a key component to the issue of privacy, "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." First, the immense storage capacity of a phone means a person can have more information in their pocket than their entire house could ever hold. The type of data a cell phone collects is equally diverse; photos, video, address, bank statements or a prescription or only a few types of data. This accumulated data can date back years.

The court also noted that "certain types of data are also qualitatively different." Internet browsing history can reveal a person's private interests or concerns. Additionally, such history can give insight into a person's medical condition if the history includes many searches related to a particular disease.

Most notable is the court's discussion of the use of mobile apps with cell phones. The court recognized that "the average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life. The court even recognized there are over a million apps available in each of the two major app stores.

In the end, the court ruled that given the immense quantity and quality of information stored on a person's cell phone, the intrusion into a person's privacy is far greater than any legitimate governmental interest in searching the data in the phone incident to an arrest. The court specifically left open the possibility of a warrantless search if it was presented with evidence of exigent circumstances which were not present in this particular arrest.

The recognition that intrusion into the data stored on a person's cell phone is greater than evidence located in a person's home will likely be used to strengthen privacy laws and increase the use of privacy notices. Additionally, appreciation of the quality of information and the ability to creating personally identifiable information from non-identifying sources will likely lead to the expansion of the need to properly disclose when certain information is obtain and what the information will be used for by the company.

© App Developer Magazine 2014