Bloomberg BNA

Criminal Law Reporter™

SEARCH AND SEIZURE

Courts Defer to Individual Privacy Interests by Requiring Warrant To Obtain Cell Phone Data and Cell Site Records in *Riley* and *Davis*



BY ANDREW SERWIN, ANNA FERRARI AND LIBBY GREISMANN

Two recent opinions have significantly restricted the practice of warrantless collection of data stored on cell phones or by cell phone service providers. In *Riley v. California*[1] the U.S. Supreme Court confirmed that a warrant is a precondition for law enforcement to perform a search of cell phone data in the context of a criminal arrest. In a separate case considering the warrantless collection of cell site location information, the Eleventh Circuit recently held in *United States v. Davis*[2] that this practice violates the Fourth Amendment.

Riley v. California

Background. The Supreme Court considered two companion cases, *Riley v. California* and *United States v. Wurie*, raising the common question of whether the police may search digital information on a cell phone seized in connection with the arrest of the phone's owner. In the former, a police officer stopped defendant David Riley for driving with expired registration tags. The officer discovered Riley's license had been suspended, which led to an investigatory search of the car and, ultimately, to Riley's arrest. Riley's smartphone, seized in the search incident to his arrest, was found to contain photographs of Riley standing in front of a car that police had previously linked to a shooting. Based on this evidence, Riley was charged with, and convicted of, assault and attempted murder. The trial court denied Riley's motion to suppress evidence obtained from his cell phone on the basis that it had been obtained without a warrant and was not justified by exigent circumstances. The California Court of Appeal affirmed the trial court's ruling, relying on California case law that permitted warrantless searches of cell phone data provided that the cell phone was on the arrestee's person at the time of the arrest.[3] The California Supreme Court declined Riley's petition for review.

In *Wurie*, police officers observed defendant Brima Wurie making an apparent drug sale. Wurie was arrested, and a ''flip phone'' was seized from his person. After it had been seized, the phone received several calls from a phone number identified as ''my house.'' The officers used the phone to determine the phone number associated with ''my house'' and used a directory to trace the number to Wurie's residence. The officers obtained a warrant to search the residence. Based on evidence obtained through this search, Wurie was charged with distributing crack cocaine, possessing crack cocaine with intent to distribute, and being a felon in possession of a firearm and ammunition. He

[1] 134 S. Ct. 999, 95 CrL 445 (U.S. 2014).
[2] 95 CrL 382 (11th Cir. 2014).
[3] See *People v. Diaz*, 51 Cal. 4th 84, 88 CrL 392 (Cal. 2011).

 ISSN 0011-1341

was later convicted of all three counts. The U.S. District Court for the District of Massachusetts denied his motion to suppress, which challenged the constitutionality of the search of his flip phone that led to the search of his residence on Fourth Amendment grounds. The First Circuit reversed, holding that cell phones should be distinguished among other items on an arrestee's person that may be searched incident to an arrest because they contain a host of personal data, and the limited threat presented by cell phones to law enforcement interests does not outweigh the intrusion upon the private information stored in the phone.[4]

Supreme Court Ruling. In a unanimous opinion authored by Chief Justice John G. Roberts Jr., the Supreme Court concluded that a warrant is necessary to conduct a search of an arrestee's cell phone data. The court identified two justifications for proceeding with a warrantless search of the area within the ''immediate control'' of an arrestee: protecting officer safety and preserving evidence. *Chimel v. California*, 395 U.S. 752 (1969). To establish the lawfulness of a search incident to an arrest, case law does not require a ''case-by-case adjudication'' of whether a suspicion exists that the arrestee may be armed or that evidence may be destroyed. *United States v. Robinson*, 414 U.S. 218, 235 (1973). *Robinson* concerned an officer who made an arrest for driving with a suspended license and conducted a warrantless inspection of the contents of a crumpled-up cigarette carton in the arrestee's pocket because the officer couldn't identify the contents (later confirmed to be capsules of heroin) without opening the carton. The Supreme Court affirmed the search, although it was not premised upon a specific concern about evidence destruction or officer safety because, as ''a custodial arrest of a suspect based on probable cause'' is lawful, ''a search incident to the arrest requires no additional justification.''

The court questioned whether applying *Robinson* to cell phones in particular would ''untether the rule from the justifications underlying the *Chimel* exception, given the large volume of personal data that cell phones are capable of storing.'' Indeed, the type of information stored on a cell phone is so unlike the physical property that was ascertained through the search in *Robinson* that the court found the issue to be outside the scope of *Robinson*. As to the first *Chimel* factor—risk of harm to the officer—the court reasoned that any threats to an officer's safety could be determined from the physical aspects of the phone alone and did not require review of any data stored on the phone. As to the second *Chimel* factor—spoliation—the court acknowledged that cell phone data is vulnerable to destruction through encryption and remote wiping, but it concluded that both of these concerns went beyond the scope of what an arrestee could do to destroy evidence within his reach. Further, it is unclear that the ability to conduct a warrantless search would lessen the chance of encryption, and law enforcement could aim to prevent remote wiping simply by disconnecting a phone from its network. Ultimately, the court concluded that such concerns were better addressed through more targeted means, such as the warrant exception for exigent circumstances.

The court also grounded its ruling in the arrestee's pronounced privacy interest in the vast amounts of data stored on a personal cell phone. The court rejected the government's argument that cell phone data is ''materially indistinguishable'' from the information that would be implicated by the search of a wallet, purse or diary. By contrast, the court found cell phone data to be fundamentally different in terms of their volume (the large storage capacity of modern phones), ''pervasiveness'' (the fact that the records touch many aspects of a person's life), and qualitative aspects (such as web browsing history, geolocation data and aggregation of personal information in mobile application software). Further, because a cell phone is not only itself a repository of information, but also a portal for accessing data stored using cloud computing, it may not be apparent to the searching party whether searched data is stored locally or pulled from the cloud. (As the court said, ''Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.'') This creates a major risk as to whether the scope of the resulting search would be actually limited to records and effects within close physical proximity to the arrestee.

In a concurring opinion, Justice Samuel A. Alito Jr. questioned whether the underlying rationale for searches incident to an arrest is not actually officer safety or evidence preservation but rather to obtain probative evidence. Instead, he found that these two rationales are served by seizing and securing items found on an arrestee's person, not by searching them. Justice Alito also noted that the majority's ruling creates a likelihood that the same type or category of information could be entitled to different levels of protection depending upon whether it was stored in physical or electronic form. The concurrence suggested that the court would be better positioned to resolve such anomalies if the legislation drew more refined distinctions about how to treat particular categories of information.

Implications. *Riley* makes clear that a warrant is needed to perform a search of cell phone data incident to an arrest, and the ruling will subject law enforcement to more judicial oversight as they attempt to search the contents of cell phones. To comply with *Riley*, law enforcement must adjust their tactics and focus on seizing and securing cell phones so that their contents may later be searched if a warrant issues.

The *Riley* opinion identifies many similarities between smartphones and computers, such as the type of data generated and stored by each and the availability of software applications on each that collect and use personal data. The concerns raised in *Riley* may require

[4] *United States v. Wurie,* 728 F.3d 1, 93 CrL 268 (1st Cir. 2013).

Andrew Serwin is a partner in Morrison & Foerster LLP's global privacy and data security practice group in San Diego. Anna Ferrari is a senior associate in Morrison & Foerster's privacy and employment practice groups and is resident in the firm's San Francisco office. Libby Greismann is an associate in Morrison & Foerster's Washington office, where she focuses her practice on complex privacy and data security issues.

  CRL ISSN 0011-1341

reconsideration of the standards for performing warrantless searches of other electronic media and application, such as personal computers and social media account information.

In addition, although *Riley* arose in the criminal arrest context, its sweeping language about the privacy interest in the contents of one's personal cell phone will surely be relied upon by plaintiffs challenging the practices of companies that collect and use their personal data without consent. Indeed, the opinion's detailed analysis of the basis for an arrestee's privacy interest in the types of information that may be stored on a cell phone, such as Internet search histories or geolocation data, may soon be found to apply with equal force to collections performed by a nongovernmental entity. Similarly, although *Riley* principally concerns data that is stored locally on cell phones, dicta in *Riley* will lend support to service providers' objections to broad, warrantless government requests for subscriber records, such as cloud data.

United States v. Davis

Background. The information at issue in *Davis*—cell site location information—typically reveals a record of calls made or received by the customer of a cell phone provider. However, this information also typically includes which cell tower carried each call, and it is therefore generally possible to deduce the approximate physical location of the customer. Prior courts had held that the Stored Communications Act, 18 U.S.C. § 2701 et seq. (SCA), permitted a governmental entity to ''require a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service'' pursuant to a court order (Section 2703(c)(1)(B)). This type of order was generally issued upon a showing of ''specific and articulable facts,'' a lesser standard than the Fourth Amendment's probable cause requirement.

Defendant Quartavious Davis was convicted of theft, conspiracy and possession of a firearm in connection with a string of seven robberies of commercial establishments. The government obtained cell site location information from Davis's cell phone service providers pursuant to Section 2703(c)(1)(B), and this information was used to convict him. In support of reversal, Davis argued that the admission of stored cell site location information that the government had obtained from Davis's cell phone provider by court order without a warrant violated the Fourth Amendment.

Appellate Decision. On appeal, Davis contended that obtaining the cell site location data without a warrant violated his constitutional rights under the Fourth Amendment and the government asserted that such evidence was properly obtained by court order under the SCA.

The Eleventh Circuit acknowledged the well-settled principle that the Fourth Amendment applies to warrantless searches and seizures of electronic data, but it questioned whether that protection was limited to the content of the data as opposed to its transmission. The court analyzed *United States v. Jones*,[5] in which the Supreme Court found that the warrantless use of a GPS tracking device to monitor the movements and location of a suspected drug dealer's car violated the defendant's Fourth Amendment rights. The Eleventh Circuit's opinion walked through the two distinct views of the interests protected by the Fourth Amendment: the property-based ''trespass theory,'' in which the amendment protects the property rights of the people, and the more modern view that the Fourth Amendment protects the privacy rights of the people whether or not the search constituted a trespass. Although *Jones* was decided under the trespass theory (in that the placing the GPS device on Jones's car constituted a trespass), four justices concurred that the same result could have been reached under a privacy theory.[6]

Although there had been no trespass to Davis's person or property, the court found *Jones*'s privacy analysis instructive. In *Jones*, the Supreme Court rejected the government's argument that the defendant had no reasonable expectation of privacy with respect to the location and movement of his automobile on public streets. Although each of a car's individual movements on public streets is exposed to the public and may be observed, a car's movements, aggregated together over the course of weeks, is not so exposed and the expectation of privacy in those movements is reasonable. Under this principle, referred to as the ''mosaic theory,'' such aggregated information would potentially reveal more private information than could be extrapolated from individual pieces of information about a person's whereabouts.

The *Davis* court found that a cell phone, which can accompany its owner virtually everywhere, undetected, would be less exposed to the public than a car's travel might, giving rise to a stronger argument in support of a reasonable expectation of privacy on the part of the cell subscriber. The Eleventh Circuit also stated that, unlike GPS location data, which under *Jones* is protected only in the aggregate, even a single point of cell site location data should be presumptively private.[7]

Although the government attempted to distinguish *Jones* on the basis that GPS location data is more precise than cell site location data, the court found this argument to contradict the very reason the location evidence was offered in the first place. If the data revealed sufficient information about a person's location to support a criminal conviction, it did not follow that the location information would remain too vague to violate a person's reasonable expectation of privacy.

The government's argument that Davis waived his expectation of privacy by disclosing his location information to his cell phone provider when he placed calls was also found to be unpersuasive. The court found no

[5] 132 S. Ct. 945, 90 CrL 537 (2012).

[6] *Jones* at 958 (Alito, J., concurring). In a separate concurrence, one additional justice considered the potential application of this theory but found it unnecessary to reach the merits of its application because the trespass theory ''supplies a narrower basis for decision.'' *Jones* at 957 (Sotomayor, J., concurring.)

[7] The court said: ''[E]ven on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way. . . . Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one . . .That is, [cell site data] is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private.''). *Davis* at **24.

indication that Davis knowingly and voluntarily disclosed his location with respect to the calls that he placed and that no disclosure could have been made by Davis with respect to the calls that he received.

Although the court concluded that Davis had a reasonable expectation of privacy in his cell site location data, and that obtaining such data without a warrant violates the Fourth Amendment, admission of this data at trial did not constitute reversible error. Because the court order was issued pursuant to judicial mandate, the ''good faith'' exception to the exclusionary rule applied.

A Conflict in Holdings. The Eleventh Circuit is not the first court to conclude that individuals have a protectable privacy interest in location data generated from cell phones. The New Jersey Supreme court held previously in *State v. Earls*[8] that the New Jersey Constitution protects an individual's privacy interest in the location of his or her cell phone such that law enforcement officers must obtain a warrant based upon a showing of probable cause, or qualify for an exception to the warrant requirement, before they may obtain related records. The *Earls* court analogized the Supreme Court's concurrences in *Jones*, while acknowledging that because *Jones* was decided under a trespass theory, it did not compel a warrant. In that respect, *Davis* expands upon *Earls* by suggesting that the Fourth Amendment does require either a warrant or a qualifying exception to the warrant requirement.

Davis, however, is in conflict with Fifth Circuit precedent finding that the government may seek location data from cell phone service providers without a warrant. *In re Application of the United States of America for Historical Cell Site Data*[9] reversed a district court's adoption of a magistrate's ruling denying the government cell site location records on Fourth Amendment grounds, holding instead that the magistrate did not have discretion to refuse to grant an order where a showing of ''specific and articulable facts'' had been made. In so ruling, the Fifth Circuit relied on the fact that the location data is a business record maintained by the third-party service provider and in that way is similar to other records that may be obtained by a subpoena. Unlike the Eleventh Circuit, the Fifth Circuit also concluded that the subscriber had conveyed its location data voluntarily to the cell phone service provider in the course of using the phone to make calls.

The Fifth Circuit's opinion echoes a prior Third Circuit ruling, *In the Matter of the Application of the United State of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*,[10] which reversed an order declining to provide cell phone location information on Fourth Amendment grounds, and holding that a magistrate judge may require a warrant only after considering whether the government has met the SCA's ''specific and articulable facts'' requirement.

The *Davis* court acknowledged these two prior rulings but declined to analyze them further because each arose in the context of a criminal investigation, as opposed to a pending criminal proceeding and because the Third Circuit's decision predated *Jones*.

The end result of *Davis*, however, extends beyond the reach of *Jones* by finding that even a single point of cell site location data is presumptively private. This conclusion is somewhat at odds with the *Davis* court's own observation that ''committing a crime is certainly not within a legitimate expectation of privacy.'' In spite of this tension, *Davis* does not appear to require a court to conduct a factual inquiry into whether a reasonable expectation of privacy actually exists in the specific context of where the phone user was—such as whether on public or private property—and what he or she was doing with the cell phone. As a result, cell site location data would require a warrant where surveillance camera footage would not, even where both pieces of evidence had been procured by third parties (and not the government) for their own business purposes and both similarly placed a criminal defendant at the scene of a crime.

Implications. The circuit split resulting from *Davis* suggests this issue is well-suited for Supreme Court review.[11] If upheld, *Davis* would expand Fourth Amendment doctrine to include the premise that certain facts about an individual's location are inherently private, such that they cannot be discovered using cell site location data obtained without a warrant, even though comparable information about a subscriber's whereabouts may already be in the public domain. A holding of this scope may have significant consequences for companies that maintain consumer location records and that may be asked or ordered to disclose these records in connection with criminal investigations and proceedings. In deference to *Davis*, pending further clarification from the Supreme Court, such companies should respond to requests for such information only where a warrant has been issued. Although *Davis* found that the district court did not err by failing to suppress cell site location evidence obtained in good faith pursuant to a court order, it is not clear from *Davis* whether a comparable good-faith exception would afford service providers with a defense to civil liability for the unlawful disclosure of this information.

[8] 214 N.J. 564, 93 CrL 552 (N.J. 2013).
[9] 724 F.3d 600, 93 CrL 605 (5th Cir. 2013).
[10] 620 F.3d 304, 87 CrL 851 (3d Cir. 2010).
[11] *Earls*, which was decided narrowly on the basis of New Jersey state law, is not in conflict with either holding, because Section 2703(d) of the SCA expressly defers to any state laws that would prohibit a court order to produce cell site location data from issuing.

  CRL ISSN 0011-1341