Recent decisions restrict law enforcement access to cellphone information: Are more on the way?

By Marcus A. Christian, Esq., and Stephen Lilley, Esq.
Mayer Brown LLP

Law enforcement members routinely use evidence from electronic devices, and particularly from mobile phones, to build corporate or securities fraud investigations and prosecutions. Such phones store volumes of user content and generate even more network metadata, all of which has been easily available to law enforcement in many circumstances. Officers have obtained incriminating evidence by simply searching cellphones incident to arrests. And during investigations, agents have obtained cell site location information[1] and other metadata from service providers without showing probable cause.

However, courts are revisiting individuals' reasonable expectations of privacy in an increasingly digital world. In *Riley v. California*, 134 S. Ct. 2473 (June 25, 2014), for example, the U.S. Supreme Court held that the Fourth Amendment generally bars law enforcement members from searching an arrested person's cellphone without first obtaining a search warrant. And in *United States v. Davis*, 754 F.3d 1205 (11th Cir. June 11, 2014), the 11th U.S. Circuit Court of Appeals held that police also must obtain a warrant for cell site information from wireless phone companies. Law enforcement agencies will feel the effects of these decisions, particularly if they are followed by further decisions that extend Fourth Amendment protections to other digital contexts, which appears possible.

WHITE-COLLAR LAW ENFORCEMENT IN A DIGITAL WORLD

While popular opinion has turned against government data collection in the wake of Edward Snowden's revelations, law enforcement agencies remain committed to using all the tools at their disposal in white-collar and other cases. FBI Director James Comey emphasized this point in recent congressional testimony, mentioning wiretaps as a "vital tool to gain concrete evidence against individuals" conducting sophisticated financial crimes.[2]

Obtaining a court's approval to intercept wire communications is difficult, however. Among other things, law enforcement members must provide facts supporting the finding that the intercepted communications will contain evidence of a crime, describing the individuals allegedly involved in the investigated crimes, and showing that agents have exhausted other viable investigative options.[3] Metadata, including call logs and historical cell site data, frequently provide the building blocks that law enforcement uses to meet those standards.

Marcus A. Christian (L) is a Washington partner in **Mayer Brown LLP**'s litigation and dispute resolution practice and white-collar defense and compliance group, and he is a member of the firm's privacy and security practice. **Stephen Lilley** (R) is a litigation and dispute resolution associate in Mayer Brown's Washington office and a member of the firm's Supreme Court and appellate and privacy and security practices.

Such metadata also can be used at other points in an investigation and prosecution. For example, Matthew Teeple, a former hedge fund analyst, recently pleaded guilty to one count of conspiracy to commit securities fraud.[4] According to the indictment, Teeple received inside tips from David Riley, a former chief information officer at Foundry Networks Inc. Teeple allegedly passed inside information from Riley about Foundry to another individual who used it to make gains and avoid losses totaling $27 million in one year.

> Courts are revisiting individuals' reasonable expectations of privacy in an increasingly digital world.

Riley now faces his own trial on an indictment based on allegations of the timing and duration of calls between Riley and Teeple, as well as their various in-person meetings. It will be interesting to see whether the government uses call logs and historical cell site data to prove the various alleged calls and meetings, and thereby to corroborate its claim that Riley provided Teeple with the relevant information.

The content of electronic communications also remains central to white-collar prosecutions. For example, take Raj Rajaratnam, the founder of the Galleon Group hedge fund. His 11-year prison sentence — the longest ever received for insider trading — depended in no small part upon an instant message.[5] By 2007, an eight-year investigation into Rajaratnam had yielded millions of pages of documents, but no charges.

That changed after Securities and Exchange Commission investigators discovered a cryptic instant message in which former Galleon employee Roomy Khan advised Rajaratnam not to trade in Polycom stock

until Khan could get "guidance." Because the instant message incriminated Khan, who had been convicted of wire fraud in connection with sharing inside information with Rajaratnam in 1998, it provided prosecutors with leverage to convince her to cooperate in the investigation of Rajaratnam. Using evidence from Khan's subsequent recordings of conversations with Rajaratnam, prosecutors obtained authorization to wiretap Rajaratnam's cellphone, which led to wiretaps on others' phones. Ultimately, more than 20 people were convicted.

RILEY V. CALIFORNIA

Law enforcement lost one ready means of gathering the content stored on mobile phones in *Riley v. California*.[6] That case consolidated two appeals.

In the first, David Riley (unrelated to Teeple's co-defendant) appealed an attempted murder and other convictions that stemmed from the search of his smartphone incident to his arrest on gun possession charges. The police found information on his phone that appeared to associate Riley with the Bloods gang and photos of Riley standing in front of a car linked to a shooting with which he ultimately was charged.

In the second case, police officers seized Brima Wurie's two mobile phones incident to a drug arrest and then were able to find a number labeled "My House" and to trace it to a house where they saw a woman who looked like the image on his phone's wallpaper. The police used this information to secure a warrant, which ultimately led to his conviction for various drug crimes.

Both cases presented a common question: Can the police, without a warrant, search digital information on a cellphone seized from an individual who has been arrested? Put another way, these cases asked how the "search incident to arrest" doctrine applies to modern cellphones.

To answer this question, Chief Justice John Roberts, writing for a majority of eight justices,[7] assessed "on the one hand, the degree to which [the search] intrudes upon an individual's privacy and on the other, the degree to which it is needed for the promotion of legitimate government interests." The court identified two legitimate government interests under existing case law: officer safety and the preservation of evidence.

Evaluating the threat posed to officer safety, the court reasoned that after "an officer has secured a phone and eliminated any potential physical threats, ... data on the phone can endanger no one." The "interest in protecting officer safety does not justify dispensing with the warrant requirement across the board," the court concluded.

The court similarly dismissed evidence preservation as a justification for warrantless searches, writing that "once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating evidence from the phone." The court also discounted the likelihood of a command being delivered to the device and erasing its contents in a way that a search incident might have prevented.

> Members of law enforcement routinely use evidence from electronic devices, and particularly from mobile phones, to build corporate or securities fraud investigations and prosecutions.

In contrast, the court found substantial privacy interests at stake. Today's phones, the court observed, have "immense storage capacity," are used extensively in documenting people's lives, store data sufficient to trace a person's movements, and provide access to data stored in other places, such as in the cloud. The court observed that "many of the more than 90 percent of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives — from the mundane to the intimate."

Allowing police to search such vast troves of personal information in 90 percent of cases, the court reasoned, "is quite different from allowing them to search a personal item or two in the occasional case." Because phones also include distinctive data such as search and browsing histories, the court noted, a phone contains "a broad array of private information never found in a home in any form — unless the phone is."

Given the limited government interests and the strong privacy interests, the court reached a "simple" result: The police must "get a warrant" before searching a cellphone seized incident to an arrest. However, proving that nothing in the Fourth Amendment context is ever that simple, the court was careful to note that police still may search a cellphone without a warrant if exigent circumstances require it.

More broadly, the unanimity in judgment also is somewhat surprising in light of the court's sharply divided 5-4 decision in *Maryland v. King*, which permitted swabbing an arrestee's DNA as part of the administrative process incident to arrest.[8] There, the court gave great weight to the government's interest in identifying the suspect and found the intrusion into an arrestee's privacy caused by a cheek swab to be "minimal," partly because the way the specimen was tested prevented discovery of genetic information.

Of course, as the court implicitly acknowledges, a mobile phone also can be used for identification purposes or to solve a cold case. The court did not dwell on that in *Riley*, focusing instead on the strength of the privacy interests triggered by the voluminous and interrelated personal data on mobile phones. In so doing, the court sounded notes similar to the concerns that five justices highlighted in two concurrences in *United States v. Jones*.[9]

The justices relied on a trespass theory in concluding the physical attachment of a GPS tracking device to a suspect's car constituted a search for purposes of the Fourth Amendment. However, five different justices indicated the GPS tracking of a subject could be a search even without a trespass, in large part because new technologies could make extensive surveillance "easy and cheap." Whether the volume and ease of surveillance made possible by new technology will figure prominently in future Supreme Court majority opinions remains to be seen.

UNITED STATES V. DAVIS

The 11th Circuit demonstrated similar concern about the sensitivity of information gathered through electronic means in *Davis*.[10] Defendant Quartavious Davis was indicted on 17 counts related to a series of armed robberies at restaurants and retail stores. At trial, the court admitted into evidence cell site location information that investigators

had obtained from phone providers pursuant to a Section 2703(d) order under the Stored Communications Act for which probable cause was not required.[11] Prosecutors used it to show that Davis was near the site of each robbery around the time they occurred. Davis was convicted on all counts and sentenced to about 162 years of imprisonment.

Addressing an issue of first impression, the 11th Circuit held that Davis' cell site location information was protected by the Fourth Amendment because cellphone users have a reasonable expectation of privacy in that information. The court found the decision in *Jones* "instructive" and discussed the various opinions and rationales in detail. Relying on its privacy rationale, the court found that cell site information gives rise to greater privacy interests than GPS data. Declining to rely on the volume-based rationale in *Jones*, the court reasoned that because a cellphone can accompany individuals into private places, "even one point of cell site data can be within a reasonable expectation of privacy."[12]

The court readily rejected the claim that like an address on an envelope or telephone routing information, individuals have no expectation of privacy in cell site information because they effectively announce their location to third-party telephone providers.[13] The court reasoned that cellphone users "voluntarily and knowingly" convey call only routing information to a telecommunications provider and probably have no idea they are conveying location information to their service provider simply by using their phones. Moreover, the court rejected the argument that the relative imprecision of cell site data makes it less deserving of Fourth Amendment protection, finding that fact not "constitutionally significan[t]."

FURTHER CONSTITUTIONAL RESTRICTIONS ON DIGITAL SURVEILLANCE?

After *Riley*, law enforcement will need to find a substitute for the opportunities that searches of cellphones incident to arrest provided to gain incriminating evidence relating to arrestees or third parties. In addition, any law enforcement aspirations to upload arrestees' cellphone data to a central database and then mine it for connections have been foreclosed. *Davis* also clarified that law enforcement agencies within the 11th Circuit will need to secure a warrant in order to obtain cell site information. The effect likely will be significant: A 2012 study by the American Civil Liberties Union found the "vast majority" of law enforcement agencies surveyed used cellphone location tracking, and that most did so without obtaining warrants.[14]

> The content of electronic communications also remains central to white-collar prosecutions.

Riley and *Davis* also leave open significant questions going forward, many of which put into question the constitutionality of various provisions of the Stored Communications Act and the overarching Electronic Communications Privacy Act. Other courts likely will have to decide whether they agree with the 11th Circuit that a warrant is necessary to obtain historical cell site information.

As the 11th Circuit noted in *Davis*, two other circuit courts already have weighed in, if in a different procedural posture.[15] Both considered the question of whether a court that finds the standard for issuance of a Section 2703(d) order has been satisfied must issue such an order.

In 2011 the 3rd Circuit concluded that the statute only permits the issuance of such an order and leaves magistrates discretion to require probable cause instead.[16] The court rejected the magistrate judge's conclusion that probable cause was required for all historical cell site location information. But the court concluded the statute should be interpreted to allow magistrates discretion to consider whether the information sought would "implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home."

The court found unpersuasive the government's argument that no Fourth Amendment concerns can be triggered since the cell site information at issue was disclosed to a third party, and suggested that Congress clarify the statute's ambiguity.

The 5th Circuit reached a different result last year. It agreed with the 3ird Circuit that the issuance of Section 2703(d) orders for historical cell site information is not per se unconstitutional, but concluded that:

- Such information is a business record.
- Cellphone users realize that they provide information to cellphone towers, making applicable doctrine relating to sharing of information with third parties.
- Magistrates have no discretion to decline to issue a Section 2703(d) order when the appropriate showing has been made.[17]

The Fourth Amendment's underlying requirements also remain uncertain beyond the context of historical cell site information. In *United States v. Warshak*, the 6th Circuit ruled that law enforcement must have a warrant, not just a Section 2703(d) order, to compel a telecommunications provider to disclose the contents of a customer's email.[18] To the extent that the Stored Communications Act provides otherwise, such as through its rule that email more than 180 days old is not protected (commonly referred to as the 180-day rule), it is unconstitutional, the court explained.

The Justice Department appears to have conceded that it must live with that standard,[19] so it may now be the de facto national rule. However, significant questions are raised even under that standard, as demonstrated by ongoing litigation as to whether a warrant secured under the SCA can be used to compel the production of data held abroad (like a subpoena) or whether it is only domestic in its reach (like a traditional Fourth Amendment warrant).[20]

CONCLUSION

One overarching issue going forward will be who decides these questions: Congress or the courts? Various judicial decisions have called for additional clarity from Congress, but whether courts will defer to those judgments remains unclear. For example, the Justice Department has pushed for the Electronic Communications Privacy Act to be amended so that email metadata, including to/from information, can be compelled with a Section 2703(d) order.[21]

But it is unclear whether courts would continue to give weight to distinctions between content and non-content (or metadata) for Fourth Amendment purposes.

In *Jones*, Justice Sonia Sotomayor noted the substantive import of location data to the extent that it demonstrates an individual attends a particular church or visits a particular doctor. This raises the question of whether courts would be willing to accept the extension of the exception for phone logs to email addresses that often disclose details about the user.

It will be interesting to see how courts and Congress navigate related areas of Fourth Amendment doctrine. For example, recent proposals to amend the Electronic Communications Privacy Act would prevent regulatory agencies from using administrative subpoenas to compel service providers to produce email content. Courts, in contrast, have long indicated that regulatory agencies such as the Securities and Exchange Commission hold a general power of inquisition such that compulsion of documents from the regulated entity directly does not implicate the Fourth Amendment.[22]

In the absence of congressional action, it seems possible that courts may permit regulatory agencies to continue to secure email content from providers without a warrant and pass that information on to criminal law enforcement agencies.

The Supreme Court's observation in *Riley v. California* that "privacy comes at a cost" should leave little doubt that if and when the high court takes up these questions, it will examine the privacy interests involved quite searchingly, despite the potential impact on law enforcement activities. In light of the rapid and significant changes surrounding law enforcement's access to digital information in financial crimes investigations, white-collar practitioners and corporate counsel should watch this area of law closely. WJ

NOTES

[1] Cell site location information is created and stored with a service provider whenever a mobile phone user places or receives a call, or transmits data. The user's service provider records both the particular tower that received the signal and the direction of the user from the tower. Using these data, law enforcement can determine a user's approximate location at the time of the transmission.

[2] *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary* (May 21, 2014) (statement of James Comey, Director, FBI).

[3] *See generally* U.S. Attorney Manual, 28 Electronic Surveillance—Title III Applications (October 2012).

[4] *See United States v. Riley,* No. 13-cr-00339 (S.D.N.Y. May 28, 2014).

[5] *See generally* Susan Pullman, *Fund Chief Snared by Traps, Turncoats,* Wall St. J., Dec. 30, 2009; George Packer, *A Dirty Business,* The New Yorker, June 27, 2011 ("Without this I.M., the case would probably have died."). This instant message apparently was obtained through an SEC subpoena of Galleon's email and instant messages. *See United States v. Rajaratnam,* 2010 WL 4867402 (S.D.N.Y. 2010) (discussing SEC subpoenas of Galleon as well as of "banks, clearing houses, telephone companies, and issuers of publicly traded securities"). Although the instant message may not have been originated or been received on a mobile phone, the principle is the same: Access to electronic content can mean the difference between a successful and failed investigation.

[6] *Riley v. California,* 134 S. Ct. 2473 (June 25, 2014).

[7] Justice Samuel Alito concurred in part and in the judgment.

[8] 133 S. Ct. 1958 (2013).

[9] *United States v. Jones,* 132 S. Ct. 945 (2012).

[10] *United States v. Davis,* 754 F.3d 1205 (11th Cir. June 11, 2014).

[11] *See* 18 U.S.C. § 2703(d) (authorizing order requiring telecommunications provider to disclose information sought upon offer of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation").

[12] In contrast, the court indicated only aggregated GPS information would invade an individual's privacy.

[13] *See United States v. Miller,* 425 U.S. 435 (1976) ("the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities").

[14] *See* Am. Civil Liberties Union, ACLU Affiliate Nationwide Cell Phone Tracking Public Records Requests, Findings and Analysis (Mar. 31, 2012), *available at* https://www.aclu.org/files/assets/cell_phone_tracking_documents_-_final.pdf.

[15] State courts also are sure to weigh in on this and related issues. *See, e.g. State v. Subdiaz-Osorio,* No. 2010AP3016-CR, 849 N.W.2d 748 (Wis. July 24, 2014) (assuming that warrantless acquisition of cellphone location data triggered Fourth Amendment protections, but apply exigent circumstances exception to the warrant requirement); *State v. Tate,* No. 2012AP336-CR, 849 N.W.2d 798 (Wis. July 24, 2014) (concluding that order satisfied Fourth Amendment requirements and that acquisition of cellphone location data accordingly was appropriate even assuming Fourth Amendment protections were triggered).

[16] *In re Application of the United States for an Order Directing a Provider of Electronic Communication Services to Disclose Records to the Government,* 620 F.3d 304 (3d Cir. 2014).

[17] *In re Application of the United States for Historical Cell Site Data,* 724 F.3d 600 (5th Cir. 2013).

[18] *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010).

[19] *See Oversight of the U.S. Dep't of Justice: Hearing Before the H. Comm. on the Judiciary* (May 15, 2013) (testimony of Eric Holder, U.S. Attorney General) ("The more general notion of having a warrant to obtain the content of communication from a service provider is something that we support."). *See also ECPA (Part 1): Lawful Access to Stored Content, H. Before the Subcomm. on Crime, Terrorism, Homeland Security and Investigations of the H. Comm. on the Judiciary* 20 (Mar. 19, 2013) (statement of Elana Tyrangiel, Acting Assistant Attorney General (recommending that statutory provision giving lesser protections to emails over 180 days old be eliminated)).

[20] *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.,* No. 13-MJ-2814,2014 WL 1661004 (S.D.N.Y. Apr. 25, 2014).

[21] The Justice Department also has recommended clarifying that a magistrate must issue a Section 2703(d) order if the appropriate showing has been made.

[22] *See generally United States v. Morton Salt,* 338 U.S. 632 (1950).