New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
OCTOBER 13, 2021

WHITE-COLLAR CRIME

Recent Woes for Prosecutors in Cellphone Searches

Three recent district court decisions exemplify how courts have struggled with the Fourth Amendment questions raised by the intrusive nature of cellphone searches.

By **Robert J. Anello**

And **Richard F. Albert**

Following the Supreme Court's lead, district courts throughout the country have scrutinized the scope and circumstances of government searches of cellphones in criminal cases. In several recent decisions interpreting the Supreme Court's decision in *Riley v. California*, which recognizes the heightened privacy interests implicated by searches of modern cellphones, the courts have grappled with thorny issues arising from the immense quantity and variety of data stored on cellphones. The trove of information available on mobile devices has been a double-edged sword for those seeking to suppress government searches. Because cellphones contain so much information, courts have required a clear nexus between the cellphone and the alleged offense to establish probable cause or particularity for a warrant; conversely, the fact that this information—including illegal content—can be stored on the cloud and accessed by users after entering the country has been used by at least one court to justify a warrantless search at the border.

Three recent district court decisions exemplify how courts have struggled with the Fourth Amendment questions raised by the intrusive nature of cellphone searches. Cellphones present Fifth Amendment problems too, as discussed in our June 9, 2021, article, "Hey SIRI, Does the Fifth Amendment Protect My Passcode?" As courts continue to grapple with applying constitutional protections to this ubiquitous form of modern technology, criminal defense attorneys should aggressively scrutinize cellphone searches.

Texas Court Suppresses Search Linking Defendant to Guns, Murder, and Child Pornography

This August, the Southern District of Texas granted a motion to suppress all cellphone evidence found pursuant to a tainted search warrant in *United States v. Opoku*, No. 4:20-CR-381, 2021 WL 3748260 (S.D. Tex. Aug. 23, 2021). Officers at the Houston Police Department arrested Javon Opoku for capital murder on Nov. 3, 2019, three days after the crime. During the arrest police seized the cellphone Opoku was carrying. On Feb. 24, 2020, while out on bond for the murder, Houston Police Department officers again stopped Opoku, this time purportedly for an expired car registration. The stop led to Opoku's arrest for theft of a firearm and carrying a handgun in a motor vehicle. During the arrest, the officers again seized his cellphone.

A few days later, a Houston Police Department officer applied for a warrant to search the 2020 cellphone for evidence related to the murder. The officer's affidavit identified Opoku and two co-defendants as gang members and included the aphorism that "gang members who commit violent crimes are known to use

ROBERT J. ANELLO *and* RICHARD F. ALBERT *are partners at Morvillo Abramowitz Grand Iason & Anello, P.C.* JORJA KNAUER, *an associate at the firm, assisted in the preparation of this article.*

their cell phones" to coordinate these crimes. The affidavit added that the phone likely contains text messages "relating to the planning and commission of the Capital Murder" and GPS data showing Opoku's location when the murder occurred. The affidavit, however, conveniently failed to mention that police seized a different cellphone during Opoku's November 2019 arrest. Based on the affidavit, a judge issued a warrant to search for all evidence found in the 2020 cellphone that related to the alleged capital murder, including all stored text messages, voicemail, all cellphone memory including photographs, any data, video, audio, and cellular files. While searching the 2020 cellphone, the officer stumbled upon video recordings which ultimately led to Opoku's indictment in federal court on one count of sexual exploitation of children in violation of 18 U.S.C. §2251.

The Southern District of Texas granted Opoku's motion to suppress all evidence obtained because of the search warrant, applying a commonsense analytical framework that would appear potentially to apply in many other cases. The court rejected the suggestion that "that anytime a crime implicates codefendants," the government can search cellphone texts or messages about planning or committing that crime. The court reasoned that cellphone searches involve so much private data that a cellphone search warrant must "be based on more than (1) the fact that a codefendant possesses a cellphone and (2) the truism that people often communicate plans via cellphone." Holding otherwise, it held, would "eliminate privacy rights in cellphones" and undermine the Supreme Court's 2014 decision in *Riley v. California*, which requires police to obtain a warrant prior to searching cellphones found on an arrestee during a search pursuant to arrest. The opinion quoted *Riley*, noting that searching a cellphone "would typically expose to the government far *more* than the most exhaustive search of a house," the paradigmatic Fourth Amendment example of an invasive, impermissible search, because modern cellphones amass so much data and so many distinct types of information about the user.

Additionally, the court noted that generalizing that violent gang members use their phones to coordinate with others about planning and committing crimes fails to justify a broad search of all cellphone memory. Even if the information in the affidavit were sufficient to create an inference that Opoku kept photographs or videos related to the crime, "any person suspected of committing any crime … would lose any privacy rights" in potentially thousands of pictures stored on the cellphone, another scenario the Supreme Court contemplated and rejected in *Riley*.

Likening a Cellphone to a Computer Yields Mixed Results. Earlier this summer, the District of Kansas declined to suppress all evidence seized from a cellphone in *United States v. Whitmore*, No. 20-CR-40004, 2021 WL 2604971 (D. Kan. June 24, 2021), after applying the Tenth Circuit's search warrant particularity requirements that apply to both computers and cellphone searches. This standard considers both computer and cellphone search warrants to be sufficiently particular if their scope is limited to either evidence of specific federal crimes or to specific types of material likely stored on the device. Because the warrant limited the search to records related to bank robbery, the crime charged, the court found the warrant sufficiently particular to justify the search for evidence related to bank robbery. The court suppressed evidence of unrelated commercial robberies, however, absent probable cause that the defendant participated in any other crimes.

During a bank robbery, bank employees witnessed the lone gunman speaking with someone on his cellphone. A few days after the robbery, and after recognizing his son in images of the robber that law enforcement posted on social media, Shawn Lamar Whitmore Jr.'s father told police he suspected his son committed the robbery and provided additional information and evidence. Law enforcement obtained an arrest warrant and then several months after the arrest applied for a warrant to search Whitmore's cellphone for evidence related to the bank robbery and unrelated commercial robberies.

The affidavit submitted with the search warrant application described how the gunman used

his phone during the robbery to talk with someone outside the bank and how law enforcement connected this phone to the defendant. The affidavit omitted any facts or circumstances related to other commercial robberies. Nor did the affidavit justify the request to include evidence of other robberies.

The District of Kansas granted Whitmore's motion to exclude evidence obtained from a search of his cellphone related to other, unspecified commercial robberies because the affidavit only described the investigation that led officers to believe the defendant committed one specific bank robbery. The affidavit failed to provide information about Whitmore's suspected participation in other crimes, depriving the search of probable cause and rendering the warrant overbroad. The court declined to suppress cellphone evidence related to the bank robbery at issue, however. Considering Whitmore's cellphone, consistent with the Supreme Court's description of a cellphone in *Riley*, to be a "powerful computer[] that also happen[s] to facilitate telephone calls," the court applied the same particularity standard the Tenth Circuit uses for computer search warrants. Applying that standard, the court approved the search for evidence related to the bank robbery because the warrant restricted the search to records related to violations of 18 U.S.C. §2113, the crime charged.

Contraband on the Cloud: Giving the Government a Free Pass for Warrantless Border Searches. Whereas the prior two cases show cellphones' unique storage capabilities working in the defendants' favor, this same feature of modern cellphones helped persuade the Northern District of Illinois to permit warrantless border searches of cellphones in *United States v. Mendez*, No. 16-CR-00163-1, 21 WL 3187718 (N.D. Ill. July 28, 2021). After arriving alone in Chicago from Ecuador via Panama City, Panama, Marcos Mendez underwent routine questioning by U.S. Customs and Border Protection Officers. The officers found child pornography while manually searching Mendez's personal cellphone.

Mendez moved to suppress, arguing that warrantless cellphone searches at the border "allow the government to arbitrarily invade the expectation of privacy in millions of pages of unrelated personal information in the process," a result forbidden by the Supreme Court's ruling in *Riley*. The Northern District of Illinois disagreed. The court reasoned that though *Riley* emphasized "the uniqueness of cell phones and the nature of the data they store," that opinion only addressed searches incident to arrest and did not address border searches, where the government's interest in preventing the entry of contraband "are at their zenith" and thus the Fourth Amendment's balance between individual privacy rights and the government's interest leans toward the government. The court relied on a prior Seventh Circuit decision, *United States v. Wanjiku*, 919 F.3d 472 (7th Cir. 2019), which observed that no circuit court, before or after *Riley*, had required more than reasonable suspicion for a border search of cell phones or electronically stored data. Significantly, the court reasoned, the fact that a cellphone seized at the border may hold child pornography on remote servers that may "continue to remain accessible inside the border" increases the government's interest in preventing this material from being imported. Accordingly, the court denied Mendez's suppression motion.

Conclusion

The Supreme Court's decision in *Riley* continues to shape lower court rulings on motions to suppress cellphone searches, with mixed results for criminal defendants. As courts continue to struggle to apply Fourth Amendment principles to this critical technology, criminal defense attorneys should push courts to scrutinize cellphone searches.