

**Fifth Circuit Court of Appeal
State of Louisiana**

No. 26-K-162

STATE OF LOUISIANA

versus

MICHAEL PAMPAS

IN RE MICHAEL PAMPAS
APPLYING FOR SUPERVISORY WRIT FROM THE TWENTY-FOURTH JUDICIAL DISTRICT
COURT, PARISH OF JEFFERSON, STATE OF LOUISIANA, DIRECTED TO THE HONORABLE
NANCY A. MILLER, DIVISION "I", No. 25-3632

TRUE COPY

May 04, 2026



LINDA TRAN
DEPUTY CLERK

Panel composed of Judges Susan M. Chehardy,
Fredericka Homberg Wicker, and Marc E. Johnson

WRIT DENIED

Relator, Michael Pampas, seeks this Court's supervisory review of the district court's March 9, 2026 ruling denying his motion to suppress evidence—specifically, cloud-based digital storage accessible by the device—obtained pursuant to a search warrant. For the following reasons, finding no abuse of the district court's discretion and no basis upon which to disturb its ruling, this writ application is denied.

FACTUAL BACKGROUND AND PROCEDURAL HISTORY

On November 20, 2025, Mr. Pampas was charged with first-degree rape upon a known juvenile under the age of thirteen, a violation of La. R.S. 14:42(A)(4); indecent behavior with a juvenile under the age of thirteen, a

violation of La. R.S. 14:81; and, production of pornography involving juveniles under the age of thirteen, a violation of La. R.S. 14:81.1(E)(5)(b). On November 21, 2025, Mr. Pampas entered pleas of not guilty.

During the course of law enforcement's investigation of the alleged crimes, in October 2024, a Cellebrite extraction of Mr. Pampas' cell phone was performed pursuant to a search warrant, which specifically sought to search data stored on remote cloud servers. After Mr. Pampas' cell phone was "extracted" pursuant to the October 2024 search warrant, Detective Emile Sanchez, detective for Criminal Investigations Division, received a tip regarding where he could retrieve additional probative evidence on Mr. Pampas' cell phone.¹ Based on this new information, Detective Sanchez requested a secondary search of Mr. Pampas' device for purposes of locating the images and/or video[s] referred to by the tipster in order to further aid in the prosecution. Specifically, Detective Sanchez requested authority to conduct a secondary "physical" search of Mr. Pampas' phone for, among other information, any and all "cloud based storage accessible by the device" as follows:

Affiant requests the issuance of a search warrant and to seize and examine electronic data including, but not limited to:

Phone Electronic data and Media – *Any* voice messages, text message, phone numbers, *pictures*, GPS, and other *electronic data and or media contained* within the hardware, the device SIM card or *within cloud based storage accessible by the device*, or cellular operating system of the cellular phone/electronic device that identifies the owner and or possessor of the cellular phone.

App Electronic Data and Media–*Any* and all messages, text messages, phone numbers, *pictures*, GPS, and other electronic data and or media contained

¹ At the suppression hearing, Detective Sanchez testified that after the Cellebrite extraction of Mr. Pampas' cell phone was conducted pursuant to the initial search warrant, he reviewed all of the information extracted at that time to the best of his ability. He explained that Cellebrite extractions are not always comprehensive depending upon the software and available data, and that it was normal for not every piece of information to be extracted from a phone.

within the hardware, software, and or microprocessors of the cellular phone/electronic device related to the below listed crimes.

Internal Storage Electronic Data and Media—Any photographs, text messages, phone logs, or GPS information located within the internal memory of the cellular phone/electronic device relator to the below listed crimes.

Hidden, Erased or Encrypted Electronic Data and Media—Any and all hidden, erased, compressed, password protected, and/or encrypted files as they relator to the below listed crimes. [Emphasis supplied.]

The affidavit further explained that Mr. Pampas' cell phone was believed to contain evidence of the crime of indecent behavior with a juvenile under thirteen. After setting forth the grounds for probable cause, which Mr. Pampas does not appear to contest, the second search warrant, prepared by Detective Sanchez, provided the following:

On July 28, 2025, [he] was contacted by Pampas' girlfriend, who advised she had logged into Pampas' Google account and located images of Pampas and the juvenile involved in either sexual acts or with the juvenile in the nude, with specific dates and folders listed for where the images are contained.

Finding sufficient probable cause under the circumstances presented to support the issuance of a second search warrant, the warrant was issued by Commisioner Paul Schneider of the Twenty-Fourth Judicial District Court authorizing the search of Mr. Pampas' cell phone and permitting the seizure and examination of the items identified in the affidavit tending to prove the offense.

Relying on the validity of the warrant, on July 28, 2025, Detective Sanchez executed the warrant and a second search of Mr. Pampas' cell phone was conducted, which included a search of his password protected Google drive that

was accessible via the phone.² The return indicates that three files were seized from the phone³ and that the images/video[s] described to Detective Sanchez by Mr. Pampas' girlfriend were located in the folders contained on Mr. Pampas' Google drive, exactly as the informant described.⁴ It detailed that all three files were located within "the 'locked' folder of the Suspect's Google Photos application." According to Detective Sanchez, "the Google drive [on Mr. Pampas' cell phone] was already signed in," such that the username and password used to access the images/video[s] were the same as those used to get into the device during the initial search of the phone. It is unclear whether Detective Sanchez was aware, at the time of the second search of Mr. Pampas' phone, that the data at issue was stored remotely on a third-party server.

Mr. Pampas filed a motion to suppress the evidence, arguing the inclusion of such "cloud-based" data makes the warrant unconstitutionally broad under the

² The initial search warrant obtained for Mr. Pampas' cell phone was obtained pursuant to an affidavit submitted on October 2, 2024; the second search warrant was obtained on July 28, 2025, both of which were based on the same probable cause affidavit, with the second affidavit containing "new information added." Specifically, the second search warrant included an additional paragraph specifically listing where Detective Sanchez was told the potential video evidence could be found and, in fact, although another extraction of the phone was not actually conducted, "additional videos were found that were not on the original extraction." Detective Sanchez testified as to the chain of custody for Mr. Pampas' cell phone from 2024 to 2025, and stated that the cell phone remained in the custody of the Kenner Police Department the entire time. He explained that the chain of custody was tracked digitally through "PSTrax" and that the phone was logged as evidence. According to the State, the chain-of-custody records at issue are maintained by the Kenner Police Department Evidence Room.

³ Specifically, the following items were seized:

- 1) File name: "20240915_040503.mp4," a 15 minute video depicting sexual intercourse between 29 year old suspect and 12 year old victim.
- 2) File name: "Screen_recording_20240808_012158_Snappchat.mp4," a video in which the suspect is masturbating while on video chat with the victim, who is showing her buttocks and vagina.
- 3) File name: "Screen_recording_20240812_025400_Messenger.mp4," a video in which the suspect is nude in the shower while on a video chat call with the victim, who is showing her bare breasts[.]

⁴ The images/video(s) obtained in 2025 pursuant to the second search warrant were not located during the original extraction conducted in 2024. Detective Sanchez explained his belief that this was because the data was "behind a locked folder" and could not be extracted by Cellebrite, even though the 2024 search warrant affidavit requested "any hidden, erased, script electronic data or media," including "any and all hidden" data. He further explained that the information he received from the tipster in 2025 was very specific as to where the potential videos could be accessed on Mr. Pampas' cell phone through the Google phone folder using the same passcode used to access the phone, generally, including for extraction.

protections afforded to him by the Fourth Amendment to the United States Constitution, which provides protection against unreasonable searches and seizures. Mr. Pampas' motion to suppress came for hearing on February 26, 2026, and March 4, 2026. At the hearing, counsel for Mr. Pampas acknowledged that data on a seized device may be extracted pursuant to a warrant but argued that this applies only to data stored on the device itself, and that Detective Sanchez exceeded the scope of the warrant by accessing cloud-based data stored outside the phone. In particular, he argued that Detective Sanchez accessed Google drive data through the phone rather than obtaining a separate warrant directed to Google.

In response, the State argued that no challenge was made to the validity of the warrant, none of the recognized grounds for challenging a warrant were present, and that the warrant was supported by probable cause and should not be suppressed. The State further argued the warrant authorized a broad search of the phone, including electronic data, media, and cloud-based storage accessible through the device. It pointed to the warrant's language authorizing the search of voice messages, text messages, phone numbers, pictures, and other electronic media "contained within the hardware of the device . . . or within cloud-based storage accessible by the device" and maintained that this language encompassed both the phone itself and any cloud-based data accessible through it.

At the close of the hearings, the district court took the matter under advisement. Thereafter, finding the search warrant indisputably contained language allowing the search of cloud-based data, finding no caselaw or authority to support Mr. Pampas' argument that the inclusion of such cloud-based data was unconstitutional, and finding the evidence would have been obtained through another warrant based on the same probable cause and, thus, the inevitable discovery rule applied, the district court issued a ruling on March 9, 2026, with written reasons, denying Mr. Pampas' motion to suppress the evidence.

The instant writ application filed by Mr. Pampas followed.

ISSUE PRESENTED

At issue is whether a search warrant authorizing the search of a defendant's physical cellular device—which warrant is indisputably based on probable cause—seeking “cloud-based storage *accessible* by the device” is sufficient to authorize law enforcement's search of a third-party server or cloud storage account, namely Google drive, where the data may not be physically stored on the phone itself, but is merely accessible through it.

Mr. Pampas maintains that he retained a reasonable expectation of privacy in his Google drive data, notwithstanding its storage with a third-party provider, and that law enforcement was required to obtain a warrant specifically authorizing access to that account. Specifically, Mr. Pampas argues his Google drive account was “accessible from any internet-connected device in the world using [his] credentials” such that his cell phone “was not the repository of the evidence” but was “merely the key,” and that, if detectives wanted to search his Google Drive account, they should have obtained a search warrant directed to Google. In particular, Mr. Pampas avers that although data information contained in or on the phone itself may be recovered or extracted pursuant to a valid search warrant in accordance with La. C.Cr.P. art. 163(E)(2), the images/video[s] at issue were not contained *on the physical phone*. He contends the warrant's “cloud-based” language fails to satisfy the particularity requirement and cannot authorize access to all third-party servers. Therefore, accessing the images/video[s] via his Google drive account constituted a violation of his constitutional rights afforded by the Fourth Amendment. Further, Mr. Pampas argues that Detective Sanchez was overly broad in his search and seizure of Mr. Pampas' Google customer data storage contained in the iCloud, outside of gmail photos, texts, and anything else actually contained on the physical phone. Mr. Pampas avers that Google stores

information in its Google drive, which is in the Google cloud and requires a separate warrant. For these reasons, Mr. Pampas argues the search warrant does not fall within La. C.Cr.P. art. 163; the search of the Google drive and/or the iCloud account specifically required a separate search warrant directed to Google, which was not obtained, mandating that the evidence at issue be suppressed. We disagree.

DISCUSSION

The Fourth Amendment of the United States Constitution and Article 1, § 5 of the Louisiana Constitution protect individuals against unreasonable searches and seizures. *State v. Williams*, 20-46 (La. App. 5 Cir. 12/30/20), 308 So.3d 791, 825, writ denied, 21-316 (La. 5/25/21), 316 So.3d 2. When evidence is seized pursuant to a search warrant, the defendant bears the burden of proof at a hearing on his motion to suppress that evidence. La. C.Cr.P. art. 703(D); *State v. Green*, 02-1022 (La. 12/4/02), 831 So.2d 962, 969. A district court is afforded great discretion in ruling on a motion to suppress, and its ruling will not be disturbed absent an abuse of discretion. *State v. Lowry*, 23-392 (La. App. 5 Cir. 5/15/24), 389 So.3d 261, 269.

Here, the State does not contest that Mr. Pampas had a privacy interest in the content of his cell phone, including the information accessible therefrom in his Google drive. It concedes that, regarding searches of data obtained from cell phones, “officers must generally secure a warrant before conducting such a search.” *Riley v. California*, 573 U.S. 373, 386 (2014). In short, when a police officer seeks to search a cell phone, he must simply “get a warrant.” *Id.* At 403. Probable cause for the issuance of a search warrant exists when the facts and circumstances within an affiant’s knowledge and of which he has reasonably trustworthy information are sufficient to support a reasonable belief that a crime has been committed and that contraband or evidence of a crime will be found at the

place to be searched. *State v. Brown*, 18-1999 (La. 9/30/21), 330 So.3d 199, 252.

Mr. Pampas does not appear to challenge the existence of probable cause for the July 28, 2025 search warrant, but rather contends that the warrant for his phone did not authorize a search of data stored on a third-party server, even though the warrant included language referencing cloud-based storage.

There is no question that in the instant case, prior to conducting a search of Mr. Pampas' phone and conducting an extraction of its content, Detective Sanchez procured a search warrant based on probable cause. Then, when he was informed of the location of additional evidence that was missed in the initial search, he procured a second search warrant seeking to search for specific additional data accessible by the phone. Notably, a second extraction of the phone was not conducted, and the same username and password used in the original search and extraction of the phone were used to access data during the second search. In other words, at the time of search, the Google account on Mr. Pampas' phone was already signed in.

Clearly, Detective Sanchez complied with *Riley*'s mandate and "[got] a warrant," indisputably based on probable cause, which specifically authorized the search of "cloud based storage accessible by the phone." Further, the second warrant, also supported by probable cause, contained a detailed account as to how Detective Sanchez became aware of the specific location of the video evidence ultimately seized. The second search warrant likewise authorized the search of "cloud based storage accessible" by Mr. Pampas' cell phone, which included the search of Mr. Pampas' Google drive account. In short, the warrant authorized the search of data accessible through the device, including cloud-based storage, and as Detective Sanchez testified, the data at issue was accessed through the phone itself.

For the foregoing reasons, we find that no privacy interest of Mr. Pampas was violated. Detective Sanchez did exactly what the United States Supreme

Court in *Riley* required him to do—he got a warrant based on probable cause. Moreover, we find Mr. Pampas failed to establish that the search of his phone exceeded the scope of the warrant. Accordingly, we find Mr. Pampas failed to meet his burden of proof at the suppression hearing and, thus, the district court did not abuse its discretion in denying Mr. Pampas’ motion to suppress. This writ application is denied.

Gretna, Louisiana, this 4th day of May, 2026.

SMC
FHW
MEJ

SUSAN M. CHEHARDY
CHIEF JUDGE

FREDERICKA H. WICKER
JUDE G. GRAVOIS
MARC E. JOHNSON
STEPHEN J. WINDHORST
JOHN J. MOLAISON, JR.
SCOTT U. SCHLEGEL
TIMOTHY S. MARCEL

JUDGES



FIFTH CIRCUIT
101 DERBIGNY STREET (70053)
POST OFFICE BOX 489
GRETNA, LOUISIANA 70054
www.fifthcircuit.org

CURTIS B. PURSELL
CLERK OF COURT

SUSAN S. BUCHHOLZ
CHIEF DEPUTY CLERK

LINDA M. TRAN
FIRST DEPUTY CLERK

MELISSA C. LEDET
DIRECTOR OF CENTRAL STAFF

(504) 376-1400
(504) 376-1498 FAX

NOTICE OF DISPOSITION CERTIFICATE OF DELIVERY

I CERTIFY THAT A COPY OF THE DISPOSITION IN THE FOREGOING MATTER HAS BEEN TRANSMITTED IN ACCORDANCE WITH **UNIFORM RULES - COURT OF APPEAL, RULE 4-6** THIS DAY **05/04/2026** TO THE TRIAL JUDGE, THE TRIAL COURT CLERK OF COURT, AND AT LEAST ONE OF THE COUNSEL OF RECORD FOR EACH PARTY, AND TO EACH PARTY NOT REPRESENTED BY COUNSEL, AS LISTED BELOW:

CURTIS B. PURSELL
CLERK OF COURT

26-K-162

E-NOTIFIED

24th Judicial District Court (Clerk)
Honorable Nancy A. Miller (DISTRICT JUDGE)
Justin C. Harrell (Relator)
Thomas J. Butler (Respondent)
Mark D. Plaisance (Relator)

Honorable Paul D. Connick, Jr. (Respondent)
Darren A. Allemand (Respondent)
Frazilia Wiggins (Relator)

MAILED

Remy V. Starns (Relator)
Attorney at Law
301 Main Street
Suite 700
Baton Rouge, LA 70825