UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

United States of America,

Plaintiff,

v.

Johnnie Lamar Haynes,

Defendant.

Case No. 19-cr-250 (WMW/ECW)

REPORT AND RECOMMENDATION

On September 26, 2019, Defendant Johnnie Lamar Haynes ("Haynes" or "Defendant") was indicted on two counts of Felon in Possession of a Firearm in violation of 18 U.S.C. §§ 922(g)(1) and 924(a)(2). (Dkt. 1.) This matter is before the Court on Defendant's Motion to Suppress Search and Seizure (Dkt. 35) ("Motion") and Defendant's Supplemental Motion to Suppress Search and Seizure (Dkt. 59) ("Supplemental Motion"). The Court held a hearing on February 3, 2020, at which the Government presented two witnesses and offered eight exhibits. Thomas Calhoun-Lopez, Assistant U.S. Attorney, appeared on behalf of the United States of America and George Dunn appeared on behalf of Defendant Johnnie Lamar Haynes, who was present at the hearing. This case has been referred to the undersigned United States Magistrate Judge for a report and recommendation pursuant to 28 U.S.C. § 636 and Local Rule 72.1.

For the reasons stated below, the Court recommends that Defendant's Motion to Suppress Search and Seizure (Dkt. 35) and Supplemental Motion to Suppress Search and Seizure (Dkt. 59) be denied.

I. FACTUAL BACKGROUND

A. TFO Lepinski's Investigation and Arrest of Haynes

At the February 3, 2020 hearing, Sergeant Adam Lepinski of the Minneapolis Police Department ("MPD"), who is assigned as a Task Force Officer ("TFO") to the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), testified about his investigation of a shooting that occurred at a gas station in North Minneapolis, Minnesota on August 5, 2019. (Tr. at 12-14.)[1] According to TFO Lepinski, an occupied vehicle was shot at, but the occupants never came forward to the authorities about the incident. (*Id.* at 14.) TFO Lepinski testified that Haynes was a suspect in the shooting. (*Id.*) TFO Lepinski issued a probable cause pickup for Haynes. (*Id.* at 15.) He also sought Haynes' arrest pursuant to an active Department of Corrections warrant in connection with a parole violation. (*Id.*)

TFO Lepinski testified that on August 17, 2019, he was working an off-duty job at a parking lot in the 500 block between Hennepin and 1st Avenue North in the bar district of downtown Minneapolis. (*Id.* at 16.) On the same night, TFO Lepinski saw Haynes on 5th Street between Hennepin and 1st Avenue North. (*Id.* at 16-17.) Haynes was walking down the sidewalk and TFO Lepinski was walking in the opposite direction. (*Id.* at 17.) TFO Lepinski, who was in a full MPD uniform, stopped Haynes and placed him in handcuffs. (*Id.*) TFO Lepinski patted down Haynes and did not feel any handguns or any other obvious weapons. (*Id.* at 17-18.) However, TFO Lepinski felt what he

[1] A copy of the hearing transcript ("Tr.") can be found at Docket Entry 79.

believed to be a cell phone in Haynes's pocket. (*Id.* at 18.) TFO Lepinski left the cell phone in Haynes's pocket and walked him to the First Precinct, located one block from the parking lot. (*Id.*)

Next, TFO Lepinski conducted a full search incident to arrest and removed Haynes's cell phone, an Apple iPhone, white in color with pinkish colored case and a cracked screen protector, from his pocket. (*Id.* at 18, 20.) TFO Lepinski believed that the phone was the same cell phone as one recorded in surveillance video of the shooting, although he was not certain. (*Id.* at 31-32; Gov't Ex. 4 at 1-3 ("August 2019 Affidavit").) TFO Lepinski testified that the cell phone was locked when he took the phone out of Haynes's pocket. (Tr. at 19.) Haynes was placed in a holding cell and TFO Lepinski took possession of the cell phone. (*Id.* at 18-19.)

B. Unlocking and Search of Haynes's Cell Phone

TFO Lepinski's body camera captured some of his interactions with Haynes. (*Id.* at 22; Gov't Exs. 1-3.) While Haynes was initially in the holding cell, TFO Lepinski believed that Haynes was not telling the truth about his name. (Tr. at 19-20; Gov't Ex. 1 ("Bodycam Footage No. 1") at 0:42-1:42.) Haynes eventually told TFO Lepinski that he was in fact Johnnie Haynes. (*Id.*)

While in the holding cell, Haynes asked TFO Lepinski for several phone numbers from his cell phone when he learned he would be spending the night in jail. (Tr. at 18; Gov't Ex. 1 at 2:33-2:35.) TFO Lepinski responded "If you want me to write some numbers down, I can do that out of your phone." (Gov't Ex. 1 at 2:35-2:39.) Haynes' cell phone was locked at this point. (Tr. at 20.) TFO Lepinski provided the cell phone to

Haynes, who then unlocked it with his thumbprint. (Tr. at 19; Gov't Ex. 1 at 2:40-2:51.) Haynes then asked if he could call his wife, and TFO Lepinski replied "Let me write down a couple of numbers for you, OK?" and "I don't want you making any calls right now, but you can write down some numbers, if you want, or I'll write them down." (Gov't Ex. 1 at 3:00-3:13.) TFO Lepinski handed the phone to Haynes, who held the phone and read several phone numbers out loud while TFO Lepinski wrote them down on a piece of paper. (Tr. at 19; Gov't Ex. 1 at 3:14-4:26.) While reading numbers with the phone in his hand, Haynes said "This the last number right here, man. And then I'm going to turn my phone off." (Gov't Ex. 1 at 4:26-4:34.) Haynes then asked to speak to someone at the front desk, and after TFO Lepinski said Haynes could not but that he was "being real cool in giving [Haynes] all the numbers," Haynes gave TFO Lepinski the final number and handed the phone back to him, who took it, gave Haynes the paper with the numbers, closed the holding cell door, and went to his computer. (*Id.* at 4:44-5:33.) Bodycam Footage No. 1 shows the screen was dark when TFO Lepinski received the phone from Haynes and that, when TFO Lepinski touched the screen after closing the holding cell door, the screen lit up displaying icons, i.e., that the phone was in an unlocked state. (*Id.* at 5:30-5:31.) Lepinski testified that while Haynes was in the holding cell, Haynes asked TFO Lepinski about locking his cell phone as TFO Lepinski was leaving the holding cell. (*Id.* at 29.)

TFO Lepinski testified that after the initial interaction with Haynes, he went to a computer down the hallway and filled out some paperwork. (*Id.* at 23.) After "a matter of minutes," TFO Lepinski changed the settings on the cell phone, which was still

unlocked. (*Id.*) TFO Lepinski disabled the automatic-lock feature by changing the settings to a setting called "never lock" to prevent the screen from going to sleep or locking. (*Id.* at 20.) TFO Lepinski believed this was the first instance where he had changed the settings on a cell phone. (*Id.* at 33.) TFO Lepinski testified that he changed the settings because he did not have the passcode for the phone and believed that he would be able to get into the phone easier to get the data off the phone if it remained unlocked. (*Id.* at 21, 30.) According to TFO Lepinski, the cell phone must go through a certain process to extract data from it. (*Id.* at 32.) This process is easier for unlocked phones. (*Id.* at 33.) However, he also testified that the same information can be retrieved without the passcode, it just takes longer. (*Id.*) TFO further testified that he did not know on August 17, 2019, when interacting with Haynes, that the lab could open phones without a passcode, and that he only learned this information when preparing for the February 3 hearing. (*Id.* at 51; *see also id.* at 39 (later learned crime lab could open phones without a passcode).)

TFO Lepinski later testified that he did not remember the exact steps he took to change the settings to prevent the phone from locking. (*Id.* at 34.) TFO Lepinski agreed that there were at least "five different things" he had to do to successfully change the settings. (*Id.* at 35.) TFO Lepinski also testified that he did not have access to a Faraday box, which prevents the phone from having cellular communication or connection to a network. (*Id.* at 35-36.) Consequently, TFO Lepinski set the phone to "airplane" mode to prevent the phone from getting wiped remotely by the user or another party. (*Id.* at 37-39.)

TFO Lepinski testified that he intended to obtain a search warrant for Haynes's cell phone. (*Id.* at 21.) Other than looking through the cell phone's contact list with Haynes, TFO Lepinski testified that he did not view or access the phone's content when he changed the settings. (*Id.*) Specifically, TFO Lepinski testified that he did not look at any photographs, videos, texts, or any contacts other than the ones he had shared with Haynes at his request, or anything else substantive on the cell phone. (*Id.* at 21-22.)

TFO Lepinski testified that even though the cell phone was unlocked, he was still interested in obtaining the cell phone's passcode in case it locked. (*Id.* at 24.) TFO Lepinski agreed that Haynes considered the information on his cell phone to be his private information. (*Id.* at 30.) TFO Lepinski testified that it is his general practice to ask for the passcode. (*Id.*) When Haynes was being transported from the holding cell to the squad car, he asked for an additional phone number. (Gov't Ex. 2 at 1:10-1:18.) TFO Lepinski asked Haynes for the passcode "so I can get back into your phone," and Haynes indicated he would use his thumb to open the phone again because his phone did not have a passcode. (*Id.* at 1:23-1:34.) As Haynes was being placed in the squad car, he asked about his phone and TFO Lepinski told him "it's still sitting open, it hasn't locked yet." (*Id.* at 3:37-3:43.) TFO Lepinski told Haynes that if he was willing to give TFO Lepinski the passcode, it would help him get his phone back faster. (Gov't Ex. 2 at 3:48-3:58.) As Haynes was being placed in the car, he asked, "is my phone still unlocked" and TFO Lepinski responded, "I think so." (*Id.* at 5:39-5:41.) TFO Lepinski testified that at this juncture, he was still thinking about the warrant he was going to obtain for the cell phone. (Tr. at 24-25.)

At Haynes's request, TFO Lepinski went back inside the precinct and retrieved another phone number from Haynes's cell phone. (*Id.* at 25.) After writing down the phone number on a piece of paper, TFO Lepinski placed the cell phone in a manila envelope, held the envelope flat to prevent the phone from locking, and returned to the squad car. (Tr. at 25-26; Gov't Ex. 3 ("Bodycam Footage No. 3") at 0:00-0:38.) TFO Lepinski handed the piece of paper to the officer in the squad car and notified Haynes of that action. (Gov't Ex. 3 at 0:37-0:40.) At that time, Haynes asked TFO Lepinski "Did you lock my phone back up? Is it locked up?" (*Id.* at 0:45-0:49.) TFO Lepinski, carrying the phone in the manila envelope, said the phone was "right here" and would be property inventoried. (*Id.* at 0:47-0:50.) Haynes responded, "But did you lock it up" and TFO Lepinski responded, "Yes, it is," to which Haynes continued, "or did you go in it?" (*Id.* at 0:50-0:52.) TFO Lepinski replied, "I got the number out of it. You asked me to, right?" and Haynes responded, "Oh, OK. Yeah." (*Id.* at 0:52-0:57.) TFO Lepinski testified that the cell phone was actually unlocked when he told Haynes that it was locked. (Tr. at 28.)

Next, TFO Lepinski had two uniformed officers transport Haynes to the jail before returning to his job at the parking lot. (Tr. at 42.) At some point during or after his shift at the parking lot, TFO Lepinski brought the phone to the violent crimes office in downtown Minneapolis and plugged it in a docking station for phones awaiting search warrants. (*Id.* at 43-44.) The phone sat unattended until TFO Lepinski returned to work on Monday evening. (*Id.* at 44.)

TFO Lepinski submitted an Application for Search Warrant on August 19, 2019. (Gov't Ex. 4.) TFO Lepinski's August 2019 Affidavit alleged the following relevant facts in support of the Application:

- On 08/05/2019, Minneapolis Police responded to a ShotSpotter activation at Lowry AV N and Logan AV N. Upon arrival, they located multiple discharged cartridge casings and a handgun magazine. The victim(s) and suspect(s) were gone when officers arrived.

- Surveillance video was obtained from two sources that show what transpired before and after the shooting. The suspect in the video is shown at the gas station and shown purchasing a Western Union using a fake name of "JOHN HART". The suspect is then observed on video surveillance taking a photograph of the Western Union receipt with his cell phone, which is an Apple iPhone in a pinkish colored case and believed to be the exact same phone listed on this warrant. After taking the photograph of the receipt, the suspect then goes outside the gas station, appears to obtain a handgun from another individual and shoots at least 13 times at a blue Pontiac G6. Two bullets travel into a nearby business that is occupied by multiple employees. No victims from the Pontiac came forward to police and it is believed that no occupants were struck, although the vehicle was occupied by at least three individuals. The individual who the shooter gets the gun from appears to come to the gas station in a hurry and likely was called by the suspect to bring the gun to his location.

- After shooting, the suspect fled the area and the handgun magazine was recovered by police in the path of his flight.

- Prior to the shooting, the surveillance video shows the suspect exiting the front passenger seat of a grey colored Dodge Challenger, MN license WYXXX. The vehicle is in the gas station lot. A black female, later identified as A.H., is the driver of this vehicle in the video.

- TFO Lepinski spoke with a confidential reliable informant ("CRI") about the case and showed a still photo of the suspect from the surveillance video to the CRI. The CRI identified the suspect as "Bad Ass". Minneapolis Police database shows the moniker of "Bad

Ass" as belonging to Johnnie Lamar Haynes, date of birth 03/24/1989. Haynes is a multi-convicted felon and thus a person prohibited from possessing a firearm.

- TFO Lepinski compared the surveillance video of the shooter to HAYNES and they appear to be the same person.

- On 08/09/2019, Minneapolis Police patrol officers located the Dodge Challenger and conducted a traffic stop on the vehicle. TFO Lepinski had previously placed an Attempt to Locate on this vehicle to the online MPD Daily Intelligence Board. When officers stopped the vehicle, the registered owner, A.H., was the driver and sole occupant of the vehicle. TFO Lepinski requested that the vehicle be towed. A.H. said she was willing to provide a statement about the shots fired incident. TFO Lepinski conducted an audio/video recorded interview with A.H. During that interview, she said she was at the gas station with "Johnnie" and identified HAYNES in a video surveillance still shot. A.H. provided TFO Lepinski her phone number as 773-368-XXXX and showed TFO Lepinski her phone call log from 8/5/19. TFO Lepinski observed the phone number of 320-455-XXXX listed multiple times on her call log on 8/5/19. A query was done on this number, which showed the subscriber as "JOHN HART", which is the same name that was listed on the Western Union receipt. "John Hart" appears to be an alias used by HAYNES.

- TFO Lepinski drafted a search warrant for "Call detail records" with historical cell tower data for numbers for HAYNES and A.H. The records showed both HAYNES and A.H. at the scene of the shooting. Furthermore, the records for HAYNES showed that he had contact with two numbers right before the shooting, one of which is presumably the person who brought him the handgun. Through various investigative techniques, TFO Lepinski believed the person who brought the handgun to HAYNES is Cortez L. SHIPP, a known associate of HAYNES. By viewing HAYNES' phone contact list, TFO Lepinski stated that he would be able to compare the numbers from the call detail records to the contacts listed in his phone.

- On 8/17/2019, at approximately 0130 hrs, TFO Lepinski was working off-duty in downtown Minneapolis, when he observed HAYNES walking down 5th Street North by 1st Avenue North. TFO Lepinski approached and arrested HAYNES for PC

> Assault/Felon in possession of a weapon related to this case, along with an outstanding warrant from DOC. When TFO Lepinski searched Haynes incident to arrest, the listed Apple iPhone, was located in HAYNES' pants pocket. The phone was taken into evidence and HAYNES was booked into jail, where he remains.
>
> - Furthermore, TFO Lepinski believes the listed phone will contain contact information for the person who HAYNES called (Cortez Shipp) to bring the gun to the scene.

(Gov't Ex. 4 at 1-3.) TFO Lepinski believed Haynes' phone would contain the photograph he took of the Western Union receipt, which he thought would confirm whether he was the shooter in the case. (*Id.* at 3.) TFO Lepinski also believed that Haynes's cell phone would contain contact information for the individual that allegedly brought the gun to Haynes. (*Id.*)

On August 20, 2019, TFO Lepinski obtained the search warrant for Haynes's cell phone. (Tr. at 26-27; Gov't Ex. 4.) TFO Lepinski testified that he did not include anything in the probable cause section of the warrant's application relating to what he saw in the cell phone while changing its settings. (Tr. at 27.) TFO Lepinski also testified that the change in the lock settings did not affect the affidavit for the warrant he submitted. (*Id.* at 28.) After TFO Lepinski obtained the search warrant, he brought Haynes's cell phone to the crime lab. (*Id.* at 48.) TFO Lepinski testified that he did not look through the phone after he brought it to the crime lab. (*Id.* at 49.) TFO Lepinski submitted a work request form asking the crime lab to search the phone. (*Id.* at 56.)

Officer Michael Gustafson, a computer forensic examiner with the MPD Crime Lab, also testified at the February 3, 2020 hearing. (*Id.* at 53-68.) Officer Gustafson testified that he searched Haynes's cell phone on August 21, 2019 using a forensic tool

called GrayKey. (*Id.* at 55.) GrayKey is only available only to law enforcement. (*Id.* at 57.) Officer Gustafson testified that GrayKey analyzes devices with an automated process. (*Id.*) According to Officer Gustafson, if the device is unlocked, the device will "ask you to trust it, which is called paired mode." (*Id.*) Officer Gustafson testified that when TFO Lepinski delivered Haynes's cell phone, "it was on, the screen was on, and the phone appeared to be unlocked." (*Id.*)

When Officer Gustafson connected Haynes's cell phone to GrayKey, the cell phone asked him if he wanted to trust the device. (*Id.*) Officer Gustafson told the cell phone to trust GrayKey, which then prompted him to enter the cell phone's passcode. (*Id.* at 58.) In order to trust the cell phone and put it into paired mode, the passcode is still required. (*Id.* at 61.) At that point, GrayKey allows one minute to enter the passcode before proceeding with its procedure as though the device was locked. (*Id.*) Gustafson testified that because he did not enter the passcode, GrayKey began its initial access procedure and attempted to gain access to the cell phone by working around the cell phone's security. (*Id.* at 59.)

The initial access procedure would have processed faster had the passcode been entered. (*Id.*) Without the passcode, some of the cell phone's information could not be accessed including some health-related data, some pictures, and some videos. (*Id.*) Officer Gustafson testified that even if the phone had been locked when connected to the GrayKey, it would have made "no difference" on his search. (*Id.*) Officer Gustafson explained that "because [he] didn't have the passcode to trust the GrayKey and [he] couldn't complete that digital handshake, the GrayKey proceeded as though the device's

passcode was active." (*Id.* at 60.) When a cell phone is left on, Officer Gustafson testified that it is in a less secure state called "after first unlock" or "AFU." (*Id.*) In these circumstances, GrayKey can extract most of the cell phone's data, even without a passcode. (*Id.*) Because Officer Gustafson did not have the passcode, GrayKey treated the phone as if it was locked. (*Id.*) Officer Gustafson was unaware that TFO Lepinski had changed the settings on the phone until he attempted to trust the device. (*Id.*)

Officer Gustafson later testified that "[t]he GrayKey cannot access 100 percent of Apple devices, but I would say if the device is left on at the time it is seized, whether it is locked or unlocked, and the user has been using the device, I would say roughly 90 percent or more of Apple devices can be accessed." (*Id.* at 62.) If the cell phone is left on, the chances increase of being able to access it with GrayKey. (*Id.*) Changing the screen lock time-out settings had no effect on Officer Gustafson's procedures. (*Id.*)

Officer Gustafson testified about the cell phone's thumbprint capabilities, known as Apple biometrics or Touch ID, and indicated that "for our purposes, the biometrics and the passcode are one and the same." (*Id.* at 63.) Normally, Officer Gustafson would perform a timestamp verification to verify the information in his report is the same as the phone. (*Id.* at 65.) However, Officer Gustafson was unable to perform the verification because the cell phone relocked after the data extraction. (*Id.*) Officer Gustafson estimated that he retrieved over 95 percent of the data that was on Haynes's cell phone. (*Id.* at 67.)

II. DISCUSSION

Haynes moves to suppress the following evidence:

> [a]ll physical evidence discovered, recovered, and/or seized arising out of the search and seizure of electronically stored data on Apple iPhone, white in color with pinkish colored case, crack screen protector (PI # 84339-002), including all SMS/MMS messaging, call log, contact list, all photo/video content, SIM card data, account information for email and social media accounts and any stored GPS locations, noted in the Application for Search Warrant by Officer Adam Lepinski, electronically signed 08/19/2019, and in the Search Warrant electronically signed by Judge Martha Holton Dimick on 08/20/2019.

(Dkts. 35, 59.)

The Court addresses Defendant's Motion and Supplemental Motion collectively below.

A. Motion to Suppress Evidence Obtained by Search and Seizure

In support of his motion to suppress the evidence arising out of the search and seizure of his cell phone, Haynes argues that "the opening of [his] phone and changing of his phone's settings constitute a search which was not supported by a search warrant or pursuant to any recognized exception to the search warrant-requirement, and therefore, the evidence should be excluded." (Dkt. 89 at 8.) Haynes further argues that TFO Lepinski's "action in going into the settings of Mr. Haynes' phone and changing those settings exceeded the scope of the consent authorization Mr. Haynes gave the police officer to retrieve phone numbers from the phone" and identified "consent searches" as one of the exceptions that did not apply to the changing of the settings. (Dkt. 59 at 3; Dkt. 89 at 8.) The Government counters that TFO Lepinski was justified in securing Haynes's cell phone. (Dkt. 94 at 5.) The Government argues that TFO Lepinski's

actions were reasonable and "tantamount to securing a scene in order to maintain the status quo while a search warrant was obtained." (*Id.* at 5-6.) In the alternative, the Government argues that the contents of Haynes's cell phone would be admissible under the independence source doctrine and inevitable discovery doctrine. (*Id.* at 8-11.)

1. Whether TFO Lepinski's Changes to the Settings Violated the Fourth Amendment

The Court first considers whether TFO Lepinski's changing of the cell phone settings to airplane mode and "never lock" violated the Fourth Amendment. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." U.S. Const. amend. IV. The basic purpose of the Fourth Amendment "'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (quoting *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967)). "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Id.* (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

Haynes argues that he had a reasonable expectation of privacy that the police would not be searching his phone to change the settings. (Dkt. 89 at 7.) Haynes also argues that TFO Lepinski's decision to change the settings constitutes a warrantless search that does not fall within any of the exceptions to the warrant requirement,

including the consent exception, and that changing the settings exceeded the scope of the consent authorization Haynes gave TFO Lepinski to retrieve phone numbers. (*Id.* at 7-8; Dkt. 59 at 3.) Relying on *Riley v. California*, 573 U.S. 373 (2014), the Government counters that TFO Lepinski took reasonable steps to secure Haynes's cell phone and to prevent the loss of evidence while he sought a warrant. (Dkt. 94 at 6-7.)

The U.S. Supreme Court in *Riley* held that the police generally may not, without a valid search warrant, search digital information on a cell phone seized from an individual who has been arrested. *See* 573 U.S. at 386. In so holding, the Supreme Court concluded: "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* at 403 (cleaned up). Data stored on cell phones is "qualitatively different" from physical records because searching a cell phone "would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 393-98.

The Supreme Court recognized, however, that a cell phone may be seized and secured to prevent destruction of evidence. *Id.* at 388-91. The Supreme Court focused on two types of destruction of evidence: remote wiping and encryption (which occurs when a phone is locked). *See id.* As explained in *Riley*:

> Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This can happen when a third party sends a remote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas (so-called "geofencing"). Encryption is a security feature that some modern cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that renders a phone all but 'unbreakable' unless police know the password.

Id. at 388-89 (citations omitted).

The Supreme Court, however, had "been given little reason to believe that either problem is prevalent." *Id.* at 389. The briefing in Riley "revealed only a couple of anecdotal examples of remote wiping triggered by an arrest." *Id.* Further, "[l]aw enforcement officers are very unlikely to come upon such a phone in an unlocked state because most phones lock at the touch of a button or, as a default, after some very short period of inactivity," and "an officer who seizes a phone in an unlocked state might not be able to begin his search in the short time remaining before the phone locks and data becomes encrypted." *Id.* at 389-90. However, the Supreme Court suggested that, "if officers happen to seize a phone in an unlocked state, they may be able to disable a phone's automatic-lock feature in order to prevent the phone from locking and encrypting data." *Id.* at 391. It further explained that "[s]uch a preventative measure could be analyzed under the principles set forth in our decision in *McArthur*, 531 U.S. 326, 121 S. Ct. 946, which approved officers' reasonable steps to secure a scene to preserve evidence while they awaited a warrant." *Id.*

As to remote wiping, the Supreme Court explained that:

> Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery. Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves. Such devices are commonly called "Faraday bags," after the English scientist Michael Faraday. They are essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use.

Id. at 390 (citations omitted).

Haynes argues that the Supreme Court's language in *Riley* is mere dicta and not the holding of the case. (Dkt. 89 at 9.) However, as the Government points out, the authority to secure a scene to maintain the status quo while obtaining a warrant existed prior to the holding in *Riley*. *See Segura v. United States*, 468 U.S. 796, 798 (1984) ("[W]here officers, having probable cause, enter premises, and with probable cause, secure the premises from within to preserve the status quo while others, in good faith, are in the process of obtaining a warrant, they do not violate the Fourth Amendment's proscription against unreasonable seizures."); *see also, e.g.*, *United States v. Ruiz-Estrada*, 312 F.3d 398, 404 (8th Cir. 2002) (securing an apartment to prevent the destruction of suspected narcotics supply while awaiting search warrant for 19 hours comports with the Fourth Amendment); *United States v. Roby*, 122 F.3d 1120, 1125 (8th Cir. 1997) (citing *United States v. Kulcsar*, 586 F.2d 1283, 1287 (8th Cir. 1978)) ("The officers entered, but took no investigative steps; they merely preserved the space and checked to assure their own safety. There was full compliance with the mandate of the Fourth Amendment."); *United States v. Burrell*, No. 06-81 (JNE/RLE), 2006 WL

1715608, at *21 (D. Minn. June 19, 2006) ("[W]e find that the 'freezing,' or seizure, of Brown's residence, until the issuance of a Search Warrant, was reasonable."). While these cases generally relate to securing the scene of a dwelling, this doctrine, as outlined in *McArthur*, could nevertheless be applied in the context of securing a cell phone as noted in *Riley*. *See* 573 U.S. at 373.

With that background, the Court considers whether TFO Lepinski's changing of the settings of Haynes' cell phone constitutes a search of his phone that violated the Fourth Amendment. The Government argues that TFO Lepinski's act in changing the settings was tantamount to securing a scene pending a search warrant. (Dkt. 95 at 5-7.) The Court has some concerns about this argument. TFO Lepinski did not "happen to seize a phone in an unlocked state" as contemplated in *Riley*. The cell phone was seized when TFO Lepinski walked Haynes to the First Precinct and searched him incident to arrest. (Tr. at 18.) The phone was locked when TFO Lepinski took it out of Haynes' pocket during the search incident to arrest. (*Id.* at 19 (phone locked when removed from Haynes' pocket); *see id.* at 18 (TFO Lepinski removed phone from Haynes' pocket during search incident to arrest).) It was not unlocked until TFO Lepinski retrieved it to obtain the phone numbers requested by Haynes and Haynes unlocked it with his thumbprint for that purpose. (*Id.* at 19.)

Further, Haynes unlocked the phone for TFO Lepinski so that he could obtain certain phone numbers (Gov't Ex. 1 at 2:35-2:51), but there is nothing in the record that suggests Haynes consented to TFO Lepinski's changing of the settings—particularly to a "never lock" setting. Rather, Haynes intended to turn the phone off when he returned it

to TFO Lepinski, Haynes was concerned about keeping his phone locked, and TFO Lepinski obfuscated as to whether the phone was locked after it was returned to him by Haynes in the holding cell. (Gov't Ex. 1 at 4:26-4:34 (Haynes saying he intended to turn phone off); Gov't Ex. 2 at 1:23-1:24 (TFO Lepinski asking Haynes for passcode "so I can get back into your phone" after he had already set the phone to "never lock"); Gov't Ex. 3 at 0:50-52 (TFO Lepinski responding "Yes, it is" when asked if the phone was locked up); Tr. at 28 (TFO Lepinski testifying that phone was unlocked when he told Haynes it was locked).) "When an official search is properly authorized—whether by consent or by the issuance of a valid warrant—the scope of the search is limited by the terms of its authorization." *Walter v. United States*, 447 U.S. 649, 656 (1980). The scope of consent to search is measured by a standard of objective reasonableness, *United States v. Urbina*, 431 F.3d 305, 310 (8th Cir. 2005), where the issue is what "the typical reasonable person [would] have understood by the exchange between the officer and the suspect," *Florida v. Jimeno*, 500 U.S. 248, 251 (1991). Here, a typical reasonable person would have understood that Haynes was not authorizing TFO Lepinski to change the settings in his phone.

Under these circumstances, it is not clear that the dicta in *Riley* suggesting that law enforcement can change settings on a phone to prevent encryption if they happen to seize a phone in an unlocked state or the case law authorizing securing a scene to maintain the status quo pending a warrant would apply to the facts of this case. *Compare United States v. Bell*, Case No. 15-10029, 2016 WL 1588098, at *2-6 (C.D. Ill. April 20, 2016) (opening flip phone to turn it off constituted warrantless search of phone not subject to

preservation of evidence exception where phone could have been turned off or the battery removed), *with United States v. Cain*, Case No. 1:15-cr-00103-JAW, 2017 WL 1507422, at *4-5 (D. Me. April 27, 2017) ("The steps taken by Agent Collier to activate airplane mode, after Defendant told Agent Collier he could look at the phone and after Defendant provided the security code, were no more intrusive than the steps that would be required to 'disable a phone's automatic-lock feature in order to prevent the phone from locking and encrypting data,' a measure the Supreme Court described as one reasonable approach to preserve data on an unlocked cellular phone.") (citing *Riley*, 573 U.S. at 391). The Court need not decide this question, however, because even if TFO Lepinski's actions constituted a search that violated the Fourth Amendment, the Court concludes for the reasons explained below that the evidence from the cell phone obtained pursuant to the search warrant is admissible under the independent source and inevitable discovery doctrines.

2. Independent Source Doctrine

The Government argues that the independent source doctrine would render the evidence obtained pursuant to the search warrant admissible notwithstanding any error made by TFO Lepinski in securing Haynes's cell phone. (Dkt. 94 at 8-10.) Haynes argues that the Government has failed to establish that the tainted evidence would have been obtained independently after the search warrant was secured. (Dkt. 89 at 10.) The Court agrees with the Government.

"The independent source doctrine allows admission of 'evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained

independently from activities untainted by the initial illegality.'" *United States v. Anguiano*, 934 F.3d 871, 874 (8th Cir. 2019) (quoting *Murray v. United States*, 487 U.S. 533, 537 (1988)). To invoke the independent source doctrine, the Eighth Circuit requires the Government to demonstrate: "(1) that the decision to seek the warrant was independent of the unlawful entry—i.e., that police would have sought the warrant even if the initial entry had not occurred—and (2) that the information obtained through the unlawful entry did not affect the magistrate's decision to issue the warrant.'" *Anguiano*, 934 F.3d at 874 (quoting *United States v. Khabeer*, 410 F.3d 477, 483 (8th Cir. 2005)).

Here, the record shows that TFO Lepinski's decision to seek the warrant was independent of the unlawful entry. With respect to the first prong, TFO Lepinski testified that his intention was to obtain a warrant to search the phone and that he only changed the settings in order to facilitate the warrant. (Tr. at 21, 25-25.) As to the second prong, TFO Lepinski testified that he never attempted to obtain or actually obtained any substantive content from the phone (other than the contact information requested by Haynes) when changing the settings. (*Id.* at 21-22, 27-28.) In addition, TFO Lepinski testified that he did not mention anything in the probable cause section of the warrant's application about changing the settings or anything he saw while doing so. (Tr. at 27.) Therefore, the record shows that TFO Lepinski's decision to change the settings to airplane mode and "never lock" did not affect Judge Dimick's decision to issue the search warrant.

Haynes argues that if TFO Lepinski "had secured the phone by turning it off or removing the battery, as suggested by the Supreme Court in *Riley*, it would have been

more difficult for the Government to obtain the protected data" because, according to Haynes, "Officer Gustafson's testimony is that if the phone is turned off, the workaround to bypass password protection is more difficult and would only be successful 90% of the time." (Dkt. 89 at 10 (citing Tr. at 62).) Officer Gustafson actually testified that "I would say if the device is left on at the time it is seized, whether it is locked or unlocked, and the user has been using the device, I would say roughly 90 percent or more of Apple devices can be accessed." (Tr. at 62:2-7.)

The Government argues that Haynes is conflating locking and remote wiping. (Dkt. 94 at 9.) When TFO Lepinski changed the settings to "never lock," he believed (apparently erroneously, as it turned out) that he was preventing the destruction of evidence that could occur if the phone locked, thereby encrypting the data. (Tr. at 38-39.) By placing the phone in airplane mode, TFO Lepinski—who did not have a Faraday bag or box or any other equipment for securing the cell phone such that it could not communicate with a network (Tr. at 36-37)—sought to prevent evidence destruction by remote wiping.

Haynes' argument assumes that the only options TFO Lepinski had were (1) turn the phone off to prevent remote wiping or (2) place the phone in airplane mode (which he contends is an illegal search). That is not accurate. TFO Lepinski had the option of doing nothing, and leaving the phone in a powered-on, locked state—the status quo of the phone when seized. Indeed, it appears unlikely that TFO Lepinski would have turned the cell phone off due to remote wiping concerns, because that would lock the phone. (*See* Tr. at 66.) If the phone had been kept in its powered-on, locked state, it would have been

in an AFU state, and GrayKey would have extracted the same data that was extracted from the phone in its unlocked state. (Tr. at 59-60.) For these reasons, the Court finds that the results of the search of Haynes' cell phone after TFO Lepinski obtained a warrant constitute an independent source of the evidence, and recommends denial of the Motion and Supplemental Motion on that basis.

3. Inevitable Discovery Doctrine

The Government also argues that the evidence retrieved from Haynes's cell phone would be admissible under the inevitable discovery doctrine. (Dkt. 94 at 10.) Under the inevitable discovery doctrine, evidence need not be suppressed if the Government can prove by a preponderance of the evidence that: "(1) there is a reasonable probability the evidence would have been discovered by lawful means in the absence of police misconduct, and (2) the government was actively pursuing a substantial, alternative line of investigation at the time of the constitutional violation." *United States v. Thomas*, 524 F.3d 855, 859 (8th Cir. 2008) (citing *United States v. Glenn*, 152 F.3d 1047, 1049 (8th Cir. 1998)).

Here, the record shows that there was, at a minimum, a reasonable probability that the evidence obtained from the cell phone would have been obtained pursuant to the warrant even if TFO Lepinski had not changed the settings. First, as discussed above, TFO Lepinski intended to seek a warrant for the cell phone and the change in settings did not affect the affidavit he submitted. (Tr. at 21, 27-28.) Second, the record reflects that if TFO Lepinski had not changed the settings to "never lock" and airplane mode (but kept the phone on), GrayKey would have obtained the same data off the phone. (*Id.* at 59.)

Finally, in view of Officer Gustafson's testimony that even if the cell phone had been turned off, GrayKey would have been able to obtain "some pictures, some videos, some user account information, things of that nature, but it won't get any communication data" unless a "brute force" method was successful (Tr. at 67), and in the absence of any evidence identified by Haynes for suppression that GrayKey would not have been able to obtain if the cell phone had been turned off, the Court finds that the Government has shown by a reasonable probability that the evidence would have been obtained pursuant to the warrant. Accordingly, the Court finds that the inevitable discovery doctrine applies, and recommends denial of the Motion and Supplemental Motion on that ground as well.

B. Whether the August 2019 Search Warrant is Supported by Probable Cause

In his Motion to Suppress Search and Seizure filed on November 12, 2019, Haynes argues that the August 2019 Search Warrant was not supported by probable cause, contains information supplied by a confidential informant whose reliability and trustworthiness was not established, and contains inaccurate information and unsupported allegations. (Dkt. 35 at 2.) Haynes reasserts these bases in his Supplemental Motion. (Dkt. 59 at 2.) He did not include any argument on these points in his post-hearing briefing.

A reviewing court must evaluate a search warrant in its entirety and in a commonsense manner. *See Illinois v. Gates*, 462 U.S. 213, 230-31 (1983). Ordinarily, searches pursuant to a warrant are reviewed to determine if there was probable cause for the search in the search warrant application and affidavit. *See id.* at 236. "Probable

cause exists when, given the totality of the circumstances, a reasonable person could believe there is a fair probability that contraband or evidence of a crime would be found in a particular place." *United States v. Fladten*, 230 F.3d 1083, 1085 (8th Cir. 2000) (citing *Gates*, 462 U.S. at 238). The task of a court issuing a search warrant is "simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. "Probable cause is a fluid concept that focuses on 'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.'" *United States v. Colbert*, 605 F.3d 573, 576 (8th Cir. 2010) (quoting *Gates*, 462 U.S. at 231). In reviewing the decision of the issuing court, the duty of the reviewing court is simply to ensure that the court had a substantial basis for concluding that probable cause existed. *See Gates*, 462 U.S. at 238-39 (citation omitted); *see also United States v. LaMorie*, 100 F.3d 547, 552 (8th Cir. 1996) (citation omitted) ("Our duty as a reviewing court is to ensure that the issuing judge had a 'substantial basis' for concluding that probable cause existed, and we owe substantial deference to the determination of probable cause by the issuing judge."). As to what this Court should consider when reviewing a search warrant for probable cause, "[w]hen the [issuing judge] relied solely on the affidavit presented to him, 'only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause.'" *United States v. Solomon*, 432 F.3d 824, 827 (8th Cir. 2005) (citing *United States v. Etheridge*, 165 F.3d 655, 656 (8th Cir.

1999), quoting *United States v. Gladney*, 48 F.3d 309, 312 (8th Cir. 1995)); *United States v. Smith*, 581 F.3d 692, 694 (8th Cir. 2009) (quoting *United States v. Reivich*, 793 F.2d 957, 959 (8th Cir. 1986)).

Here, Haynes has not identified any specific deficiencies, including the alleged "inaccurate information and unsupported allegations" in the August 2019 Affidavit, nor can the Court discern any after careful review. The facts in the affidavit as set forth above, including the surveillance video showing the suspect using an iPhone in a pinkish case to take a photograph of a Western Union receipt before apparently obtaining the handgun used in the shooting, the interview with A.H., the identification by the CRI of a photo of the suspect from the surveillance video as "Bad Ass," the database showing Haynes uses the moniker "Bad Ass," and cell phone call records showing Haynes' and A.H.'s cell phones at the scene of the shooting, along with the reasonable inferences drawn therefrom, established a sufficient nexus between the evidence sought—the photograph of the receipt and contact information for the person believed to have brought the handgun to the scene of the shooting—and the cell phone. To the extent Haynes challenges the reliability of the CRI, the CRI's identification of the suspect as "Bad Ass," where that moniker is recorded as belonging to Haynes, is corroborated by the interview with A.H. and the cell phone call detail records. *See United States v. Faulkner*, 826 F.3d 1139, 1144 (8th Cir. 2016) (holding reliability of confidential informant "can be established through independent corroboration"). Accordingly, based on the totality of the circumstances, the Court concludes that the search warrant was supported by probable cause.

C. Haynes's Motion for a *Franks* Hearing

Finally, in his Supplemental Motion, Haynes seeks a *Franks* hearing regarding the August 2019 Affidavit.[2] (Dkt. 59 at 4-5, *see* Dkt. 60 (affidavit of counsel).) Haynes argues that TFO Lepinski made a material omission, in reckless disregard of the truth, in his allegation of facts in support of the issuance of the search warrant by failing to disclose to the Court that he had accessed Mr. Haynes' cell phone to change the settings. (Dkt. 60.) The Government contends that Haynes has failed to show that the August 2019 Affidavit contained any false statements or material omissions or that statements or omissions were made knowingly and intentionally, or in reckless disregard for the truth. (Dkt. 62 at 4.) In addition, the Government argues that even if Haynes had shown TFO Lepinski made a false statement that was knowingly and intentionally made, or made in reckless disregard of the truth, he has not shown that including the fact that he changed the phone settings in the August 2019 Affidavit would have affected the finding of probable cause. (Dkt. 62 at 4-5.) The Court agrees.

Pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), a defendant may seek a hearing to challenge a search warrant on the ground that the supporting affidavit contains factual misrepresentations or omissions relevant to the probable cause determination. *See United States v. Daigle*, 947 F.3d 1076, 1084 (8th Cir. 2020). "However, in order to merit a *Franks* hearing, a defendant must show both (1) that the affiant knowingly and intentionally made false statements or made them in reckless disregard for the truth and

[2] Haynes did not address his request for a *Franks* hearing in his post-hearing brief; nevertheless, the Court addresses the request here.

(2) if the false information is excised (or the omitted information is included), the affidavit no longer establishes probable cause." *Id.* This "requirement is not met lightly and requires a defendant to offer specific allegations along with supporting affidavits or similarly reliable statements." *United States v. Gonzalez*, 781 F.3d 422, 430 (8th Cir. 2015) (citation omitted); *see also Franks*, 438 U.S. at 171 ("Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained."); *United States v. Mathison*, 157 F.3d 541, 548 (8th Cir. 1998) ("A mere allegation standing alone, without an offer of proof in the form of a sworn affidavit of a witness or some other reliable corroboration, is insufficient to make the difficult preliminary showing [under *Franks*]."). Moreover, "[a] *Franks* hearing must be denied unless the defendant makes a **strong** initial showing of deliberate falsehood or reckless disregard of the truth." *United States v. Freeman*, 625 F.3d 1049, 1052 (8th Cir. 2010) (internal quotations and citation omitted) (emphasis added).

Here, even if the Court assumed TFO Lepinski's failure to disclose that he had changed the settings on the phone to airplane mode and "never lock" constituted an omission that was made intentionally and knowingly or with reckless disregard for the truth, there is no reason to believe that learning of the change in settings would have affected Judge Dimick's probable cause decision. TFO Lepinski has testified that he only changed those two settings, and Haynes has not explained how changing those settings would have affected the likelihood that the sought-after evidence relating to the shooting (photos and contact information) would be found on the cellular phone or any other aspect of the probable cause finding, much less that the omission was necessary to the

finding of probable cause. As discussed in Section II.B, *supra*, the Court finds ample probable cause to support the warrant. Consequently, the Court recommends denial of Haynes' request for a *Franks* hearing on the information provided in the August 2019 Affidavit.

III. RECOMMENDATION

Based on the files, records, and proceedings herein, **IT IS RECOMMENDED THAT:**

1. Defendant's Motion to Suppress Search and Seizure (Dkt. 35) be **DENIED**; and

2. Defendant's Supplemental Motion to Suppress Search and Seizure (Dkt. 59) be **DENIED**; and

3. Defendant's request for a *Franks* Hearing be **DENIED**.

DATED: April 27, 2020

s/Elizabeth Cowan Wright
ELIZABETH COWAN WRIGHT
United States Magistrate Judge

NOTICE

Filing Objections: This Report and Recommendation is not an order or judgment of the District Court and is therefore not appealable directly to the Eighth Circuit Court of Appeals.

Under District of Minnesota Local Rule 72.2(b)(1), "a party may file and serve specific written objections to a magistrate judge's proposed finding and recommendations within 14 days after being served a copy" of the Report and Recommendation. A party may respond to those objections within 14 days after being served a copy of the objections. D.

Minn. LR 72.2(b)(2). All objections and responses must comply with the word or line limits set for in D. Minn. LR 72.2(c).