[PUBLISH]

In the

United States Court of Appeals

For the Eleventh Circuit

No. 23-10184

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

JOHNNIE LEEANOZG DAVIS,

Defendant- Appellant.

Appeal from the United States District Court
for the Middle District of Alabama
D.C. Docket No. 2:21-cr-00101-MHT-JTA-1

Before WILLIAM PRYOR, Chief Judge, and JORDAN and BRASHER, Circuit Judges.

BRASHER, Circuit Judge:

The main question in this appeal is an issue of first impression about Fourth Amendment standing to challenge a geofence warrant. Johnnie Davis was convicted under 18 U.S.C. § 2119 of committing a string of carjackings in the Montgomery, Alabama, area. Before trial, Davis moved to suppress two pieces of evidence (1) the location of his girlfriend's phone that the police obtained from Google through a geofence warrant and (2) inculpatory statements Davis made after being arrested on state charges. At trial, Davis moved for a judgment of acquittal on the grounds that the government failed to prove his intent to cause death or serious harm to his victims. The district court denied these motions.

Davis raises the same three arguments on appeal. He argues that the geofence warrant that led the police to identify his girlfriend's phone did not adequately define the places and things to be searched. He argues that he should have been presented to a United States magistrate judge before being interviewed, even though he was in state custody. And he argues that his use of a gun to commit the carjackings was insufficient to establish the intent element of the crime.

We reject these arguments. We agree with the district court that Davis lacks Fourth Amendment standing to challenge the geofence warrant because the search did not disclose any information about the data on his own electronic device, reflected only

his limited movements in public areas, and did not encompass his home. Because we cannot say the district court clearly erred in finding that federal law enforcement did not improperly collude with state law enforcement in arresting and interviewing Davis, we likewise agree with the district court that the federal presentment requirements set out in Federal Rule of Criminal Procedure 5(a) and 18 U.S.C. § 3501(c) did not apply when Davis was in state custody. Finally, we agree with the district court that Davis's use of a gun during the carjackings sufficiently established Davis's intent to cause death or serious harm.

Accordingly, we affirm.

I.

The Montgomery Police Department began investigating a string of carjackings and robberies that occurred between 2014 and 2017 in the Montgomery, Alabama, area. In 2017, the MPD sought assistance from the FBI to seek warrants for cell tower location information to further the investigation. Nathan Faggert, who served as a Sergeant with the MPD and as a task force officer with the FBI, initiated an FBI investigation into thirty-five incidents he believed were committed by the same suspect. Faggert worked the investigation in a dual capacity, and the MPD and the FBI collaborated through him and another MPD detective. Faggert regularly updated his supervisors at the MPD and the FBI about the progress of the investigation and how the FBI could best support the MPD—the FBI primarily focused on digital information gathering while

the MPD responded to robberies, interviewed witnesses, and developed leads.

During the ongoing investigation, four more robberies and three more carjackings occurred on January 23, 2020, October 30, 2020, and November 11, 2020. Law enforcement suspected that the same person responsible for the crimes under investigation also committed the three new offenses.

The carjacking and robbery on January 23, 2020, involved a masked man who approached a vehicle, gestured toward a gun in his waistband, and demanded the vehicle, telling the driver not to move and that he wanted her car. The victim testified that she believed the robber would have shot her had she not complied. Later that night, a masked man used the stolen car to rob a gas station in the area. The MPD obtained video surveillance of the area where the suspect dumped the stolen vehicle, and the video showed the suspect get into another car to make his escape. The getaway vehicle's license plate was registered to Stacey Gilbert, the sister of Davis's girlfriend, Portia Gilbert.

Faggert prepared and presented a geofence warrant to Google, seeking information on Google devices and accounts located within forty to one hundred meters of six locations on January 23 and 24, around the time of the carjacking and robbery occurred. The times and locations corresponded with video surveillance that captured the suspect in action.

Google responded to the warrant by providing an anonymized list of devices and accounts that connected to its services at

the times and locations designated in the warrant. Faggert analyzed this data and identified three devices relevant to the investigation. Google "unmasked" those devices, i.e., disclosed the identifying information, and Faggert determined that only one device appeared to be related. Specifically, Google identified a Gmail account open on a device in the getaway car as it was captured by video surveillance at the areas of the carjacking, business store robbery, and where the carjacked vehicle was abandoned. The device belonged to Portia Gilbert, and the Gmail account was registered to Gilbert's daughter.

Another carjacking and robbery occurred in the Montgomery area on October 30, 2020. A man and his fifteen-year-old son, who had pulled over to switch drivers, were approached by a masked man, who put two pistols in the son's face and told them to run. The father later testified that the man probably would have shot his son if they had not given up the car. That same night, the stolen car was used in a robbery at a nearby Dollar General.

MPD obtained video surveillance from the night of October 30 that showed a man exit a vehicle in the area of the carjacking and walk towards the scene of the carjacking. MPD obtained other video surveillance that showed the same vehicle at a gas station. MPD determined that the vehicle was rented to Davis, pulled the GPS data for the vehicle, and discovered that it was near the carjacking on October 30. The police used the cell phone number Davis listed in the rental agreement to obtain a warrant that allowed police to track the phone in real time.

A final carjacking and robbery took place on November 11, 2020. A masked man approached the victim's vehicle, stuck a gun through the window, and told the driver, "don't think about it." The perpetrator stole the car, and the victim later said that he believed he could have been shot. Later that night, a masked man used the car to rob a Fresh Market and a Dollar General store in the area. Upon learning of these new crimes, law enforcement checked the status of Davis's phone and discovered that it was present at both the Fresh Market and the Dollar General during the crimes.

The next day, Faggert and another Montgomery Police Detective sought and executed state search and arrest warrants for Davis and residences he was known to frequent. Faggert arrested Davis on eight state charges related to the string of robberies and carjackings. The MPD took Davis into custody and placed him in a holding cell. He was provided lunch, waived his Miranda rights, and gave a statement to Faggert and an FBI special agent about eight hours after he was initially detained. He confessed to the October 30 and November 11 crimes but denied involvement in the January 23 crimes.

Faggert initiated this federal case by filing a complaint against Davis on December 3, 2020. A grand jury of the Middle District of Alabama returned a 10-count indictment against Davis and later returned a 14-count superseding indictment. Davis was tried on the superseding indictment, which alleged three counts of carjacking in violation of 18 U.S.C. § 2119; four counts of Hobbs Act

robbery in violation of 18 U.S.C. § 1951; and seven counts of brandishing a firearm during those crimes of violence in violation of 18 U.S.C. § 924(c)(1)(A).

Davis moved to suppress his post-arrest inculpatory statements admitting to two of the carjackings and three of the robberies. He argued that they were obtained in violation of his right to presentment under Federal Rule of Criminal Procedure 5(a) and 18 U.S.C. § 3501(c) because the investigation and his arrests were federal in nature and his statements took place about eight hours after he was detained. The magistrate judge found that Davis was in custody only on state charges at the time he gave the statements and that state law enforcement did not improperly collude with federal law enforcement to deny his presentment rights. The district court adopted the magistrate judge's report and recommendation to the extent that it found Davis lacked a federal right to presentment.

Davis also moved to suppress the evidence that the government obtained via the geofence warrant. He argued that the warrant was invalid, and the *Leon* good faith exception did not apply. The magistrate judge held two hearings on the motion and recommended that the district court deny it, concluding that Davis lacked Fourth Amendment standing to challenge the warrant because he had no privacy interest in the search of his girlfriend's phone or her daughter's Google account. It also concluded that even if Davis had Fourth Amendment standing, his challenges to the warrant failed

because the *Leon* good faith exception applied. The district court adopted the magistrate judge's recommendation.

At the end of trial, the district court dismissed the Hobbs Act robbery counts and accompanying brandishing counts because the government did not establish an interstate nexus for those crimes. The jury convicted Davis on the remaining counts, and Davis was sentenced to 315 months of imprisonment. This timely appeal followed.

II.

We review a district court's denial of a motion to suppress under a mixed standard, reviewing the district court's findings of fact for clear error and its application of law to those facts *de novo*. *See United States v. McCall*, 84 F.4th 1317, 1322 (11th Cir. 2023). We review challenges to the sufficiency of the evidence *de novo* but "view[] the evidence in the light most favorable to the government and draw[] all reasonable inferences and credibility choices in favor of the jury's verdict." *United States v. Taylor*, 480 F.3d 1025, 1026 (11th Cir. 2007).

III.

Davis raises three issues in his appeal. First, he argues the district court erred in allowing the evidence obtained from the geofence warrant. He says that he has Fourth Amendment standing to challenge the geofence warrant because the search invaded his reasonable expectation of privacy. He also challenges the merits of the warrant and says the *Leon* good faith exception does not

apply. Second, he argues the district court erred in denying his motion to suppress the inculpatory statements he made to law enforcement after his arrest because the government violated his right to presentment under Federal Rule of Criminal Procedure 5(a) and 18 U.S.C. § 3501(c). He says that the federal presentment rules apply even though he was arrested on state charges and taken into state custody because the investigation and his arrest were federal in nature due to improper collusion between federal and state authorities. Third, Davis argues the district court should have granted his motion for judgment of acquittal because the government did not present sufficient evidence of his intent to kill or seriously harm his victims under 18 U.S.C. § 2119. We address each argument in turn.

A.

We begin with Davis's argument that the district court erred in denying his motion to suppress the information law enforcement discovered via the geofence warrant. His argument is two-part. First, he says that the district court erred in concluding that he lacked Fourth Amendment standing to challenge the warrant. Second, he says the warrant was invalid and that the *Leon* good faith exception does not apply to excuse the lack of a valid warrant. We agree with the district court that Davis lacks Fourth Amendment standing to challenge the geofence warrant, so we need not consider whether the warrant was defective or if the *Leon* good faith exception applies.

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 government officials." *Camara v. Mun. Ct. of City and Cnty. of S.F.*, 387 U.S. 523, 528 (1967). Thus, Fourth Amendment protection "extend[s] to any thing or place with respect to which a person has a 'reasonable expectation of privacy.'" *United States v. Ross*, 963 F.3d 1056, 1062 (11th Cir. 2020) (en banc) (quoting *California v. Ciraolo*, 476 U.S. 207, 211 (1986)). Conversely, "an individual's Fourth Amendment rights are *not* infringed—or even implicated—by a search of a thing or place in which he has no reasonable expectation of privacy." *Id.*

We refer to "whether an individual has a reasonable expectation of privacy in the object of the challenged search" as Fourth Amendment standing. *Id.* But Fourth Amendment standing is nothing more than "a useful shorthand for capturing the idea that a person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search." *Byrd v. United States*, 584 U.S. 395, 410–11 (2018). It "should not be confused with Article III standing, which is jurisdictional and must be assessed before reaching the merits." *Id.*

Whether and when a geofence warrant affects a person's reasonable expectation of privacy is an issue of first impression for our circuit. *See, e.g.*, *United States v. Davis*, 2022 WL 3009240, at *7

(M.D. Ala. July 1, 2022) (explaining that district courts in our circuit are "in unchartered territory in light of the paucity of decisions" from the Eleventh Circuit on geofence warrants (internal quotation marks omitted)), *report and recommendation adopted*, 2022 WL 3007744 (M.D. Ala. July 28, 2022). So we will first explain how a geofence warrant generally operates and then consider the Fourth Amendment implications.

1.

A geofence warrant is a specific type of warrant used to collect information on the presence of a cell phone or other device within a specific area during a set time frame, typically corresponding with the timing and location of a crime. *See*, *e.g.*, *Matter of Search of Info. That is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 69 (D.D.C. 2021). These warrants seek data from a company, like Google, that has access to device location through the company's users. *See United States v. Rhine*, 2023 WL 372044, at *66–67 (D.D.C. Jan. 24, 2023). Geofence warrants are particularly useful when investigators know the location and time of a crime but cannot identify a suspect. *Id.* at *66.

Although a court may order a company to turn over data in other ways, geofence warrants served on Google have typically followed a three-step process. *See*, *e.g.*, *United States v. Chatrie*, No. 22-4489, ___ F. 4th ___, 2024 WL *3335653*, at *2–*3* (4th Cir. July 9, 2024). First, law enforcement specifies the geographic area and timeframe for the search, directing the company where and when to gather data. Second, the company provides law enforcement

with an anonymized list of users or devices that match the warrant's temporal and geographical criteria. At this point, law enforcement may seek additional information about specific users outside of the initial search parameters. Third, law enforcement analyzes that information and requests that the company "unmask" certain users and release further identifying information. Law enforcement then uses that identifying information to determine whether any of the users may be connected to the crime.

Law enforcement and Google followed that process here. The geofence warrant directed Google to gather user information within fifteen to forty minutes, and within a forty-to-one-hundred-meter radius of six specified locations. These times and locations corresponded to video surveillance and other evidence from the January 23, 2020, robbery and carjacking, and each location was a section of a public road the suspect travelled on in carrying out the crimes. Google provided an anonymized list of users present at the specified times and locations. Law enforcement identified three devices on the list that appeared to be connected to the investigation, and Google "unmasked" the identifying information for those devices.

A Gmail account on one of those devices was open in the getaway car when video surveillance captured the suspect entering the car. The device belonged to Davis's girlfriend, and the Gmail account on the device was registered to her daughter. Law enforcement later determined that the device was in the areas where the January 23 carjacking and robbery occurred, as well as in the area

where the stolen car was later recovered. This is the evidence that Davis seeks to suppress.

2.

We now turn to whether Davis has Fourth Amendment standing to challenge the search of Google's records. The Fourth Amendment's protections "extend to any thing or place with respect to which a person has a 'reasonable expectation of privacy[.]'" *Ross*, 963 F.3d at 1062 (quoting *Ciraolo*, 476 U.S. at 211). We thus answer the standing question by deciding whether Davis has a cognizable Fourth Amendment privacy interest in the place, items, or property searched under the geofence warrant. We hold that he does not.

We will start with the third-party doctrine. A geofence warrant authorizes the government to search information in the database of a communications company, not in the possession of the user. Ordinarily, a person cannot challenge the search of a third party, even if it divulges "information he voluntarily turn[ed] over to [that] third part[y]." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *see Alderman v. United States*, 394 U.S. 165, 174 (1969) ("Fourth Amendment rights are personal rights which . . . may not be vicariously asserted."). The government routinely makes informal requests and issues subpoenas to businesses to get information about their customers, such as bank records. The background presumption in our law is that the government may access voluntarily disclosed electronic data in the same way without implicating an individual's privacy interest. *See United States v. Trader*, 981 F.3d

961, 967–68 (11th Cir. 2020) (third-party doctrine allows government to find email address and internet protocol address that were disclosed to Kik); *United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019) (no Fourth Amendment "search" when T-Mobile voluntarily shared cell-site data). In other words, we start from the presumption that an individual like Davis cannot challenge a search of Google's records.

Davis argues that, notwithstanding Google's status as a third party, he has a privacy interest that allows him to challenge this geofence warrant. Specifically, he argues that he "possessed a privacy interest in the tracking of his movements through the movements of" his girlfriend's phone. We disagree. We consider the applicability of three individual privacy interests and hold that none of them apply to the geofence search at issue in this appeal.

First, and most obviously, the third-party doctrine does not apply to a search of a person's private information in the possession of a third party if that person did not voluntarily disclose that information to the third party. The Supreme Court has recognized that we have a privacy interest in the "digital content on cell phones." *Riley v. California*, 573 U.S. 373, 385 (2014). But, under the third-party doctrine, this interest is not protectible if the individual voluntarily disclosed that information to the third party that is the target of the search.

In the usual case, we would need to assess whether the information in Google's possession was voluntarily disclosed. But we need not address that question here because the geofence warrant

revealed a third party's Gmail account registered in someone else's name on a phone that Davis did not own or exclusively use. Even if a person has a privacy interest in the data on his own phone, he does not have that interest in the data on someone else's phone. Because the geofence revealed the location of an open program that was not Davis's and was not on a phone in his exclusive possession or control, he cannot argue that he had a privacy interest in this data that gives him Fourth Amendment standing to challenge the search. In other words, because the information that Google disclosed wasn't Davis's to begin with, it doesn't matter whether the information was voluntarily or involuntarily provided to Google.

Second, Davis argues that a geofence warrant may invade an individual's reasonable expectation of privacy if it effectively tracks that individual's movements over an extended period of time. The Supreme Court has held that a person has a reasonable expectation of privacy in the whole of his physical movements that may be implicated by near-constant electronic surveillance. *See Carpenter v. United States*, 585 U.S. 296, 310–13 (2018); *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring), 430 (Alito, J., concurring in judgment). Because we are so attached to our cell phones, "when the Government tracks the location of a cell phone" for an extended period, "it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Carpenter*, 585 U.S. at 311–12.

Again, however, this geofence warrant doesn't implicate those Fourth Amendment concerns. As the district court explained, the scope of this search was far more restricted than "near perfect surveillance." That is, the geofence warrant captured only information within one hundred meters of specific locations for fifteen to forty minutes at each location. *Cf. Carpenter*, 585 U.S. at 316 (declining to address "tower dumps" or "a download of information on all the devices that connected to a particular cell site during a particular interval"). One of our sister circuits recently agreed that a limited search via a geofence warrant served on Google that seeks a user's location history does not implicate the same privacy concerns raised in *Carpenter*. *See Chatrie*, 2024 WL 3335653.

Moreover, this warrant did not track Davis's personal movements because the information it returned was not linked to his own cell phone, an account in his name, or something he exclusively used. Instead, the location of Davis's girlfriend's phone could "be translated" into Davis's location "only indirectly," and Davis lacks a privacy interest in this kind of indirect location data in the records of a third party. *Trader*, 981 F.3d at 968.

Third, it is axiomatic that a person has a reasonable expectation of privacy in his home. *See Kyllo v. United States*, 533 U.S. 27, 33 (2001). And that reasonable expectation of privacy generally prevents the government from using new technology "to explore details of the home that would previously have been unknowable without physical intrusion." *Id.* at 40.

Of course, the geofence warrant here did not seek data from Davis's home or any other area in which Davis had a reasonable expectation of privacy. The warrant sought Google user location information for six public locations and up to one hundred meters around those areas. To the extent the warrant returned information about someone's private property, it was not Davis's. Accordingly, Davis cannot establish that he had a reasonable expectation of privacy based on the areas searched via the geofence warrant.

Although Davis lacks any of these interests, he argues that he has Fourth Amendment standing to challenge the search because he has a Google account, even though it was not the account that Google identified and disclosed to law enforcement. Davis's theory is that Google's initial search of its internal data touched all Google accounts that exist, as it culled that data for accounts within the geofence parameters. Even though only a subset of that data was turned over to law enforcement, Davis argues that every Google account holder has Fourth Amendment standing to challenge the geofence warrant that caused Google to look at its data. We disagree for two reasons.

First, there is no evidence in the record to support Davis's claim that the geofence warrant required Google to search every existing Google account. The warrant requested information only for devices and accounts present within certain areas and during specific times. The record does not establish how Google compiled

that information, so Davis's assertion that his account must have been implicated is speculative.

Second, even if Google did have to search every single account when it sought to determine which devices were subject to the warrant, that search would not implicate Davis's Fourth Amendment rights. The Constitution is not concerned with a private party's search of its own records. *See*, *e.g.*, *Walter v. United States*, 447 U.S. 649, 656 (1980); *Chatrie*, 2024 WL 3335653, at *8, n.16 (explaining that "*Carpenter* . . . held that a search only occurs once the *government* accesses the requested information."). It is undisputed that no information related to Davis's device or account was divulged to the government. The initial trove of data that Google released was not only anonymous but also limited to the areas and times specified in the warrant. Nothing in the record suggests that Davis had a Google account or device within the searched locations, and even if he did, neither Davis's devices nor his account were later "unmasked." Even if Davis's Google account was swept up in Google's preliminary review, the government's search did not touch on a privacy interest because the government never received any information about his account.

To sum up, Davis lacks standing to challenge this geofence warrant. The background presumption is that an individual has no standing to challenge the search of records that he voluntarily gave to a third party. And no arguable exception to that presumption applies here. The mere fact that Google may have reviewed Davis's Google account is irrelevant if Google did not disclose information

about that account to law enforcement. Because the geofence warrant did not implicate Davis's expectation of privacy in anything, he lacks Fourth Amendment standing to challenge it.

B.

Davis next argues that his inculpatory statements to law enforcement after his arrest should be suppressed because the government violated his right to timely presentment under Federal Rule of Criminal Procedure 5(a) and 18 U.S.C. § 3501(c).

Rule 5(a) imposes a duty on law enforcement to present a person to a federal magistrate "without unnecessary delay" when the person is arrested for a federal offense. *Corley v. United States*, 556 U.S. 303, 308 (2009). Section 3501(c) operates as a six-hour "safe harbor" period following a person's arrest or detention, wherein statements made "shall not be inadmissible solely because of delay in bringing such person before a magistrate judge." 18 U.S.C. § 3501(c). That period may extend beyond six hours if the delay in presentment to a judicial officer is "reasonable considering the means of transportation and the distance to be traveled to the nearest available such magistrate judge or other officer." *Id.* Thus, if a defendant makes incriminating statements beyond the safe harbor period and before presentment to the magistrate judge, those statements must be suppressed if the delay was unreasonable or unnecessary. *See Corley*, 556 U.S. at 322.

The general rule is that the presentment requirements of Section 3501(c) and Rule 5(a) do not apply "[u]ntil a person is arrested or detained for a *federal* crime." *United States v. Alvarez-*

Sanchez, 511 U.S. 350, 358 (1994) (emphasis added). This is true even when the person is arrested and held on state charges but officers "believe or have cause to believe that the person also may have violated federal law." *Id.* Indeed, "[a]s long as a person is arrested and held only on state charges by state or local authorities," Section 3501(c) and Rule 5(a) are not triggered. *Id.*

An exception to this general rule "might" exist "if the defendant [can] demonstrate the existence of improper collusion between federal and state or local officers." *Id.* at 359 (citing *Anderson v. United States*, 318 U.S. 350 (1943)). Such a situation may arise "if state or local authorities, acting in collusion with federal officers, were to arrest and detain someone in order to allow the federal agents to interrogate him in violation of his right to a prompt federal presentment." *Id.* But "routine cooperation between local and federal authorities" does not rise to this standard because "[o]nly by such an interchange of information can society be adequately protected against crime." *Id.* at 360 (internal quotations omitted). We have explained that "[t]he necessary inquiry is whether the cooperation between state and federal officials had as its purpose a mere interchange of information and resources between two legitimate investigations, one state and the other federal, or to permit in-custody investigation and interrogation by federal officials without compliance with Rule 5(a)." *Barnett v. United States*, 384 F.2d 848, 858 (5th Cir. 1967). That purpose is to be "determined objectively from all surrounding circumstances," and neither "[a] high degree of cooperation by state officials in making the subjects available for interrogation by federal officers" nor the fact "that the

individuals were taken into state custody because of information furnished to state officials by federal officers" is conclusive. *Id.* The burden is on the defendant to prove a violation of Rule 5(a). *Id.* at 859.

About eight hours after he was detained, Davis made inculpatory statements admitting to two of the three carjackings. Although he was arrested by state law enforcement officers for state law offenses, he alleges that there was improper collusion between state and federal officials, such that Rule 5(a) and Section 3501(c) make his statements inadmissible. Davis points to federal and state officials working together on the investigation; state law enforcement obtaining federal warrants from a federal judge; Faggert, who led the investigation, working as a state officer and an FBI agent, aware of potential federal prosecution; and the case ultimately proceeding on federal charges instead of state charges. Thus, Davis says that the federal presentment rules apply, that law enforcement violated those rules in obtaining his inculpatory statements, and the statements should therefore be suppressed. We disagree.

The district court adopted the magistrate judge's findings that there was no evidence of improper collusion between federal and local authorities. We cannot say that these findings were clearly erroneous. The magistrate judge found that in 2014 the local authorities began to investigate the robberies and carjackings Davis committed and the FBI did not begin its investigation until three years later. It also found that the testimony established that it was routine for local law enforcement to arrive at crime scenes,

gather evidence, and interview witnesses before involving the FBI, so there was no evidence the FBI initiated the state investigation. Additionally, the magistrate judge noted that Davis was arrested and detained for state offenses at the time he made his inculpatory statements. Thus, the magistrate judge concluded that Davis did not establish that the FBI manipulated its collaborative relationship with local law enforcement, a collusion between local and federal authorities to cause his confession, or that he would not have been arrested had the FBI not assisted the investigation.

On these facts, we agree with the district court that this is an investigation and prosecution where there was "routine cooperation between local and federal authorities" that should be encouraged to "adequately protect[] [society] against crime." *Alvarez-Sanchez*, 511 U.S. at 360. State law enforcement began its investigation into the string of carjackings and robberies three years before any federal involvement. When federal law enforcement did become involved, it was to provide additional resources to supplement the state investigation. True, Faggert played a large role acting both as a state and a federal law enforcement officer. Yet the federal and state authorities maintained different responsibilities throughout the investigation—state authorities focused on responding to the crimes, interviewing witnesses, and developing leads, and federal authorities focused on gathering digital information. Thus, although the federal resources played a key role in Davis's arrest, there is no evidence suggesting that the state would not have pursued Davis but-for the federal investigators' efforts. The record establishes the opposite: Davis was arrested by state

authorities on state warrants for state crimes and held in state custody. That federal authorities could have and did bring federal charges is of no consequence. *See id.* at 358.

Davis has not satisfied his burden to establish that federal and state law enforcement improperly colluded in the investigation. Accordingly, we affirm the district court's denial of his motion to suppress his inculpatory statements made to law enforcement after his arrest.

C.

Finally, we turn to Davis's argument that the district court should have acquitted him of carjacking. A federal carjacking conviction under 18 U.S.C. § 2119 requires the government to prove the defendant "(1) with intent to cause death or serious bodily harm (2) took a motor vehicle (3) that had been transported, shipped or received in interstate or foreign commerce (4) from the person or presence of another (5) by force and violence or intimidation." *United States v. Diaz*, 248 F.3d 1065, 1096 (11th Cir. 2001). Section 2119's intent element is objective: "[t]he intent of the defendant . . . is to be judged objectively from the visible conduct of the actor and what one in the position of the victim might reasonably conclude." *United States v. Guilbert*, 692 F.2d 1340, 1344 (11th Cir. 1982).

Davis says the government did not meet this burden for the three carjacking counts because the evidence does not support the inference that the victims could have reasonably believed Davis would kill or seriously harm them. We disagree. We have held that

Section 2119's intent element is satisfied when the government presents evidence that the defendant put a gun to a victim's face and told the victim to get out of the car, and the victim testified that he feared for his life. *See United States v. Fulford*, 267 F.3d 1241, 1244 (11th Cir. 2001). The government presented similar evidence here for each of the carjackings. During the January 23, 2020, carjacking, Davis gestured towards a gun in his waistband and demanded the vehicle. The victim testified that she believed that if she did not comply, Davis would have shot her. During the October 30, 2020, carjacking, Davis pointed two pistols at the 15-year-old victim's face and demanded the car. The victim's father was at the scene and testified that, if they had not given up the car, Davis probably would have shot his son. During the November 11, 2020, carjacking, Davis pointed a gun at the victim's head and told him, "don't think about it." The victim testified that he thought he would have been shot if he did not comply.

This evidence is sufficient for a reasonable jury to conclude that Davis had the intent to kill or seriously harm each of the victims of the three carjackings.

IV.

The district court is **AFFIRMED**.

JORDAN, Circuit Judge, Concurring:

I join all of the court's opinion except for Part III.A. As to Part III.A, I concur in the judgment. Although I agree that Mr. Davis lacks an enforceable Fourth Amendment expectation of privacy that entitles him to suppression of the evidence at issue, my reasoning differs somewhat from that of the court.

I

Geofence warrants present difficult constitutional issues, as evidenced by the Fourth Circuit's recent 2-1 ruling that such a warrant does not result in a Fourth Amendment search. *See United States v. Chatrie*, No. 22-4489, ___ F. 4th ___, 2024 WL 3335653 (4th Cir. July 9, 2024). If a challenge to a geofence warrant reaches this court in the future, we need to be precise in describing the technology on the ground and the way companies respond.

Let's start with the basics. "A geofence warrant is based on the concept of a selected virtual perimeter along with the traditional notion of a search warrant. It seeks cell phone location information that is stored by third-party companies and identifies everyone at a location (provided that they have a cell phone and it is turned on) during a particular time. In other words, law enforcement officials use a geofence search warrant to target a crime scene instead of a specific suspect, striving to work backwards in the hopes of developing a suspect[.]" Brian L. Owsley, *The Best Offense is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 Hofstra L. Rev. 829, 833 (2022).

A

Geofence warrants served on Google follow a three-step process, but that's only because Google has required law enforcement to follow its own three-step internal procedures. *See United States v. Chatrie*, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022). *See also* Haley Amster & Brett Diehl, *Against Geofences*, 74 Stan. L. Rev. 385, 389 (2022) ("In response to increasing government requests for information, Google has crafted a three-step, self-directed process for law-enforcement officials trying to obtain user data."). A former Google legal specialist explained in the *Chatrie* case that the company "instituted a policy of objecting to any warrant that failed to include deidentification and narrowing measures"—e.g., the company's own three-step process. *See* Declaration of Sarah Rodriguez, D.E. 96-2 at ¶ 5, *United States v. Chatrie*, No. 3:19cr130 (E.D. Va.).

Google's ability to comply with geofence warrants has historically relied on a feature called Location History (LH). Google developed the three-step "narrowing protocol" to comply with geofence warrants reliant on LH data "[i]n light of the significant differences between [cell site location information (CSLI)] and Google LH data"—namely that LH data "can be considerably more precise" than CSLI. *See* Brief for Google LLC as *Amicus Curiae* Supporting Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant, 2019 WL 8227162,

at 15, 17, filed in *United States v. Chatrie*, No. 3:19cr130 (E.D. Va.) (Google *Amicus* Brief).[1]

As described in *Chatrie*, 590 F. Supp. 3d at 914–16, here's how Google's three-step process works. At step one, "law enforcement obtains legal process compelling Google to disclose an anonymized list of all Google user accounts for which there is saved LH information indicating that their mobile devices were present in a defined geographic area during a defined timeframe." Google *Amicus* Brief at 17. Once Google returns the anonymized list, "the government reviews the anonymized production version to identify the anonymized device numbers of interest." *Id.* At step two, law enforcement can compel the company to provide additional information outside the initial search parameters. *See id. See also Chatrie*, 2024 WL *3335653*, at *3 (explaining that at step two, "the original geographical and temporal limits no longer apply," and "for any user identified at [s]tep [o]ne, law enforcement can request information about his movements inside and outside the geofence over a broader period"). At step three, "the government can compel Google to provide account-identifying information for the anonymized device numbers that it determines are relevant to the investigation"—typically, Gmail address and the first and last name provided on the account. *See Google Amicus* Brief at 19.

[1] CSLI is the data that was at issue in *Carpenter v. United States*, 585 U.S. 296 (2018).

B

It may be true, as some noted, that "Google's process has effectively become the current way geofence warrants are carried out." Orin Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at United States v. Chatrie*, The Volokh Conspiracy (Mar. 11, 2022), https://reason.com/volokh/2022/03/11/the-fourth-amendment--and-geofence-warrants-a-critical-look-at-united-states-v-chatrie. But there are at least three reasons why the Google paradigm cannot generally describe how law enforcement authorities will seek, or how judges will word, geofence warrants for other providers or how those other providers will respond to such warrants.

First, we only know how Google processes geofence warrants and how many it receives because Google has chosen to share process details and related data. One recent law review article summarized Google's publicly available data this way:

> According to data released by Google, geofence warrants "recently constitut[ed] more than 25% of all [U.S.] warrants" received by the company. Google disclosed that it received 982 geofence-warrant requests in 2018. . . . In 2019, the number of geofence warrants received by Google increased by a further 755% over the previous year to 8,396.14 In 2020, the last year for which specific statistics are publicly available at the time of writing, Google received 11,554 geofence warrants.

Amster & Diehl, *Against Geofences*, 74 Stan. L. Rev. at 389–90.

There is some data available regarding other companies, but it is marginal. For example, Apple publishes some data on how many geofence warrants it receives, but also states that it "does not have any data to provide" in response to them. *See* Apple *Transparency Report: Government and Private Party Requests, January 1–June 30, 2023* at 17–18 (last accessed Jul. 15, 2024), www.apple.com/legal/transparency/pdf/requests-2023-H1-en.pdf (reporting that Apple received 16 geofence warrant requests in the first half of 2023).

No other company's processes or data is as well-known or well-understood as Google's. We know that companies like Apple, Uber, Lyft, Microsoft, and Yahoo have received geofence warrants, but the details about how they respond are sketchy. *See generally* Emily Brodner, *Navigating the Terrain of Geofence Warrants*, 7 Ariz. L.J. Emerging Tech. 2, 4–5 (2024) (describing what is known about Uber, Lyft, Microsoft, and Yahoo). We also don't know if any federal or state enforcement authorities adhere to any specific protocol(s) when they serve geofence warrants on companies other than Google. In short, we don't have enough information to say that there is a standard or across-the-board paradigm for geofence warrants.

Second, in December of 2023 Google limited its ability to comply with geofence warrants by changing the way location data is stored. *See* Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google: The Keyword (Dec. 12, 2023)

(explaining that Google users' location history data will now be stored on each user's device and, when backed up on the cloud, will be encrypted "so no one can read it, including Google"); *Chatrie*, WL *3335653*, at *43 (Wynn, J., dissenting) ("Ironically, court decisions like this one could also hinder legitimate law enforcement efforts. Shortly after oral arguments in this case, Google—apparently predicting the majority opinion's flawed reading of *Carpenter*—shut down the technology that permits geofence intrusions, thereby reducing the potential for legitimate investigatory uses of this innovative technology, even with a warrant."). But it is unclear whether this change will prevent Google from complying with geofence warrants going forward. *See* Brodner, *Navigating the Terrain of Geofence Warrants*, 7 Ariz. L.J. Emerging Tech. at 3–4 ("Google continues to collect and store substantial amounts of location data through other means and will likely still be able to respond to geofence warrants. For instance, even if Location History is saved on the user's device, Google's privacy policy states: 'Location History doesn't impact how location information is saved or used by Web & App Activity or other Google products, e.g., based on your IP address. You may still have other settings that save location information.' Despite the policy change, Google is likely still equipped to respond to geofence warrants.").

Third, Google's three-step process may guide some geofence responses, but there is no meaningful guarantee that this process will always be followed. Though "all geofence warrants provide a search radius and time period, they otherwise vary greatly." Note, *Geofence Warrants and the Fourth Amendment*, 134

Harv. L. Rev. 2508, 2514 (2021). And even Google noted in its *amicus* brief in *Chatrie* that at step two it may be compelled to provide additional information outside the initial search parameters. *See* Google *Amicus* Brief at 18 ("[L]aw enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request."). Bounds, therefore, are sometimes pushed:

> Some, for example, will expand the search area by asking for devices located "*outside* the search parameters but within a 'margin of error.'" They also vary in the evidence that they request. Some ask for an initial anonymized list of accounts, which law enforcement will whittle down and eventually deanonymize. Others ask for lists of all implicated users, their phone numbers, IP addresses, and more.

Note, *Geofence Warrants*, 134 Harv. L. Rev. at 2514–15. "Google purports to 'always push back on overly broad requests,'" but it is "unclear how Google determines whether a request is 'overly broad.'" *Id.* at 2515 & n.67.[2]

---

[2] In at least one case where a geofence warrant was issued to Google, law enforcement authorities devised a modified two-step process to narrow the list of individuals whose data they would obtain. *See In re Search of Information that is Stored at the Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 87 (D.D.C. 2021) ("[A]ny overbreadth concerns raised by the requested geofence are further addressed by the warrant's two-step search procedure, which ensures identifying information associated with devices found within the geofence will be produced only pursuant to a further directive from the

In sum, geofence warrants do not typically play out in a certain way.

C

The court says that "there is no evidence in the record to support [Mr. Davis'] claim that the geofence warrant required Google to search every existing Google account." But the court is mistaken on this point. As the Fourth Circuit recognized, Google does have to search every one of its accounts in order to comply with a geofence warrant for a particular location during a specific time window. *See Chatrie*, 2024 WL *3335653*, at *2 ("Google does not keep any lists like this on-hand. So it must first comb through its entire Location History repository to identify users who were present in the geofence.").

Indeed, that Google has to look at all of its accounts is a matter of public record—one that Google has explained in detail in court filings. *See* Google *Amicus* Brief at 19 ("Google has no way to identify which of its users were present in the area of interest without searching the LH information stored by *every Google user* who has chosen to store that information with Google.") (emphasis added). *See also* Rodriguez Declaration at ¶ 7 ("Google must conduct the search across *all* LH data to identify users with LH data during the relevant timeframe, and run a computation against every set of stored LH coordinates to determine which records

---

Court."). So even for Google geofence warrants the three-step process is not always followed.

match the geographic parameters in the warrant. Google does not know which users may have such saved LH data before conducting the search and running the computations."). The literature on geofence warrants also demonstrates that Mr. Davis' assertion is correct. *See, e.g.,* Note, *Geofence Warrants*, 134 Harv. L. Rev. at 2515 ("[B]ecause it has no way of knowing which accounts will produce responsive data, Google searches the entirety of Sensorvault, its location history database, to produce an anonymized list of the accounts—along with relevant coordinate, timestamp, and source information—present during the specified timeframe in one or more areas delineated by law enforcement."); Amster & Diehl, *Against Geofences*, 74 Stan. L. Rev. at 401 n.74 ("Geofence warrants do not necessarily limit the data searched to the subset of users actually present in the geofence. Depending on how a corporation indexes data, all accounts may need to be queried to identify records that match the warrant's specified place and time. This is the case for Google, which has stated that its database is structured such that it requires a search of all users to produce the initial data dump.").

Sgt. Faggert, who requested the geofence warrant in this case, seemed to understand the breadth of his requested search. As the magistrate judge explained, "[Sgt.] Faggert testified that this first set of results could have included anyone within the specified geographical coordinates and timeframe who possessed a cellular device enabled with Google's location capabilities." D.E. 138 at 7. Specifically, Sgt. Faggert recognized that "the warrant ask[ed] Google to search its database for users that are identified in that area with the established parameters for information," and agreed

that "the reason a geofence warrant is requested is because law enforcement cannot identify a suspect at the time of the investigation." D.E. 120 at 12.

Finally, the magistrate judge's report, which was adopted by the district court, details the three-step process as it was explained in the warrant. *See* D.E. 138 at 5–6. Step one, mirroring Google's own language, provides that "Google shall query location history data based on the Initial Search Parameters." D.E. 138 at 5. Based on what we know, it is not clear to me how Google could be expected to comply with step one—to find which accounts (and thereby potentially which users) were present within the geofence during the specified time period—without searching all accounts to see which ones fell into the "Initial Search Parameters." After all, Google cannot know, without first reviewing all of its accounts, which ones satisfy the search parameters.

In sum, Mr. Davis is correct in asserting that Google searches all of its accounts in order to respond at step one to a geofence warrant which seeks to learn which users were within a particular geographic location during a specific period of time.

D

The court characterizes the six searched areas as "public locations." I'm not sure this is completely accurate. It is true that there is no evidence in the record that any of Mr. Davis' own private spaces (such as a business or home) was electronically searched, but at least some of the six searched areas included homes and private businesses. Sgt. Faggert acknowledged as much

at the evidentiary hearing on the motion to suppress. *See* D.E. 120 at 22–24 (testifying that homes are present in some of the specified areas). For example, Location 3 covered the following geographic area, which clearly and visibly included houses:

D.E. 131-14 at 3, 7 (warrant requesting a geofence with the initial parameters of the third location as "[b]etween 01/23/2020 at 2106 hours Central Time or 01/24/2020 at 0306 hours UTC and 01/23/2020 at 2146 hours Central Time or 01/24/2020 at 0346 hours UTC located within the geographical region bounded by and within the geographical radius of 100 meters of (32.350394, -86.234718)").

So, though the geofence warrant here may not have implicated Mr. Davis' dwelling—the "first among equals" for purposes

of the Fourth Amendment, *Florida v. Jardines*, 569 U.S. 1, 6 (2013)—the record shows that some people's homes and businesses were within the geographic areas that were the subject of the warrant. I leave for another day the constitutional implications of this reality, but I do not think it is correct to characterize the areas targeted here as purely public. *Cf.* Elizabeth N. Jones, *Crim Pro, Rewired: Why Current Police Practices Require Candor in the Classroom*, 21 Seattle J. Social Justice 541, 562 (2023) ("If one's home is within a police-generated geofence location, can the data from a cell phone inside the house be gathered?").

II

The magistrate judge concluded that Mr. Davis had not shown that "any of his data was in the parameters" of the search undertaken by Google in response to the geofence warrant. *See* D.E. 138 at 19. That statement, however, is only partly correct. Nevertheless, I conclude that the geofence warrant here did not cause an invasion of Mr. Davis' privacy in the Fourth Amendment sense so as to warrant suppression.

A

As a general matter, a defendant seeking to suppress evidence under the Fourth Amendment must show that he had an expectation of privacy in the place searched. *See Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980) ("Petitioner, of course, bears the burden of proving not only that the search of Cox's purse was illegal, but also that he had a legitimate expectation of privacy in that purse."); *United States v. Harris*, 526 F.3d 1334, 1338 (11th Cir. 2008) ("The

accused bears the burden of demonstrating a legitimate expectation of privacy in the area searched."). For Mr. Davis, that required some evidence that he had a Google account such that Google's step one search would have required a review of his account.

In the district court, Mr. Davis claimed that he possessed a Google account, but that assertion was made only in his reply to the government's response to his motion to suppress, *see* D.E. 110 at 1, or by his counsel to the magistrate judge, *see* D.E. 135 at 58, and was not supported by any testimony of his own. "[A]bsent a stipulation or agreement, unsupported factual statements in a memorandum of law do not constitute evidence[.]" *McKenny v. United States*, 973 F.3d 1291, 1302 (11th Cir. 2020). The same goes for counsel's "factual assertions at a . . . hearing." *United States v. Washington*, 714 F.3d 1358, 1361 (11th Cir. 2013).

Mr. Davis did not take the stand at the suppression hearing. And because there was no testimony from him that he had a Google account, the magistrate judge concluded that he did not show "that any of his data was in the parameters of the Google . . . search" or that "a device that was associated with his data was somehow searched or seized." D.E. 138 at 19.

This conclusion, however, was only partially correct. At the suppression hearing, Sgt. Faggert testified that he had requested a search warrant for multiple Gmail accounts belonging to Mr. Davis. *See* D.E. 120 at 46 (testimony); D.E. 131-11 (FBI 302 report explaining that a search warrant was issued for several Gmail accounts). And he confirmed that "Mr. Davis was a Google

subscriber or account holder." D.E. 120 at 46–47. This testimony was sufficient to establish that Mr. Davis had one or more Google accounts and that, as a result, his accounts were reviewed by Google at step one of its response to the geofence warrant. Those accounts, though, were not the subject of Mr. Davis' motion to suppress.

B

Under the exclusionary rule, "evidence seized as the result of an illegal search may not be used by the government in a subsequent criminal prosecution." *United States v. Martin*, 297 F.3d 1308, 1312 (11th Cir. 2002). The evidence that Mr. Davis sought to suppress was not information related to or gleaned from his own Gmail accounts with Google. Instead, Mr. Davis asked the district court to suppress the evidence obtained from Google at step three of the geofence warrant showing that a device with an accessed Gmail account—described as the "Yonna Gmail account—that he was not associated with was located in a sedan that the suspect used to depart the area of a robbery on January 23, 2020. *See* D.E. 138 at 8–9 & n.11.

In order for Mr. Davis to successfully mount a Fourth Amendment challenge based on a protected expectation of privacy, he had to at least show that he owned or used the "Yonna Gmail account" or that he borrowed or used the cellphone which had that account open within the time periods specified in the geofence warrant. *See Rawlings*, 448 U.S. at 104. But Mr. Davis did not testify to either of these matters at the suppression hearing, and

therefore failed to carry his burden on expectation of privacy. *Cf. United States v. Gibson*, 996 F.3d 451, 462 (7th Cir. 2021) (expressing skepticism that the defendants had a Fourth Amendment expectation of privacy given that "[t]here was no evidence . . . that either defendant personally possessed or used the -5822 phone during the 90-day tracking period" or "ever used the phone for personal, rather than commercial, purposes"); *United States v. Beaudion*, 979 F.3d 1092, 1099 (5th Cir. 2020) (explaining a defendant's assertion that he sometimes used his girlfriend's phone for personal activities did not confer a reasonable expectation of privacy when "[t]here [wa]s no indication that [he] ever used or possessed the phone outside of [his girlfriend's] presence"); *United States v. Dore*, 586 F. App'x 42, 46 (2d Cir. 2014) ("As Dore conceded below, he did not submit an affidavit establishing that the cell phones in question belonged to him or that he had a subjective expectation of privacy in them. Nor did Dore assert a privacy interest in the cell phones in some other manner. Consequently, Dore does not have standing to assert Fourth Amendment rights in those phone records.").

The court goes further and says that "[e]ven if a person has a privacy interest in the data on his own phone, he does not have that interest in the data on someone else's phone." I'm not sure this dicta is correct. A person can open up his or her own data (say, for example, a Gmail account or an app) using a cellphone borrowed from someone else, and it seems to me that such a person may maintain an expectation of privacy in the data. In any event, because Mr. Davis presented no evidence suggesting that he used the "Yonna Gmail account" or borrowed the cellphone which had

the account open, there is no need to discuss any other aspects of the privacy question.

C

I have concerns about the lack of particularity in the geofence warrant issued in this case, largely for the reasons set out in *Chatrie*, 590 F. Supp. 3d at 927–36, and in *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 740–56 (N.D. Ill. 2020). I also have concerns about the fact that the geofence warrant that was filed with the clerk of court was not the same version that Sgt. Faggert served on Google. *See* D.E. 138 at 11. But because Mr. Davis lacks a protected expectation of privacy in the "Yonna Gmail account" and in the cellphone which accessed that account, I do not reach these issues.

III

I concur in the judgment as to Part III.A and join the rest of the court's opinion.