

No. 21-752

---

**In the Supreme Court of the United States**

---

*Rex Hammond, PETITIONER, v.*

*United States of America, RESPONDENT.*

---

*ON PETITION FOR A WRIT OF CERTIORARI  
TO THE UNITED STATES COURT OF  
APPEALS FOR THE SEVENTH CIRCUIT*

**James Patterson McBaine Honors  
Moot Court Competition  
2025 Record**

## TABLE OF CONTENTS

1. Record Instructions	Page 3
2. Questions Presented	Page 4
3. <i>United States v. Hammond</i> , 996 F.3d 374 (7th Cir. 2021)	Page 5
4. <i>United States v. Hammond</i> , 2018 WL 5292223 (N.D. Ind. Oct. 24, 2018)	Page 21

## RECORD INSTRUCTIONS

The judicial opinions contained in this packet have been edited for purposes of the 2025 James Patterson McBaine Moot Court Competition. While you may access and read the full opinions online, you need only be familiar with the material contained in the excerpts below. You are not expected to be familiar with or to address the arguments and parts of the case that have been removed.

This packet also includes “Questions Presented” based on the Petitioner’s petition for writ of certiorari. For your brief, you may choose to edit the questions presented as you see fit, though their substance should remain the same. Outside of the material in this packet, you should not attempt to access the underlying briefs or petitions from *these cases or any other related case*, in accordance with the rules of the competition.

## QUESTIONS PRESENTED

1. In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Court held that the government’s use of an individual’s historical “cell site location information” (CSLI) to determine his past movements over a lengthy period of time constitutes a search within the meaning of the Fourth Amendment, requiring a warrant. But the Court expressly left open the question whether a government agent’s use of “real-time CSLI” to track a person in real time likewise constitutes a search. *Id.* at 2220. The question reserved in *Carpenter*—over which lower courts are divided—is the first question presented here: **Whether a government agent’s direction to a wireless carrier to send a signal to a person’s phone, so that the phone reveals the person’s precise location and movements in real time is a search within the meaning of the Fourth Amendment.**
2. In *Illinois v. Krull*, 480 U.S. 340 (1987), the Court held that the good faith exception to the exclusionary rule prevents exclusion when officers have acted “in objectively reasonable reliance on a statute” that was subsequently found unconstitutional. *Id.* at 349. But the Court “decline[d] the State’s invitation to recognize an exception for an officer who erroneously, but in good faith, believes he is acting within the scope of a statute.” *Id.* at 360 n.17. The question reserved in *Krull*—over which lower courts again are divided—is the second question presented here: **Whether a government agent’s good faith but objectively incorrect reading of a statute prevents the exclusion of constitutionally tainted evidence in a criminal trial.**

United States Court of Appeals, Seventh Circuit.

UNITED STATES of America, Plaintiff-Appellee,

v.

Rex HAMMOND, Defendant-Appellant.

No. 19-2357

|  
Argued October 27, 2020

|  
Decided April 26, 2021

|  
Rehearing and Rehearing En Banc Denied August 19, 2021

**Procedural Posture(s):** Appellate Review.

**Opinion:** St. Eve, Circuit Judge:

Over the course of a three-week crime spree in October 2017, Rex Hammond robbed, or attempted to rob, seven stores at gunpoint in Indiana and Michigan. Five of the seven incidents took place in northern Indiana, where the government charged Hammond with five counts of Hobbs Act robbery and several attendant weapons charges. The charges included one count of being a felon in possession of a firearm in violation of 18 U.S.C. § 922(g) and two counts of brandishing a weapon during a crime of violence in violation of 18 U.S.C. § 924(c). A jury convicted Hammond of all charges, and the district court sentenced him to forty-seven years in prison.

Hammond now appeals his conviction and sentence. He argues that the district court should have suppressed certain cell site location information that law enforcement collected to locate him during his robbery spree and to confirm his location on the days of the robberies, based on *Carpenter v. United States*, — U.S. —, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018). We reject this argument and affirm Hammond's conviction and sentence in all respects.

## I. Background

In October 2017, a series of armed robberies plagued northern Indiana and southern Michigan. Each robbery involved a white man wearing a long sleeved, gray t-shirt; a winter hat; a black face mask; clear, plastic gloves; and bright blue tennis shoes. During each incident, the perpetrator walked straight up to the register and demanded that the cashier withdraw cash from the register and put it into a bag that the man provided. Based on the similarities among the robberies, law enforcement suspected that the same perpetrator had committed them. Robberies took place on Friday, October 6 in Logansport, Indiana; Saturday, October 7 in Peru, Indiana; and Monday, October 9 in Auburn, Indiana. On October 10, the

perpetrator attempted two unsuccessful robberies in southern Michigan—one in Portage and one in Kalamazoo.

During the first attempted robbery on October 10, the cashier fled the scene, leaving the suspect to attempt opening the cash register himself. He failed and fled. The perpetrator then attempted a second robbery, this time at a liquor store in the adjoining town of Kalamazoo. This endeavor also ended poorly for the robber. Rather than placing the cash into the robber's bag as directed, the store clerk placed the cash from the register on the counter. This forced the robber to attempt to stuff the cash into the bag and gave the store clerk an opportunity to grab the gun, a desert-sand colored Hi-Point, and swipe it behind the counter. The robber fled without the weapon.

Leaving his weapon behind had two important consequences: First, there was a two-week hiatus between the Kalamazoo attempted robbery and the resumption of the robberies on October 24. In that time, the robber secured a new weapon—a dark colored, .22 caliber revolver. Witnesses prior to the Kalamazoo robbery described the robber's weapon as a “light brown gun.” After October 10, witnesses described the robber's weapon as a “dark revolver.” The robber committed two additional robberies using the dark revolver, on October 25 in Decatur, Indiana and October 27 in Logansport, Indiana. Despite the change in weapon, other similarities with the earlier robberies indicated that the same suspect likely committed the late October robberies.

Second, in addition to forcing the robber to find a new weapon, the Kalamazoo store clerk's quick thinking also gave law enforcement their first substantial clue as to the identity of the robber. By this time, federal and state law enforcement agencies had begun cooperating with each other to investigate the string of incidents. So, on Wednesday, October 25, officers from several jurisdictions met to review surveillance of the robberies, including Agent Andrew Badowski of the Bureau of Alcohol, Tobacco and Firearms (“ATF”); Detective Jacob Quick of the Indiana State Police; Detective Tyler Preston of the Logansport, Indiana police; Detective Stacey Sexton of the Auburn, Indiana police; and Detective Cory Ghiringhelli of the Kalamazoo, Michigan police.

Upon recovery of the desert-sand colored Hi-Point, ATF Agent Badowski traced the weapon to Todd Forsythe, who reported that he had sold the weapon to “Rex.” Forsythe also provided Badowski with the cell phone number that “Rex” used to arrange the gun sale. On Saturday, October 28, Badowski conveyed this information to Detective Quick, who traced the phone number to the defendant, Rex Hammond. Using Indiana DMV records, the officers also confirmed that Hammond's vehicle, a light-colored Chrysler Concorde, matched descriptions of the vehicle used during the robberies and caught on surveillance footage near the scenes of the crimes. Officers also learned that Hammond had several prior convictions in Indiana, including armed robbery.

The parties dispute exactly when officers learned all of this information: Hammond asserts that officers knew that he was the prime suspect by Saturday, October 28 and that officers could have sought a warrant at the time. In contrast, the government emphasizes that while officers suspected Hammond had committed the robberies, they spent the weekend confirming that the evidence linked Hammond to the robberies, including re-interviewing Forsythe on Sunday, October 29. Detective Ghiringhelli testified that “the information identifying our suspect came over the weekend. I believe it came the evening of the 28th,

which was a Saturday. It either came the 28th or 29th. It was that weekend.” Ghiringhelli also testified that he believed that he had probable cause to arrest Hammond by Monday, October 30.

On that Monday, Ghiringhelli submitted an “exigency” request under 18 U.S.C. § 2702(c)(4) to AT&T, requesting cell site location information (“CSLI”) to geolocate Hammond using the cell phone number that Forsythe had provided. In addition to real-time “pings” to nearby cell towers, Ghiringhelli requested Hammond's historical CSLI dating back to the beginning of the robbery spree on October 7. AT&T complied with Ghiringhelli's request. The historical CSLI records confirmed that Hammond's phone was near Portage and Kalamazoo, Michigan on October 10, and AT&T began providing real-time CSLI, consisting of “pings” to Hammond's location roughly every fifteen minutes, commencing at approximately 6 p.m. on October 30.

Using this real-time CSLI, Ghiringhelli directed Detectives Quick and Sexton to Elkhart, Indiana around 7:30 or 8 p.m. on Monday, October 30. The officers could not locate Hammond in Elkhart. Around 11:30 p.m., Hammond's CSLI pinged near the Indiana toll road in South Bend. Following that ping, Quick and Sexton recognized Hammond's light blue Chrysler Concorde in a Quality Inn parking lot in South Bend. Quick ran the license plate and confirmed it belonged to Hammond. The detectives called for backup and began following Hammond when he exited the parking lot after midnight. As Hammond drove south from South Bend toward Marshall County, Detective Quick called the county's sheriff's department, informed the department that he was following an armed robbery suspect, and requested a traffic stop. After apparently realizing that officers were following him, Hammond lost the officers by engaging in evasive driving maneuvers. While waiting on updated CSLI information from Ghiringhelli, Quick and Sexton met with Marshall County Deputy Kerry Brouyette. During this meeting, Brouyette recognized Hammond drive past them, so the officers resumed their pursuit. Brouyette ultimately stopped Hammond's car around 1:23 a.m. for speeding and failing to signal. At the time, Hammond wore a gray t-shirt, a winter hat, and bright blue tennis shoes, matching the description provided by the robbery victims.

After Detective Quick confirmed with Logansport<sup>1</sup> Detective Preston that they should arrest Hammond immediately, the officers ordered Hammond and his passenger, Alexandra Latendresse, out of the vehicle. They arrested Hammond and read him his *Miranda* rights. Hammond told officers that everything in the car belonged to him, and Latendresse told officers that Hammond had told her that they were going to “get[ ] some money.” Detective Quick later sought and obtained a search warrant for Hammond's car, which contained a black .22 caliber revolver, 44 rounds of .22 caliber ammunition, methamphetamine, a white plastic bag, rubber gloves, a cell phone, and a Garmin GPS Unit.

A grand jury indicted Hammond on January 10, 2018 for five counts of Hobbs Act robbery, in violation of 18 U.S.C. § 1951; two counts of brandishing a firearm during a crime of violence, in violation of 18 U.S.C. § 924(c); and one count of being a felon in possession of a firearm, in violation of 18 U.S.C. § 922(g).

Also in January 2018, the government filed an *ex parte* application for a court order for Hammond's historical CSLI. Although the application acknowledged that law enforcement had already obtained “partial phone records” from Hammond's phone, the application did not rely on those records as a basis for granting the application. The magistrate judge found “reasonable grounds to believe that the records

. . . are relevant and material to an ongoing criminal investigation” and ordered AT&T to disclose the historical CSLI records pursuant to 18 U.S.C. § 2703(d). The records confirmed that around the time of each robbery, Hammond's phone connected to AT&T towers near the stores.

Approximately six months after the magistrate judge issued the § 2703(d) order, the Supreme Court held that the collection of historical CSLI over the course of 127 days, without a warrant, was a search in violation of the Fourth Amendment. *Carpenter*, 138 S. Ct. at 2217. As such, *Carpenter* held that the government must “generally” obtain a warrant before obtaining such records. *Id.* at 2222.

Relying substantially on *Carpenter*, Hammond moved the district court in September 2018 to suppress all cell phone data related to Hammond's phone number, the physical evidence recovered from Hammond's car, and the statements made by Hammond and Latendresse during the October 31 traffic stop. After a lengthy suppression hearing, the district court ruled that although the collection of Hammond's CSLI was a search, Detective Ghiringhelli had relied in good faith on the Stored Communications Act in requesting the information from AT&T. In the district court's view, because the Supreme Court had not yet decided *Carpenter* at the time of the search, it was reasonable for Detective Ghiringhelli to rely on the Stored Communications Act's provisions in requesting cell phone data from AT&T.

The government tried Hammond before a jury in April 2019. The government called roughly thirty witnesses over the course of three days; the defense did not call any witnesses and immediately rested. The jury returned a verdict of guilty on all counts after roughly one hour of deliberations.

The district court sentenced Hammond to forty-seven years (564 months) in prison: ten, twelve, fourteen, sixteen, and eighteen years to run concurrently for each of the five Hobbs Act robbery convictions, plus consecutive, mandatory minimum sentences of seven, seven, and fifteen years for the two brandishing-a-weapon counts and felon-in-possession count, respectively. This appeal followed.

## **II. Discussion**

### **A. Suppression of Cell Site Location Information and Resulting Evidence**

Hammond first challenges the district court's denial of his motion to suppress the CSLI obtained from AT&T and the evidence derived from that data, including the physical evidence recovered from his car and his and Latendresse's statements to officers during the traffic stop. Hammond focuses on the Supreme Court's decision in *Carpenter*, which found that the collection of historical CSLI without a warrant constituted a search in violation of the Fourth Amendment. 138 S. Ct. at 2220. Hammond argues that *Carpenter* compels the exclusion of the CSLI collected in this case. In response, the government asserts a litany of reasons why suppression is unwarranted.

The government collected three different types of CSLI<sup>2</sup> from Hammond's phone: (1) the historical CSLI collected by the government under the authority of the magistrate judge's § 2703(d) order, (2) the historical CSLI collected by Ghiringhelli to confirm Hammond's proximity to the Michigan robberies, and (3) the “real time” CSLI collected by Ghiringhelli for several hours to physically locate Hammond in Indiana. Each of these categories requires a separate Fourth Amendment analysis. As we explain below,



we hold that the first category—the historical CSLI collected under the magistrate judge's § 2703(d) order—was a search for Fourth Amendment purposes, but was collected in good faith reliance on § 2703(d) of the Stored Communication Act, which was settled law at the time the government collected the data. As a result, the Fourth Amendment does not require the district court to exclude this evidence from the jury's consideration. The second category of CSLI—the historical CSLI collected by Ghiringhelli—was not introduced at trial nor did it “taint” any other evidence. Accordingly, there is no need to exclude evidence never admitted at trial or used improperly to obtain additional evidence. Finally, the collection of the CSLI in the third category—Hammond's real-time CSLI—was not a search for Fourth Amendment purposes based on the facts of this case. We discuss each of these categories of CSLI below.

## 1. Standard of Review

We review a district court's denial of a motion to suppress “under a ‘dual standard of review’; we review legal conclusions de novo but findings of fact for clear error.” *United States v. Edgeworth*, 889 F.3d 350, 353 (7th Cir. 2018) (quoting *United States v. Tepiew*, 859 F.3d 452, 456 (7th Cir. 2017)). “A factual finding is clearly erroneous only if, after considering all the evidence, we cannot avoid or ignore a definite and firm conviction that a mistake has been made.” *United States v. Thurman*, 889 F.3d 356, 363 (7th Cir. 2018) (quoting *United States v. Burnside*, 588 F.3d 511, 517 (7th Cir. 2009)).

## 2. Analysis

The Fourth Amendment provides: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated[.]” U.S. Const. Amend. IV. “The ‘touchstone’ of the Fourth Amendment analysis is whether a person has a ‘constitutionally protected reasonable expectation of privacy.’” *Henry v. Hulett*, 969 F.3d 769, 776–77 (7th Cir. 2020) (citing *Oliver v. United States*, 466 U.S. 170, 177, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984)); *see also Riley v. California*, 573 U.S. 373, 381, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). As explained in Justice Harlan's concurring opinion in *Katz v. United States*, the Fourth Amendment requires both that the defendant held a subjective expectation of privacy and that “society is prepared to recognize [that expectation] as ‘reasonable.’” *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring)); *see also Byrd v. United States*, — U.S. —, 138 S. Ct. 1518, 1526, 200 L.Ed.2d 805 (2018) (recognizing the primacy and wide acceptance of Justice Harlan's concurrence); *Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (same). “To determine whether someone has a legitimate expectation of privacy, courts must consider (1) whether that person, by his conduct, has exhibited an actual, subjective expectation of privacy and (2) whether his expectation of privacy is one that society is prepared to recognize as reasonable.” *United States v. Sawyer*, 929 F.3d 497, 499 (7th Cir. 2019).

If a defendant has the requisite expectation of privacy, the Fourth Amendment generally requires law enforcement to obtain a warrant before executing a search. *See Riley*, 573 U.S. at 382, 134 S.Ct. 2473. “In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.” *Id.* (citing *Kentucky v. King*, 563 U.S. 452, 459–60, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011)). “One well-recognized exception applies when ‘the exigencies of the situation make the needs of

law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment.” *King*, 563 U.S. at 460, 131 S.Ct. 1849 (quoting *Mincey v. Arizona*, 437 U.S. 385, 394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978)).

The Supreme Court “fashioned the exclusionary rule” to “compel respect for the constitutional guaranty” of freedom from unreasonable searches. *United States v. Martin*, 807 F.3d 842, 846 (7th Cir. 2015) (quoting *Davis v. United States*, 564 U.S. 229, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011)). “The [exclusionary] rule is not a ‘personal constitutional right,’ and its application ‘exact[s] a heavy toll on both the judicial system and society at large,’ as its effect often ‘is to suppress the truth and set the criminal loose in the community without punishment.’” *Id.* (quoting *United States v. Calandra*, 414 U.S. 338, 348, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974); *Davis*, 564 U.S. at 237, 131 S.Ct. 2419). “The exclusionary rule is designed primarily to deter unconstitutional conduct.” *United States v. Curtis*, 901 F.3d 846, 849 (7th Cir. 2018). The exclusionary rule therefore does not apply when law enforcement has relied in good faith on a facially valid warrant, *United States v. Leon*, 468 U.S. 897, 922, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984); a then-valid statute, *Illinois v. Krull*, 480 U.S. 340, 357, 107 S.Ct. 1160, 94 L.Ed.2d 364 (1987); or binding circuit precedent, *Davis*, 564 U.S. at 232, 131 S.Ct. 2419. Succinctly, “[s]uppression of evidence...has always been our last resort.” *Hudson v. Michigan*, 547 U.S. 586, 591, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006).

#### **i. Historical CSLI Obtained Pursuant to § 2703(d) Order**

We first address the government's collection of Hammond's historical CSLI from AT&T pursuant to the § 2703(d) order.

Section 2703 of the Stored Communications Act, entitled “Required disclosure of customer communications or records,” authorizes courts to “order cell-phone providers to disclose non-content information if the government ‘offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought are relevant and material to an ongoing criminal investigation.’” *Curtis*, 901 F.3d at 848 (quoting 18 U.S.C. §§ 2703(c)(1)(B), (d)).

Based on this statutory authority, in January 2018, the government sought a § 2703(d) order from the magistrate judge directing AT&T to release Hammond's historical CSLI to the government. In its application for the order, the government recounted the distinctive details of the five Indiana robberies, Agent Badowski's investigation into the abandoned Hi-Point, the gun-seller's identification of “Rex” and his cell phone number, Hammond's ownership of the phone number, and the similarities in appearance between Hammond's driver's license photo and the images of the suspect from the security footage of the robberies. Based on this evidence, the government represented that “there [were] reasonable grounds to believe that the records . . . are relevant and material to an ongoing criminal investigation.” The magistrate judge agreed and issued the order.

Six months after the magistrate judge issued its order in January 2018, the Supreme Court decided *Carpenter*, which held that the government “must generally obtain a warrant supported by probable cause before acquiring [historical CSLI].” 138 S. Ct. at 2221. Authorization by § 2703(d) is constitutionally insufficient. *Id.* Hammond now seeks to exclude the historical CSLI based on *Carpenter*'s holding.

We addressed this argument in *Curtis*. 901 F.3d at 848. There, the government relied on § 2703(d) to collect the defendant's CSLI for 314 days, before the Supreme Court issued its decision in *Carpenter*. We concluded that the district court properly admitted the CSLI obtained pre-*Carpenter* based on the good faith exception to the warrant requirement. *Id.* (citing *Krull*, 480 U.S. at 349–50, 107 S.Ct. 1160) (holding that the good faith exception announced in *Leon*, 468 U.S. 897, 104 S.Ct. 3405, is “equally applicable” to cases in which law enforcement reasonably relied on a statute authorizing warrantless searches that is later found to violate the Fourth Amendment); *see also United States v. Castro-Aguirre*, 983 F.3d 927, 935 (7th Cir. 2020).

While *Carpenter* now makes clear that law enforcement's reliance on a § 2703(d) order is insufficient to satisfy the Fourth Amendment's warrant requirement for the collection of historical CSLI,<sup>3</sup> our decision in *Curtis* is equally clear that the exclusionary rule does not apply where the government relied in good faith on § 2703(d) prior to *Carpenter*. *Id.* at 848. As a result, “even though it is now established that the Fourth Amendment requires a warrant for the type of cell-phone data present here, exclusion of that information [is] not required because it was collected in good faith” reliance on § 2703(d). *Id.* at 849. As we said in *Castro-Aguirre*, “[w]e are not inclined to revisit *Curtis*,” and Hammond provides no argument to do so. 983 F.3d at 935. Thus, the district court properly admitted the historical CSLI obtained pursuant to the § 2703 order, “because the government, following the procedures set forth in the Act, gathered it in good faith.” *Id.*

Hammond contends that the historical CSLI that Ghiringhelli collected, which we discuss below, tainted the CSLI obtained pursuant to the § 2703(d) order. Hammond is mistaken. Though the government's § 2703(d) application referenced the partial records that the government already possessed due to the detective's investigation, it did not rely on those records. The application merely disclosed that “[p]artial phone records for the target phone were obtained by Kalamazoo, Michigan Department of Public Safety investigators.” The application did not rely on facts discovered due to those records—for example, the application does not represent that those records confirmed Hammond's proximity to any one of the robberies. Indeed, the above quoted sentence could be excised from the application without altering the quantum of evidence before the magistrate judge showing that the historical CSLI was materially related to an ongoing criminal investigation. Accordingly, the historical CSLI obtained by Ghiringhelli did not taint the historical CSLI obtained via the § 2703(d) order. *See Wong Sun v. United States*, 371 U.S. 471, 487, 83 S.Ct. 407, 9 L.Ed.2d 441 (1963) (evidence from an “independent source” need not be excluded).

## **ii. Historical CSLI Requested by Detective Ghiringhelli**

We now turn to the historical CSLI collected by Detective Ghiringhelli. While the prosecutor obtained Hammond's historical CSLI under § 2703(d) of the Stored Communications Act, Detective Ghiringhelli relied on § 2702 of the Act, entitled “Voluntary disclosure of customer communications or records.” Unlike § 2703, § 2702 does not compel telecommunications carriers to provide records to law enforcement. Instead, § 2702 permits carriers to release records to a governmental entity, “if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.” 18 U.S.C. § 2702(c)(4).

Regardless of the differences between §§ 2702 and 2703, any alleged Fourth Amendment violation by Ghiringhelli's request for Hammond's historical CSLI is a violation in want of a remedy. Critically, the historical CSLI requested by Ghiringhelli was never introduced at trial, nor did it bear "fruit." *See Wong Sun*, 371 U.S. at 487, 83 S.Ct. 407. Investigators did not use this subset of historical CSLI to locate Hammond himself or to locate any other evidence used against him. Thus, even if Detective Ghiringhelli violated Hammond's Fourth Amendment rights, the district court could not exclude evidence that was never used or admitted in the first place.

We reiterate that the only historical CSLI introduced at trial was the historical CSLI that the government obtained under the magistrate judge's order, *not* the detective's § 2702 request to AT&T. As explained above, the latter did not taint the former, because the § 2703(d) application did not rely on the records obtained by Detective Ghiringhelli under § 2702 in any substantive way.

In any event, the historical CSLI that the government ultimately introduced at trial was also admissible under the independent source doctrine. "[T]he central question under the independent source doctrine is whether the evidence at issue was obtained by independent legal means." *United States v. Bell*, 925 F.3d 362, 370 (7th Cir. 2019) (quoting *United States v. May*, 214 F.3d 900, 906 (7th Cir. 2000)). Here, the government ultimately obtained Hammond's historical CSLI based on a good faith reliance on § 2703(d), independent from Detective Ghiringhelli's § 2702 request.

### iii. Real-Time CSLI

Finally, we address the CSLI collected by Detective Ghiringhelli in real time, which officers used to physically locate Hammond in Indiana. For the reasons explained below, we agree with the government that the collection of Hammond's real-time CSLI did not constitute a search under the particular circumstances of this case.<sup>4</sup>

The "narrow" *Carpenter* decision did not determine whether the collection of real-time CSLI constitutes a Fourth Amendment search. 138 S. Ct. at 2220. There, the Court explicitly did "not express a view on matters not before [the Court]," including "real-time CSLI." *Id.*; *see also United States v. Green*, 981 F.3d 945, 958 (11th Cir. 2020) ("The question of whether acquiring [real-time tracking data] constitutes a search was unanswered in 2013 and remains unanswered today.") (citing *Carpenter*, 138 S. Ct. at 2217–19, 2221); *United States v. Thompson*, No. 13-40060-10-DDC, 2019 WL 3412304, at \*7 (D. Kan. July 29, 2019) ("And, extending *Carpenter's* holding about the seizure of historical CSLI to the seizure of real-time CSLI is far from clear because *Carpenter* emphasized that historical CSLI allowed the government to learn of a person's whereabouts on a nearly 24-hour, seven-day-a-week basis. Meanwhile, seizing CSLI in real-time only reveals a person's whereabouts at the moment of its seizure." ).<sup>5</sup>

To answer this open question, we turn to the Supreme Court's jurisprudence pre-*Carpenter*. Before the ubiquity of cell phones, the Court held in *United States v. Knotts* that law enforcement agents did not conduct a "search" when they attached a beeper to a drum of chloroform to track the chloroform's (and the defendants') movements. 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983). There, the beeper only tracked the chloroform from its place of purchase in Minnesota (where the manufacturer consented to the installation of the beeper) to a secluded cabin in Wisconsin where the defendants used it to manufacture

illicit drugs. *Id.* at 277–78, 103 S.Ct. 1081. The Court reasoned that the defendant-driver had no reasonable expectation in his privacy while [traveling] on public roads:

A person [traveling] in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the suspect] [traveled] over the public streets he voluntarily conveyed to anyone who wanted to look [at] the fact that he was [traveling] over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

*Id.* at 281–82, 103 S.Ct. 1081.

The Court took up the constitutionality of more modern modes of tracking in *United States v. Jones*. There, the Court decided that law enforcement's attachment of a GPS unit to a suspect's car for twenty-eight days was a Fourth Amendment search. *United States v. Jones*, 565 U.S. 400, 404, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). The majority grounded its analysis in common law trespass doctrine and emphasized that the “[g]overnment physically occupied private property for the purpose of obtaining information.” *Id.*

*Carpenter* then answered a question that *Jones* left open—whether a physical intrusion onto the defendant's property was *necessary*, and not just *sufficient*, to constitute a search. In *Carpenter*, prosecutors sought a § 2703(d) order for the historical CSLI from the cell phones of several suspects in a series of robberies in Michigan and Ohio in 2011. *Carpenter*, 138 S. Ct. at 2212. The § 2703(d) application requested records spanning 127 days, as well as records for some shorter periods of time. *Id.* *Carpenter* moved to suppress this evidence, but the district court and the Court of Appeals for the Sixth Circuit refused because “*Carpenter* lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers.” *Id.* at 2213.

Diverging from the Sixth Circuit's analysis, the *Carpenter* majority held that the third-party disclosure doctrine did not apply to law enforcement's collection of historical CSLI from cell phone carriers.<sup>6</sup> 138 S. Ct. at 2217. The Court refused to extend the third-party disclosure doctrine to the “novel circumstances” presented by the case—namely, the government's harvesting of a “detailed chronicle of a person's physical presence compiled every day [and] every moment, over [potentially] several years.” *Id.* at 2217, 2220.

Rejecting the third-party doctrine in the context of cell phones, the Court reasoned that society simply does not expect that the police would be able to follow an individual's every movement for weeks at a time:

Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so “for any extended period of time was difficult and costly and therefore rarely undertaken.” For that reason, “society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.”

Allowing government access to cell-site records contravenes that expectation . . . . As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not

only his particular movements, but through them his “familial, political, professional, religious, and sexual associations.”

*Carpenter*, 138 S. Ct. at 2217. Accordingly, “[w]hether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, . . . an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.” *Id.* Therefore, “an order issued under Section 2703(d) of the [Stored Communications] Act is not a permissible mechanism for accessing historical cell-site records.” *Id.* at 2221. Instead, the government must obtain a warrant for historical CSLI.

Given that *Carpenter* disclaimed providing any answer to the question before us, we consider whether the facts of this case are more similar to *Carpenter* or to *Knotts*, and importantly, how the principles and expectations that animated those decisions play out in this case. Here, we are persuaded that the unique facts of this case have more in common with *Knotts* than *Carpenter*. And, although *Carpenter* rejected *Knotts*’ reasoning as applied to *historical* CSLI, we agree with the Sixth Circuit that given the opinion’s limited holding, *Carpenter* otherwise “left undisturbed [the Supreme Court’s] holding in *Knotts*[.]” *See United States v. Trice*, 966 F.3d 506, 518 (6th Cir. 2020).

To review a few of the critical facts of this case, recall that Ghiringhelli’s monitoring of Hammond’s location lasted only a matter of hours—from roughly 6 p.m. on October 30 until close to midnight, when officers were able to physically follow Hammond without the aid of the CSLI pings. This is very different from the 127 days of monitoring at issue in *Carpenter* and more similar to the monitoring of the discrete car trip at issue in *Knotts*. Furthermore, Ghiringhelli’s real-time CSLI request only collected location data that Hammond had already exposed to public view while he travelled on public, interstate highways and into parking lots within the public’s view. *See Knotts*, 460 U.S. at 281–82, 103 S.Ct. 1081; *see also Cardwell v. Lewis*, 417 U.S. 583, 590, 94 S.Ct. 2464, 41 L.Ed.2d 325 (1974) (plurality op.) (“A car has little capacity for escaping public scrutiny.”).

Crucially, unlike in *Carpenter*, the record of Hammond’s (and *Knotts*’) movements for a matter of hours on public roads does not provide a “window into [the] person’s life, revealing . . . his familial, political, professional, religious, and sexual associations” to the same, intrusive degree as the collection of historical CSLI. *Carpenter*, 138 S. Ct. at 2217 (internal quotations omitted). Law enforcement used the real-time CSLI to find Hammond’s location in public, not to peer into the intricacies of his private life. The records here and in *Knotts* do not suggest that law enforcement used either the real-time CSLI or the beeper to examine the defendants’ movements inside of a home or other highly protected area. And, Hammond does not argue that he was in private areas during this time period. In *Carpenter*, law enforcement’s surveillance became a “search” because the surveillance followed *Carpenter* long enough to follow him into, and record, his private life. But here, and in *Knotts*, law enforcement only followed Hammond on public roads, for the duration of one car trip. *See also United States v. Skinner*, 690 F.3d 772, 780–81 (6th Cir. 2012) (distinguishing “comprehensive tracking” from the collection of real-time CSLI to merely locate a drug-trafficking suspect) (superseded by statute on other grounds).

The *Carpenter* majority was particularly concerned with the “retrospective quality” of the data that law enforcement collected about *Carpenter*’s movements. *See* 138 S. Ct. at 2218. “[T]he retrospective quality

of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection.” *Id.* The real-time CSLI collected in this case does not have the same “retrospective quality” of the historical CSLI in *Carpenter* and again, is much more akin to the beeper data in *Knotts*. Real-time CSLI collected over the course of several hours simply does not involve the same level of intrusion as the collection of historical CSLI.

Furthermore, one of the aggravating considerations in *Carpenter* was that the historical CSLI contravened society's expectations not only of their own privacy, but also of law enforcement's capabilities. *Carpenter* recognized that “[p]rior to the digital age, law enforcement might have pursued a suspect for a brief stretch[.]” *Id.* at 2217. The collection of historical CSLI in *Carpenter* was different because it would be too costly and difficult to follow a suspect for over four months. *See id.* As a result, “society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.” *Id.* But here, as in *Knotts*, the “government surveillance . . . amounted principally to the following of an automobile on public streets and highways.” *Knotts*, 460 U.S. at 281, 103 S.Ct. 1081. And in this case, society is fully aware that officers may follow and track a suspect's movements for several hours. In sum, law enforcement's ability to locate Hammond on public roads for a six-hour period using real-time CSLI is not inconsistent with society's expectations of privacy from law enforcement's prying eyes. *See Carpenter*, 138 S. Ct. at 2217.

Our conclusion here is buttressed by our decision in *United States v. Patrick*, where we held that the government did not violate the Fourth Amendment when officers used a cell-site simulator<sup>7</sup> to locate a suspect for whom officers had probable cause and two warrants (one for his arrest and one that “authorized [officers] to locate [the defendant] using cell-phone data”). 842 F.3d 540, 542, 545 (7th Cir. 2016). There, the defendant attempted to challenge the “validity of the location-tracking warrant by contending that his person was not contraband or the proceeds of a crime.” *Id.* at 542. But we reasoned that officers “were entitled to arrest him without a warrant of any kind, let alone the two warrants they had . . . [because] probable cause alone is enough for an arrest in a public place.” *Id.* (citing *United States v. Watson*, 423 U.S. 411, 96 S.Ct. 820, 46 L.Ed.2d 598 (1976)).

A person wanted on probable cause (and an arrest warrant) who is taken into custody in a public place, where he had no legitimate expectation of privacy, cannot complain about how the police learned his location. Recall that the cell-site simulator (unlike the GPS device in *Jones*) was not used to generate the probable cause for arrest; probable cause to arrest Patrick predated the effort to locate him . . . . A fugitive cannot be picky about how he is run to ground. So it would be inappropriate to use the exclusionary rule[.]

*Id.* at 545.

While we acknowledge that *Patrick*'s facts and the legal landscape in which it was decided differ from the facts and legal landscape of this case, *Patrick* is still persuasive. Here, the district court found, and we agree, that the law enforcement officers involved in this case collectively had probable cause to arrest Hammond. *See United States v. Smith*, 989 F.3d 575, 582 (7th Cir. 2021) (collective knowledge doctrine “permits a stop at the direction of, or based on information relayed from, another law enforcement

agency”) (citing *United States v. Khan*, 937 F.3d 1042, 1052 (7th Cir. 2019)). “Police officers possess probable cause to arrest when the facts and circumstances within their knowledge and of which they have reasonably trustworthy information are sufficient to warrant a prudent person in believing that the suspect has committed an offense.” *United States v. Haldorson*, 941 F.3d 284, 290–91 (7th Cir. 2019) (quoting *United States v. Howard*, 883 F.3d 703, 707 (7th Cir. 2018)). As summarized by the district court:

Collectively, the officers knew that a white male had committed several armed robberies; that the gun the robber had used in the earlier robberies traced back to a person named “Rex”; that “Rex’s” phone number belonged to Rex Hammond; that Rex Hammond had several previous convictions for armed robberies; that the person described by Rex Hammond’s driver’s license was consistent with the race, height, weight, and build of the robber shown in the various videos; and that a car similar to what the videos suggested was the getaway car in the robberies was registered to Mr. Hammond.

Reviewing the totality of these circumstances, we have no trouble agreeing with the district court that the officers had probable cause to arrest Hammond. *See id.* at 291 (analyzing probable cause under the totality of the circumstances).

Although Ghiringhelli did not seek a warrant, the fact that officers had probable cause to arrest Hammond is still relevant to the question of whether society is prepared to recognize Hammond’s subjective expectation of privacy as “reasonable.” *See Carpenter*, 138 S. Ct. at 2217. We conclude that his expectation of privacy was not reasonable in light of these facts. *Cf. United States v. Riley*, 858 F.3d 1012, 1018 (6th Cir. 2017) (per curiam) (holding that the use of seven hours of GPS location data to locate a suspect for whom a valid search warrant had been issued was not a search “so long as the tracking [did] not reveal movements *within* the home (or hotel room), [did] not cross the sacred threshold of the home.”) (emphasis in original).

It is also critical to acknowledge the stakes of what was essentially a slow-speed car chase here: Officers were pursuing an individual suspected of committing at least five successful armed robberies and two attempted armed robberies within a short period of time. The suspect had thus already committed several, violent felonies and was likely to do so again. Officers had reason to believe he was armed (he was) and likely to attempt another armed robbery (he intended to).<sup>8</sup>

To conclude, we hold that Detective Ghiringhelli did not conduct a Fourth Amendment “search” by requesting the real-time CSLI of a suspect for multiple armed robberies, for whom officers had probable cause, where the officers only collected real-time CSLI for a matter of hours while the suspect travelled on public roadways, and law enforcement limited its use of the CSLI to the purpose of finding the armed suspect who they had reason to believe was likely to engage in another armed robbery. Hammond’s purported, subjective expectation of privacy under these circumstances is not one “that society is prepared to recognize as ‘reasonable.’” *See Katz*, 389 U.S. at 361, 88 S.Ct. 507. We stress that this holding, like that of *Carpenter*, is narrow and limited to the particular facts of this case.

As a result of this conclusion, none of the evidence stemming from Hammond’s October 31 arrest must be suppressed: the collection of his real-time CSLI was not a search; the resulting traffic stop was valid under *Whren v. United States*, 517 U.S. 806, 116 S.Ct. 1769, 135 L.Ed.2d 89 (1996); officers read



Hammond his *Miranda* rights prior to his verbal statements, *Miranda v. Arizona*, 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966); and the physical evidence recovered from the car was discovered pursuant to a valid search warrant, *United States v. Clemens*, 58 F.3d 318, 321 (7th Cir. 1995). Thus, we also find no constitutional infirmity with the officers' actions after they had located Hammond (and Hammond does not identify any such infirmity).

#### **iv. Good Faith Exception**

In the alternative, although we have concluded that the collection of Hammond's real-time CSLI was not a search, we also hold that the evidence collected as a result of his arrest should not be suppressed because law enforcement collected Hammond's real-time CSLI in good faith reliance on 18 U.S.C. § 2702. *See Krull*, 480 U.S. at 357, 107 S.Ct. 1160 (extending *Leon*'s good faith exception to officer's good faith reliance on a then-constitutional statute); *Davis*, 564 U.S. at 232, 131 S.Ct. 2419 (extending good faith exception to reliance on binding circuit precedent). At bottom, "exclusion is not appropriate where 'the police act with an objectively reasonable good-faith belief that their conduct is lawful.'" *United States v. Kienast*, 907 F.3d 522, 527 (7th Cir. 2018), cert. denied, — U.S. —, 139 S. Ct. 1639, 203 L.Ed.2d 902 (2019) (quoting *Davis*, 564 U.S. at 238, 131 S.Ct. 2419 (2011)); *see also United States v. Rainone*, 816 F.3d 490 (7th Cir. 2016).

Section 2702(c)(4) permits telephone carriers to release records to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."

Here, the district court credited Detective Ghiringhelli's testimony that he had a "good faith belief that an emergency was at hand."

The robber thought to be Mr. Hammond had entered several places the public visits to shop and did so with his finger on (or at least adjacent to) the trigger. The timing of the previous robberies supported at least a strong possibility that another robbery would occur soon. Detective Ghiringhelli also was troubled by the video in which the robber set the handgun on the counter to collect money; Detective Ghiringhelli viewed that as unsafe handling of a firearm, which could pose a further risk to the public.

Detective Ghiringhelli believed in good faith that a federal statute allowed him to act as he did, based on what he (and AT&T) believed to be an emergency, rather than obtaining a warrant. Application of an exclusionary rule is unnecessary under those circumstances.

While we review the district court's legal conclusion that Detective Ghiringhelli relied in good faith on § 2702 de novo, we review the district court's factual findings for clear error. *Edgeworth*, 889 F.3d at 353. Given that Detective Ghiringhelli saw the suspect haphazardly handling his weapon, and even had his finger on the trigger of the weapon upon entering the stores he robbed, we cannot conclude that the district court's factual findings regarding a pending emergency—that there was a strong possibility of another robbery and that the detective was alarmed at the suspect's handling of his weapon—were clearly erroneous. *See Thurman*, 889 F.3d at 363.

We also agree with the district court's legal conclusion that Detective Ghiringhelli reasonably relied on § 2702 of the Stored Communications Act in requesting Hammond's real-time CSLI. At the time of the detective's request, *Carpenter* had not yet explained the Supreme Court's concerns regarding the use of historical CSLI, let alone real-time CSLI. Indeed, although we had not yet opined on the issue, both the Eleventh and Fifth Circuits had affirmatively held that defendants did not have a reasonable expectation of privacy in their historical CSLI. *See United States v. Daniels*, 803 F.3d 335, 351 (7th Cir. 2015); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc); *In re United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).

Finally, our conclusion that Detective Ghiringhelli reasonably relied on the statutory authority of § 2702 is further reinforced by our decision in *Patrick*. There, we said that a suspect “wanted on probable cause” could not “complain about how the police learned his location.” 842 F.3d at 545. We further explained that from the defendant's perspective, “it is all the same whether a paid informant, a jilted lover, police with binoculars, a bartender, a member of a rival gang, a spy trailing his car after it left his driveway, *the phone company's cell towers*, or a device pretending to be a cell tower, provided the location information.” *Id.* (emphasis added). Thus, pre-*Carpenter*, it also would have been reasonable for Ghiringhelli to rely on this binding circuit precedent in locating Hammond with his real-time CSLI. *See Davis*, 564 U.S. at 232, 131 S.Ct. 2419.

### **III. Conclusion**

In light of the foregoing, Hammond's conviction and sentence are AFFIRMED.

## Footnotes

- 1 The location of the first and last of the Indiana robberies.
- 2 “CSLI is location information generated by cellular phone providers that indicates which cell tower a particular phone was communicating with when a communication was made.” *United States v. Curtis*, 901 F.3d 846, 847 (7th Cir. 2018) (citation omitted). “Any cell phone with a functioning battery regularly communicates with cell towers. The phone leaves behind a trail” of this data. *United States v. Castro-Aguirre*, 983 F.3d 927, 934 (7th Cir. 2020).
- 3 Although the Supreme Court decided *Carpenter* after the government applied for and received the § 2703(d) order and received Hammond's records, *Carpenter* controls our analysis. See *United States v. Maez*, 960 F.3d 949, 954 (7th Cir. 2020) (“Current law governs our review on direct appeal.”).
- 4 The district court believed that the government had conceded the threshold question that the collection of Hammond's real-time CSLI constituted a search and that *Carpenter* would apply. The district court then denied Hammond's motion to suppress by relying on the good faith exception to the Fourth Amendment's warrant requirement. See *Curtis*, 901 F.3d at 847–48. On appeal, the government clarifies that it did not concede that the Fourth Amendment applies to Hammond's real-time CSLI. To the contrary, in its response to Hammond's motion to suppress, the government “accept[ed] for the sake of argument (without conceding) that real-time data is subject to the same Fourth Amendment protections as historical data.”
- 5 We also have yet to answer this question post-*Carpenter*, or the related question of whether the use of a cell-site simulator to locate a suspect is a search under the Fourth Amendment. See *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (“Questions about whether use of a simulator is a search, . . . have yet to be addressed by any United States court of appeals. We think it best to withhold full analysis until these issues control the outcome of a concrete case.”).
- 6 The third-party disclosure doctrine ordinarily excludes from the Fourth Amendment's protections any information that the defendant has already shared with a third party, because “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 2216 (quoting *Smith v. Maryland*, 442 U.S. 735, 743–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)).
- 7 The Department of Justice Policy Guidance at the time defined a cell-site simulator as follows: A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device. *Patrick*, 842 F.3d at 543 (citing Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015) at 2).

- 8 Recall that Hammond's passenger, Latendresse told officers that Hammond told her that they were “going to get some money.”

2018 WL 5292223

United States District Court, N.D. Indiana, South Bend Division.

UNITED STATES of America

v.

Rex HAMMOND

CAUSE NO. 3:18-CR-5 RLM-MGG

|

Signed 10/24/2018

**OPINION AND ORDER**

Robert L. Miller, Jr., Judge

Defendant Rex Hammond moves to suppress certain evidence in connection to his January 10, 2018 indictment and subsequent arrest. Mr. Hammond is charged with five counts of violating the Hobbs Act, 18 U.S.C. § 1951, two counts of using, carrying and brandishing a firearm during the commission of a crime in violation of 18 U.S.C. § 924(c), and one count of being a convicted felon in possession of a firearm in violation of 18 U.S.C. § 922(g). The indictment alleges that these violations occurred during multiple robberies of Indiana and Michigan gas stations and at least one liquor store. A hearing on Mr. Hammond's motion to suppress was held on October 9, 2018. For the following reasons, the court denies Mr. Hammond's motion

***I. Background***

Between October 6 and 10, 2018, armed robberies were committed at convenience stores in the Indiana towns of Logansport, Peru, and Auburn, and in the Michigan towns of Portage and Kalamazoo. In each instance, the robber had roughly the same build, wore roughly the same clothes, took roughly the same actions, and carried a handgun that was unusual because it was tan. Agent Andrew Badowski of the Bureau of Alcohol, Tobacco and Firearms called a meeting in Coldwater, Michigan of law enforcement officers who were investigating those robberies. After viewing the surveillance videos, the officers concluded that a single robber had committed all of the crimes. They also viewed surveillance videos from nearby businesses and saw what they thought might be the getaway vehicle (a light-colored mid-sized American car) and a person who they thought might have been the robber without his mask. Each of the attending officers resumed their investigations. On the same day as the Coldwater meeting, a convenience store was robbed at gunpoint in Decatur, Indiana; another armed robbery took place two days later at a Logansport liquor store. Those robberies bore the hallmarks of the robberies discussed at the Coldwater law enforcement meeting.

Agent Badowski undertook the tracing of the firearm. During the Kalamazoo robbery, the perpetrator had set the handgun on the counter to collect money, and the cashier knocked the gun onto the cashier side of the counter; the robber fled with the money but without the gun. Agent Badowski traced the gun's serial number to the last federally licensed dealer to have it, and worked from purchaser to purchaser until, on October 28, he spoke with a man who said he had sold the gun to a man he knew only as "Rex" and was

able to provide “Rex's” phone number. Agent Badowski passed that information on to Indiana State Police Detective Jacob Quick the next day, Sunday, October 29.

Detective Quick asked an Auburn police officer to run the number through a program (“Whooster”) to obtain the name identified with it, and learned the number was assigned to a Rex Hammond. Detective Quick accessed motor vehicle records and got copies of Rex Hammond's most recent driver's license, and the registration for a light-colored Chrysler Concorde that the officers thought might have been the getaway car. The photograph, height and weight on Rex Hammond's driver's license was consistent with what the officers had seen in the videos. Detective Quick sent the information around to the other investigators.

Kalamazoo Police Detective Cory Ghiringhelli was one of the investigators who received the information from Detective Quick. On Monday, October 30, Detective Ghiringhelli learned from the internet that Mr. Hammond's phone number was associated with AT&T, so he asked AT&T to “ping” the phone – meaning to identify the phone's location. Detective Ghiringhelli didn't have a warrant, but asked AT&T to provide the pinging service on the basis of an exigency: the robber had been entering places of business with his finger on or just adjacent to the trigger of a handgun, had handled the handgun unsafely in the Kalamazoo robbery when he laid it on the counter, and had committed an armed robbery two days before and two days before that, suggesting the next armed robbery might be imminent. AT&T agreed to provide the service. AT&T started “pinging” Mr. Hammond's phone at about 6:00 p.m. AT&T would report the phone's location every 15 minutes.

Detective Ghiringhelli notified Detective Quick that the “ping” showed Mr. Hammond's phone first in, then moving away from, Elkhart. Detective Quick and Auburn police detective Stacy Sexton set out in separate unmarked vehicles to track Mr. Hammond's phone. After getting to South Bend, they saw Mr. Hammond's car headed southbound and pursued it, radioing for assistance as they did. Given the time of night and the frequency of the robberies, Detective Quick believed that Mr. Hammond was going to commit another one that night. Mr. Hammond turned off the highway in Marshall County (about 35 miles into the pursuit) and Detective Sexton reported that Mr. Hammond had realized he was being followed. Detective Quick radioed other officers that they had lost Mr. Hammond.

Later that evening, Patrolman Ryan Hollopeter of the Marshall County Police reported seeing the car and that he was going to stop it. By the time Detective Quick arrived, Mr. Hammond's car was parked with several Marshall County Police cars behind it. Mr. Hammond was ordered out of the car. Logansport Police Detective Tyler Preston, who had been traveling toward the reported pings arrived, told everyone on the scene that his county's prosecutor had issued an “arrest on sight” order with respect to Mr. Hammond. Mr. Hammond was taken to jail, and Detective Preston arrived the next day with an arrest warrant for Mr. Hammond on the two Logansport robberies.

Police found a gun, masks, grocery bags (the robber had a grocery bag attached to his wrist to collect the money) and other items of evidentiary value.

On January 10, 2018, the United States Attorney's office applied for a warrant under 18 U.S.C. § 2703(d) for phone records from September 6 through October 31, 2017. Magistrate Judge Michael Gotsch Sr. issued the warrant.

## ***II. Discussion***

### **A. Evidence gathered from warrantless search**

Mr. Hammond moved to suppress everything that flows from the “ping” information obtained from AT&T, including the items found in his car after his arrest. He also moved to suppress information acquired through the 2018 warrant for phone records. Mr. Hammond's argument is based on *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018), in which the Supreme Court held that the Fourth Amendment requires a warrant for police to get certain cell phone information. See also *Utah v. Strieff*, 136 S. Ct. 2056 (the Constitution protects against unreasonable searches and seizures). Mr. Hammond contends that the historic data and “ping” information obtained by Detective Ghiringhelli is inadmissible because it violates the constitutional protections guaranteed to him by the Fourth Amendment. Mr. Hammond further argues that searches stemming from the use of this data are “fruit from the poisonous tree” and so should also be suppressed. *Nardone v. United States*, 308 U.S. 338, 341 (1939); *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920).

The government doesn't dispute Mr. Hammond's argument that *Carpenter v. United States* applies to real time or “ping” data, as well as historical data. The government concedes that in light of *Carpenter v. United States*, a search warrant should have been acquired before accessing the “ping” information, but points to *United States v. Curtis*, 901 F.3d 846 (7th Cir. 2018), in which the court of appeals held that a warrantless acquisition of the phone information can be admissible under the “good-faith” exception to the warrant requirement. In *Curtis*, the government conducted a search via court order pursuant to the Stored Communications Act. *United States v. Curtis*, 901 F.3d at 847-848. Detective Ghiringhelli's October 30 request to AT&T for “ping information” was also made pursuant to the Stored Communications Act, specifically 18 U.S.C. § 2702(c)(4):

(c) Exceptions for disclosure of customer records. -- A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2) ) --

\* \* \*

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency . . .

Resolution of this issue is straightforward: if Mr. Hammond's phone data was collected in a good-faith reliance on the Stored Communications Act, the evidence needn't be suppressed. *United States v. Curtis*, 901 F.3d at 847-848. Detective Ghiringhelli requested Mr. Hammond's historical phone data and “ping” information believing that there were exigent circumstances to do so. AT&T, an entity familiar with these types of requests, also made the determination that circumstances warranted the release of the phone data. Detective Ghiringhelli had a good faith belief that an emergency was at hand. The robber thought to be Mr. Hammond had entered several places the public visits to shop and did so with his finger on (or at least adjacent to) the trigger. The timing of the previous robberies supported at least a strong possibility that

another robbery would occur soon. Detective Ghiringhelli also was troubled by the video in which the robber set the handgun on the counter to collect money; Detective Ghiringhelli viewed that as unsafe handling of a firearm, which could pose a further risk to the public.

Mr. Hammond argues that no emergency existed because Detective Ghiringhelli had plenty of time to get a warrant. But a warrant wouldn't have addressed the emergency, because it wouldn't have located Mr. Hammond. Given Detective Ghiringhelli's belief that there was a strong possibility that Mr. Hammond would endanger the public soon by engaging in another armed robbery, finding Mr. Hammond was just as important as arresting him. The information Detective Ghiringhelli acquired from AT&T filled that purpose.

“Whether the exigent circumstances exception justifies warrantless action is judged by an objective standard: we ask whether it was reasonable for the police officers on the scene to believe, considering the circumstances they faced, that there was a compelling need to act and no time to obtain a warrant.” *Sutterfield v. City of Milwaukee*, 751 F.3d 542, 557 (7th Cir. 2014) (citing *Mich. v. Tyler*, 436 U.S. 499, 509 (1978) ). Detective Ghiringhelli reasonably thought that he, other officers, and the public faced a compelling need to act without a warrant. A willingness to use a weapon can be one such circumstance that can compel exigency. *United States v. Daws*, 711 F.3d 725, 728 (citing *Estate of Bing v. City of Whitehall*, 456 F.3d 555, 564 (6th Cir. 2006) ). In *United States v. Daws*, the court found that officers reasonably believed that exigent circumstances existed to obtain a warrantless search when the defendant had committed armed robbery while brandishing a firearm. 711 F.3d at 728. The exigent circumstances exception isn't limited to physical searches; it applies to all types of searches and seizures under the Fourth Amendment, including searches of phone data. *United States v. Banks*, 884 F.3d 998, 1011-1012 (10th Cir. 2018).

Detective Ghiringhelli believed in good faith that a federal statute allowed him to act as he did, based on what he (and AT&T) believed to be an emergency, rather than obtaining a warrant. Application of an exclusionary rule is unnecessary under those circumstances. See *United States v. Curtis*, 901 F.3d at 849. Accordingly, the court needn't address the parties' arguments about whether the eventual stop of Mr. Hammond's car was sufficiently attenuated from the unconstitutional use of the “ping” information; because of the good faith exception to the warrant requirement, the “ping” information wasn't illegally obtained.

### **C. The Government's 18 U.S.C. § 2703(d) warrant**

Mr. Hammond also contends that the government's application for the January search warrant under 18 U.S.C. § 2703(d) was defective, but he bases that argument on the application's having contained information the government obtained through the “ping” request. Because there was nothing unlawful about the “ping” request, Mr. Hammond's challenge to the January warrant can't succeed, either.

### ***III. Conclusion***

For the reasons stated above, the court DENIES Mr. Hammond's motion to suppress. [Doc. No. 30].  
SO ORDERED.



