UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	18 CR 185-1
	)	
vs.	)	Judge Gary Feinerman
	)	
TOBIAS DIGGS, MARVON HAMBERLIN, and JOSHUA McCLELLAN,	)	
	)	
	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

Tobias Diggs, Marvon Hamberlin, and Joshua McClellan are charged under the Hobbs Act, 18 U.S.C. § 1951(a), for the robbery of a Razny Jewelers store in Hinsdale, Illinois on March 17, 2017. Doc. 1. While investigating the robbery, a Hinsdale detective obtained from a third party—without a warrant—more than a month's worth of Global Positioning System ("GPS") location data for a vehicle associated with Diggs. Doc. 56-1 at 2-5. Diggs moves to suppress the GPS evidence. Doc. 49. The motion is granted.

Background

Because there are no "disputed issues of material fact that will affect the outcome" of Diggs's motion, an evidentiary hearing is not required. *United States v. Edgeworth*, 889 F.3d 350, 353 (7th Cir. 2018) (internal quotation marks omitted). The undisputed facts, drawn primarily from police reports and search warrant applications, are as follows.

While investigating the Razny Jewelers robbery, Hinsdale detectives came to believe—based on witness statements, video surveillance, and an anonymous tip relayed by another law enforcement officer—that the getaway vehicle was a 2003 Lexus RX with Michigan license plate number DPA 8960. Doc. 50-1 at 4-5; Doc. 56-1 at 2-4. The Lexus was registered to

Diggs's wife, Devinn Adams. Doc. 49 at 1; Doc. 50-1 at 5. Adams bought the car on credit from Headers Car Care in July 2016. Doc. 55-1 at 2. Her contract with Headers includes this provision: "If your vehicle has an electronic tracking device, you agree that we may use this device to find the vehicle." *Id*. at 4. Although Adams owned the Lexus, Diggs "regularly drove" it. Doc. 55 at 4.

On March 29, 2017, Hinsdale detectives issued an alert "on multiple databases" seeking information about the Lexus. *Id*. at 3. On April 4, 2017, a Headers employee told one of the detectives that the Lexus was equipped with a GPS tracking device serviced by Air Assault Asset Track GPS Systems. Doc. 49-1 at 3-4; Doc. 56-1 at 2-3. The Headers employee gave the detective her login credentials for Air Assault's website and authorized him to access "all the GPS records associated with the Devinn Adams/Lexus RX account." Doc. 56-1 at 3. The GPS records included historical data tracking the Lexus's "movement and global position." *Ibid*.

Without first obtaining a warrant, the detective downloaded a spreadsheet containing GPS data for the period from March 1, 2017 through April 4, 2017. *Ibid*.; Doc. 49-1 at 6, 8, 10. The spreadsheet sets forth time-stamped entries giving the Lexus's approximate street address (usually at the block level, such as "5701-5799 S Campbell Ave, Chicago, IL, 60629") each time it was turned on, approximately every five minutes while it was being driven, and each time it was parked. Doc. 56-1 at 3-4; Doc. 49-1 at 8. According to the detective, "[g]reater detail" beyond those approximate street addresses "c[ould] be extracted from the map points" using "the software program that manages the GPS data," which allowed the detective to "narrow[]" each recorded location "to specific latitude and longitude way points." Doc. 56-1 at 3.

The GPS data reflect that the Lexus traveled to Hinsdale on the date of the robbery, March 17, 2017, and on each of the two previous days. *Id*. at 3. The data also reflect that the

Lexus traveled to and from all three defendants' "family residence[s]" from March 15 through March 17. *Id*. at 4 (capitalization altered). The March 17 data show the Lexus driving from Diggs's address to McClellan's, then to Hamberlin's, then to Hinsdale, and then back to Hamberlin's. *Id*. at 3-5. The data place the Lexus on the same block as Razny Jewelers at the time of the robbery, and in the alleyway "directly behind" the store during the robbery. *Id*. at 5. Later on March 17, the Lexus was parked in the garage at Diggs's girlfriend Jessica Christian's mother's home, where it remained until the police seized it on April 4. *Id*. at 3; Doc. 49-1 at 4.

Discussion

Diggs argues that the Hinsdale police's warrantless acquisition of the Lexus's long-term historical GPS data was an unreasonable search in violation of the Fourth Amendment as interpreted by *United States v. Jones*, 565 U.S. 400 (2012), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018). Doc. 49 at 1-4; Doc. 56 at 4-10. The government responds that acquiring the data was not a Fourth Amendment search because: (1) unlike in *Jones*, the police made no physical intrusion on the Lexus, Doc. 55 at 10-12; and (2) under the third-party doctrine, Diggs lacked a reasonable expectation of privacy in the data because he voluntarily provided it to the third party (Headers) from which the police obtained it, *id*. at 5-10. The government submits in the alternative that even if the Hinsdale police violated the Fourth Amendment, the good-faith exception to the exclusionary rule applies because the police adhered to binding appellate precedent in obtaining the data. Doc. 62 at 1-5.

I. Whether Law Enforcement's Acquisition of the GPS Data Violated the Fourth Amendment

The Fourth Amendment prohibits "unreasonable searches." U.S. Const. amend. IV. To determine whether that prohibition has been violated, the court must "ask[] two questions: first, has there been a search … , and second, was it reasonable?" *United States v. Correa*, 908 F.3d

208, 217 (7th Cir. 2018); *see also Carpenter*, 138 S. Ct. at 2215 n.2 (cautioning against "conflat[ing] the threshold question whether a 'search' has occurred with the separate matter of whether the search was reasonable"). The parties dispute only the first question.

"The Supreme Court uses two analytical approaches to decide whether a search has occurred. One is the property-based or trespass approach. The other is based on expectations of privacy." *Correa*, 908 F.3d at 217 (citations omitted); *see also United States v. Thompson*, 811 F.3d 944, 948 (7th Cir. 2016) ("A search occurs either when the government physically intrudes without consent upon a constitutionally protected area in order to obtain information or when an expectation of privacy that society is prepared to consider reasonable is infringed.") (citation and internal quotation marks omitted). "The two approaches work together" in that "'property concepts' are instructive in 'determining the presence or absence of [protected] privacy interests.'" *Correa*, 908 F.3d at 217 (quoting *Byrd v. United States*, 138 S. Ct. 1518, 1526 (2018)). Diggs invokes only the privacy-based approach, arguing that he had a reasonable expectation of privacy in his movements, as chronicled by a month's worth of GPS data tracking the vehicle he was driving. Doc. 49 at 3-4; Doc. 56 at 4-5. Under the principles set forth in *Jones* and *Carpenter*, Diggs is correct.

In *Jones*, the government attached a GPS tracking device to a target's vehicle and used it to monitor the vehicle's movements over a 28-day period. 565 U.S. 400, 403-04. The Supreme Court unanimously held that a search occurred, but split evenly as to why. The five-Justice majority held that the government conducted a search by "physically occup[ying] private property for the purpose of obtaining information." *Id*. at 404-05. In a concurrence joined by three other Justices, Justice Alito rejected the majority's "trespass-based theory," concluding instead that "the use of longer term GPS monitoring in investigations of most offenses" is a

search because it "impinges on expectations of privacy" to a "degree … that a reasonable person would not have anticipated." *Id*. at 419-21, 424, 430 (Alito, J., concurring in the judgment). Justice Sotomayor adopted both theories, joining the majority in holding that "[w]hen the Government physically invades personal property to gather information, a search occurs," while agreeing with Justice Alito that long-term GPS monitoring implicates privacy concerns by "enabl[ing] the Government to ascertain, more or less at will, [individuals'] political and religious beliefs, sexual habits, and so on." *Id*. at 414-16 (Sotomayor, J., concurring). Thus, as the Court recognized in *Carpenter*, although *Jones* was formally resolved under the property-based approach, "[a] majority of [the] Court [in *Jones*] … recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements." *Carpenter*, 138 S. Ct. at 2217; *see also United States v. Caira*, 833 F.3d 803, 808 (7th Cir. 2016) ("Traditionally, a person had no reasonable expectation of privacy in his movements on public streets, so it would not be a 'search' if officers watched him. But two concurring opinions [in *Jones*], signed by five Justices total, expressed the view that technology has changed the constitutional calculus by dramatically increasing the amount and precision of data that the government can easily collect.") (citation omitted).

The GPS data at issue here fits squarely within the scope of the reasonable expectation of privacy identified by the *Jones* concurrences and reaffirmed in *Carpenter*. The GPS data provide "a precise, comprehensive record of [Diggs's] public movements" over the course of a month. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *see also id*. at 430 (Alito, J., concurring in the judgment) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."). Moreover, "the retrospective quality of the data here" impinges even further on privacy

concerns than did the live data in *Jones* because it "gives police access to a category of information otherwise unknowable" by enabling the police to "travel back in time to retrace [Diggs's] whereabouts, subject only to the retention polic[i]es" of Headers and Air Assault. *Carpenter*, 138 S. Ct. at 2218. Thus, while the law enforcement tactic employed in *Jones*—attaching a GPS tracking device to a vehicle—required the police to "know in advance [that] they want to follow a particular individual," the tactic employed here—accessing a historical database of GPS information—means that "[w]hoever the suspect turns out to be, he has effectively been tailed" for the entire period covered by the database. *Ibid*.

True enough, the facts in *Jones* differ slightly from the facts here, as the defendant in *Jones* "was the exclusive driver" (but perhaps not the owner) of the tracked vehicle, 565 U.S. at 404 n.2 (internal quotation marks omitted), while Diggs "regularly drove the Lexus" but did not own it and was not its only driver, Doc. 55 at 4; *see* Doc. 56-1 at 3 (noting that surveillance video indicates that Christian drove the Lexus on at least one occasion). But the government does not argue that the possibility that some of the GPS data here reflected other persons' movements reduces the robustness of the resulting record of Diggs's movements to the point where he lacks a reasonable expectation of privacy in that record as a whole. Any such argument is therefore forfeited. *See United States v. Stanbridge*, 813 F.3d 1032, 1038 (7th Cir. 2016) (holding that the government forfeited an argument against suppression by failing to make it in the district court); *Nichols v. Mich. City Plant Planning Dep't*, 755 F.3d 594, 600 (7th Cir. 2014) ("The non-moving party waives any arguments that were not raised in [a] response … ."); *Alioto v. Town of Lisbon*, 651 F.3d 715, 721 (7th Cir. 2011) ("We apply [the forfeiture] rule where a party fails to develop arguments related to a discrete issue … ."). In any event, given the duration and level of detail of the GPS data, the possibility that some of the data does not reflect

Diggs's movements does not push the government's acquisition of the data back over the line at which it became a search. *Cf. Carpenter,* 138 S. Ct. at 2217 n.3 (holding that "accessing seven days of [cell-site location information] constitutes a Fourth Amendment search," and declining to decide whether there is some shorter period for which obtaining the data would not be a search).

Invoking the third-party doctrine, the government next argues that Diggs gave up any reasonable expectation of privacy in his physical movements as revealed by the GPS data because the Lexus's owner (Adams) voluntarily turned over the data to a third party (Headers), which in turn gave the data to the police. Doc. 55 at 5-10. The third-party doctrine arises from *Smith v. Maryland*, 442 U.S. 735 (1979), where the government used a pen register to record outgoing phone numbers dialed on a landline, and *United States v. Miller*, 425 U.S. 435 (1976), where the government subpoenaed the defendant's bank records. *See Carpenter*, 138 S. Ct. at 2216 (explaining the doctrine's origins). As the Court observed some forty years later in *Carpenter*, *Smith* and *Miller* "held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties[,] … even if the information is revealed on the assumption that it will be used only for a limited purpose." *Ibid*. (internal quotation marks omitted). *Carpenter* explained, however, that *Smith* and *Miller* did not erect a bright-line rule: "The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Id*. at 2219. Thus, even where an individual voluntarily provides information to a third party, courts must "consider[] the nature of the particular documents sought to determine whether there is a legitimate expectation of privacy concerning their contents." *Ibid*. (internal quotation marks omitted).

Carpenter defeats the government's third-party argument here. *Carpenter* held that obtaining historical cell-site location information ("CSLI")—time-stamped records of a cell phone's connection to a cell tower—from a third party (a wireless carrier) was a search because it intruded on the target's "legitimate expectation of privacy in the record of his physical movements as captured through CSLI." 138 S. Ct. at 2211-12, 2217. The Court rejected the government's characterization of its acquisition of historical CSLI as "a garden-variety request for information from a third-party witness," reasoning that "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller*"—telephone numbers and bank records—"and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id*. at 2216-19. Given the heightened privacy concerns at play, the Court "decline[d] to extend *Smith* and *Miller* to the collection of CSLI." *Id*. at 2219-20.

Applying the third-party doctrine to the GPS data here would require essentially the same extension of the doctrine that the Court rejected in *Carpenter*. *Carpenter* understood CSLI to present "many of the qualities of the GPS monitoring … considered in *Jones*"—both are "detailed, encyclopedic, and effortlessly compiled"; both "provide[] an intimate window into a person's life"; and, in the context of historical information, both provide a "tracking capacity [that] runs against everyone" without any need for the police to "know in advance whether they want to follow a particular individual, or when." *Id*. at 2216-18. Indeed, at the time of the search in *Carpenter*, CSLI was still "less precise than GPS information." *Id*. at 2218-19. Accordingly, *Carpenter* compels the conclusion that, given the privacy concerns implicated by the "detailed and comprehensive record of [Diggs's] movements" captured by the Lexus's GPS tracker, "the fact that the [police] obtained the information from a third party does not overcome [Diggs's] claim to Fourth Amendment protection." *Id*. at 2217, 2220.

The government next argues that Diggs relinquished any reasonable expectation of privacy in the GPS data when he abandoned the Lexus in someone else's garage. Doc. 55 at 12-14. That argument rests on a misunderstanding of the privacy interests at play. Obtaining the GPS data implicated Diggs's privacy interest in the historical record of his location—as revealed by the Lexus's movements—over the month before he allegedly abandoned the Lexus. *See Carpenter*, 138 S. Ct. at 2217 (characterizing the relevant privacy interest as "a legitimate expectation of privacy in the record of [the target's] physical movements as captured through CSLI"). The government's argument regarding Diggs's abandonment of the Lexus, by contrast, addresses only his privacy interest (or lack thereof) in the Lexus itself. Doc. 55 at 12-14.

That distinction is crucial. If Diggs lacked a Fourth Amendment interest in the Lexus on April 4, 2017, the police could have searched the vehicle without implicating his Fourth Amendment rights. *See Byrd*, 138 S. Ct. at 1530 ("[A] person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search … ."). But it would not follow that Diggs lacked a Fourth Amendment interest in the GPS data the Lexus transmitted to Air Assault before he abandoned the vehicle. Diggs's reasonable expectation of privacy in the GPS data arises from the story that data tells about his movements over the course of a month, not from any expectation of privacy in the vehicle's interior after he left it in someone else's garage. As Diggs observes, if a person who abandoned the physical object that created a set of data—but that did not itself hold the data—also abandoned his privacy interests in that data, then anyone who trades in his cell phone for a newer model would lose his privacy interests in the CSLI his wireless carrier had collected from the old device. Doc. 56 at 12-13. That is not how the Fourth Amendment works; rather, the reasonable expectation of privacy inquiry arises from the information that was searched. *See Carpenter*,

138 S. Ct. at 2219 ("[W]hen the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy *in the whole of his physical movements*.") (emphasis added); *United States v. Alexander*, 573 F.3d 465, 472 (7th Cir. 2009) ("A person cannot have a reasonable expectation of privacy in abandoned property … . To demonstrate the abandonment, the government must prove … that the defendant relinquished his property interests in *the item to be searched*.") (emphasis added) (internal quotation marks omitted).

Finally, the government says in a footnote that "[i]t is not clear that [Diggs] actually" "has sufficient standing with respect to the Lexus to bring a Fourth Amendment claim related to it." Doc. 55 at 5 n.3. Because the government takes no clear position, addresses the issue only in a footnote, and cites no authority for the proposition that a person who "regularly drove" the Lexus, *id*. at 4, has no reasonable expectation of privacy in his location as revealed by long-term historical GPS data reflecting the vehicle's movements simply because he "lacked a sufficient possessory interest in the Lexus," *id*. at 5 n.3, the issue is forfeited. *See Evergreen Square of Cudahy v. Wis. Housing & Econ. Dev. Auth.*, 848 F.3d 822, 829 (7th Cir. 2017) ("A party may waive an argument by presenting it only in an undeveloped footnote."); *M.G. Skinner & Assocs. Ins. Agency v. Norman-Spencer Agency, Inc.*, 845 F.3d 313, 321 (7th Cir. 2017) ("Perfunctory and undeveloped arguments are waived, as are arguments unsupported by legal authority.").

Even setting aside forfeiture, any challenge to Diggs's Fourth Amendment "standing" would fail on the merits. Fourth Amendment "standing" is merely a "shorthand for … the idea that a person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search," and thus is "not distinct from the merits and is more properly subsumed under substantive Fourth Amendment doctrine." *Byrd*, 138 S. Ct. at 1530 (internal quotation marks omitted). Because, as shown above, Diggs had a reasonable

expectation of privacy in the GPS data, he had "a cognizable Fourth Amendment interest" in that data and accordingly may seek relief for law enforcement's intrusion on that interest. *Ibid*. Diggs need not also establish a property interest in the vehicle itself. *See id*. at 1526 ("Expectations of privacy protected by the Fourth Amendment … need not be based on a common-law interest in real or personal property, or on the invasion of such an interest.") (internal quotation marks omitted).

Accordingly, the government's warrantless acquisition of historical GPS data revealing Diggs's movements over the course of more than a month was a search. The next question is whether the search was reasonable. It was not. As the Court explained in *Carpenter*, "warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing. Thus, in the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." 138 S. Ct. at 2221 (alteration, citation, and internal quotation marks omitted) (holding that a warrantless search of CSLI records was unreasonable); *see also United States v. Brewer*, 915 F.3d 408, 413 (7th Cir. 2019) ("GPS vehicle monitoring generally requires a warrant … ."). The government does not argue that any exception to the warrant requirement applies here, thus forfeiting the point. *See Stanbridge*, 813 F.3d at 1038; *Nichols*, 755 F.3d at 600; *Alioto*, 651 F.3d at 721. The search accordingly violated the Fourth Amendment. *See Carpenter*, 138 S. Ct. at 2221.

II. Whether the Good-Faith Exception to the Exclusionary Rule Applies

The government next argues that the good-faith exception to the exclusionary rule applies to its search of the GPS data because an objectively reasonable officer could have conducted the search in reliance on pre-*Carpenter* "case law regarding the third-party doctrine." Doc. 62 at 1-5. The government invokes the version of the good-faith exception applied in *Davis v. United*

States, 564 U.S. 229 (2011), which held that "when the police conduct a search in objectively reasonable reliance on binding appellate precedent, the exclusionary rule does not apply." *Id*. at 249-50. Diggs responds that the government has not identified any precedent that qualifies as binding appellate precedent under *Davis*. Doc. 63 at 9-13.

The *Davis* good-faith exception applies only "when 'binding appellate precedent specifically *authorizes* a particular police practice.'" *United States v. Jenkins*, 850 F.3d 912, 918 (7th Cir. 2017) (quoting *Davis*, 564 U.S. at 241). The reasoning behind the exception is this: Because the exclusionary rule is a deterrence mechanism rather than "a personal constitutional right," there is nothing to deter—and thus no basis for suppression—when officers conducting a search "scrupulously adhere[] to governing law" that "is later overruled." *Davis*, 564 U.S. at 232, 248-49 (internal quotation marks omitted); *see also id*. at 241 (noting that "well-trained officers will and should use [a] tool" specifically authorized by binding appellate precedent). As the Seventh Circuit has held, that reasoning does not "reach so far as to excuse mistaken efforts to *extend* controlling precedents." *Jenkins*, 850 F.3d at 920 (internal quotation marks omitted). Illustrating the point, the Seventh Circuit held in *Jenkins* that binding appellate precedent recognizing "a categorical rule that permitted the police to conduct a search of a person incident to a lawful arrest"—and even applying that rule to "the search of a vehicle's compartments and any containers therein" when "the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search"—did *not* specifically authorize a warrantless search of a cell phone found during a search of the defendant's vehicle conducted while he was standing at the front of an officer's squad car. *Id*. at 916, 918-20. Likewise, in *United States v. Whitaker*, 820 F.3d 849 (7th Cir. 2016), the Seventh Circuit held that *Davis* did not apply where, although "there was no recognized expectation of privacy in the common areas of a multi-unit

apartment building" at the time of the search, "no appellate decision specifically authorize[d] the use of a super-sensitive instrument, a drug-detecting dog, by the police outside an apartment door to investigate the inside of the apartment without a warrant." *Id*. at 854-55; *cf. United States v. Velazquez*, 906 F.3d 554, 555-56, 560-61 (7th Cir. 2018) (holding that *Davis* applied where the police, acting with probable cause but without a warrant, brought a drug-sniffing dog onto the defendant's driveway to sniff a vehicle and then-controlling circuit precedent "permitted the warrantless search of a vehicle parked close to a house on the defendant's private driveway so long as there was probable cause to believe that the search would uncover contraband or evidence of a crime").

The government argues that binding appellate precedent authorized the search here because as of April 4, 2017, the date the police downloaded the GPS data, "a number of courts had held that defendants did not have a reasonable expectation of privacy in location information … maintained by a third party," and the Seventh Circuit had held that the third-party doctrine survived *Jones*. Doc. 62 at 1-3. The government points to three appellate cases: the Seventh Circuit's 2016 decision in *United States v. Caira*, *supra*; the Fourth Circuit's decision in *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc), *abrogated by Carpenter*, 138 S. Ct. 2206; and the Sixth Circuit's decision in *Carpenter* itself, *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206.

In *Caira*, the Seventh Circuit characterized the third-party doctrine as "a bright-line application of the reasonable-expectation-of-privacy test," explaining that *Smith* and *Miller* "held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties[,] even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 833 F.3d at

806 (alteration and internal quotation marks omitted). Given *Caira*'s understanding of *Smith* and *Miller*, a reasonable officer at the time of the search here might not have anticipated that the Supreme Court a year later in *Carpenter* would hold that permitting the warrantless collection of CSLI from a third party would represent not "a straightforward *application* of the third-party doctrine, but instead a significant *extension* of it to a distinct category of information." 138 S. Ct. at 2219 (emphasis added). Even so, Diggs argues that given *Carpenter*'s narrow view of the third-party doctrine's reach, the mere recitation of the doctrine in pre-*Carpenter* cases like *Caira* did not specifically authorize its application to GPS data. Doc. 63 at 9-13. Diggs is correct.

This court must take the Supreme Court at its word as to the third-party doctrine's pre-*Carpenter* reach. *See Mathis v. United States*, 136 S. Ct. 2243, 2254 (2016) ("[A] good rule of thumb for reading [Supreme Court] decisions is that what they say and what they mean are one and the same … ."). The Supreme Court could have described what it was doing in *Carpenter*, not as declining to extend the third-party doctrine to a context not addressed in *Smith* and *Miller*, but as partially scaling back the once-categorical doctrine to account for "the seismic shifts in digital technology" that gave rise to widespread, long-term location tracking. 138 S. Ct. at 2219. Had it done so, the *Davis* good-faith exception might very well have applied here. *See United States v. Gary*, 790 F.3d 704, 709-10 (7th Cir. 2015) (holding that cases setting out a "categorical rule allowing the police to conduct a search of a person incident to a lawful arrest" amounted to binding appellate precedent specifically authorizing a warrantless search of a cell phone discovered on an arrestee's person, reasoning that "even the *Riley* Court recognized that its holding … excepting cell phones from [the] categorical rule … was a novel approach" and that Seventh Circuit precedent at the time of the search "had refused to differentiate between physical items and digital data in searches incident to arrest"). But instead, the Court said that the third-

party doctrine was *never* broad enough to encompass technology-enabled long-term location tracking in the first place. *See Carpenter*, 138 S. Ct. at 2219; *cf.* Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, Lawfare (updated June 22, 2018, 4:56 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision ("The old understanding was that the third-party doctrine is a bright-line rule … . Part of the [Court's] thinking … is an adoption of Carpenter's rhetoric in his brief that the third-party doctrine only 'diminishes' an expectation of privacy. That's not what the cases say; the cases say that the doctrine entirely eliminates an expectation of privacy.").

Although *Carpenter* post-dates the GPS search here, it is just as controlling as to what the third-party doctrine authorized at the time of the search as it is on the doctrine's scope going forward. In the qualified immunity context, lower courts are bound by Supreme Court decisions addressing what was or was not clearly established at some prior point in time. *See Kisela v. Hughes*, 138 S. Ct. 1148, 1154 (2018) (explaining that the court of appeals erred in holding that a circuit decision defeated qualified immunity where the Supreme Court "ha[d] already instructed the Court of Appeals not to read [that] decision … too broadly in deciding whether a new set of facts is governed by clearly established law"). So, too, for the *Davis* good-faith exception, which likewise turns on the state of the law at some point in the past. *See Jenkins*, 850 F.3d at 918-19 (examining a 2015 Seventh Circuit decision addressing the state of the law in 2009 to determine whether binding appellate precedent had authorized a search conducted in 2012). *Carpenter* thus teaches that general statements of the third-party doctrine uttered in pre-*Carpenter* decisions not only do not cover CSLI, but never did. And as noted above, what *Carpenter* said about the third-party doctrine as to CSLI applies with full force to GPS data. It follows that for the *Davis* good-faith exception to apply to the GPS search here, the government needs more than general

statements of the third-party doctrine in a binding appellate decision issued before the search; rather, the government must point to binding appellate precedent applying the doctrine to long-term historical GPS data or its equivalent.

The government has identified no such binding appellate precedent. *Caira* applied the third-party doctrine to "records of the I.P. addresses [the defendant] used to log in to his Hotmail account," which revealed the location of his home and workplace. 833 F.3d at 808. In so holding, the Seventh Circuit distinguished the IP address records from the "longer term use of GPS technology" at issue in *Jones*, calling the defendant's attempt to equate IP addresses with GPS technology an "unhelpful exaggeration." *Ibid*. (internal quotation marks omitted). As the Seventh Circuit explained, the defendant's home and work IP addresses—in contrast to GPS technology, which "can monitor every single movement"—revealed "no information about how he got from home to work, how long he stayed at either place, … where he was when he was *not* at home or work," or where he was "[o]n days when he did not log in." *Ibid*. (internal quotation marks omitted). *Caira* therefore did not specifically authorize the GPS search here.

The government does not argue that *Caira*'s description of the third-party doctrine as "a bright-line application of the reasonable-expectation-of-privacy test," *id*. at 806, was sufficient for *Davis* purposes to establish a categorical rule in the Seventh Circuit specifically authorizing the police to collect *any* type of information, including GPS data, voluntarily turned over to a third party. It thus forfeits the point. *See Stanbridge*, 813 F.3d at 1038; *Nichols*, 755 F.3d at 600; *Alioto*, 651 F.3d at 721. Even setting aside forfeiture, *Caira*'s broad characterization of the third-party doctrine did not say enough about its scope to specifically authorize every possible application. To the contrary, by distinguishing long-term GPS data from IP addresses, *Caira* implicitly recognized the possibility that the doctrine did not reach long-term GPS data. *See* 833

F.3d at 808. Indeed, *Smith* itself—which *Caira* quoted for the bright-line rule, *id*. at 806—distinguished the pen register used there from a listening device with the observation that "pen registers do not acquire the *contents* of communications," thereby suggesting that the doctrine did not in fact apply categorically to all types of information shared with third parties. *Smith*, 442 U.S. at 741. The Seventh Circuit's decision in *United States v. Patrick*, 842 F.3d 540 (7th Cir. 2016), confirms that whether the third-party doctrine reached GPS data remained unsettled at the time of the GPS search. Although the government conceded in *Patrick* that it conducted a search when it gathered CSLI with a cell-site simulator, the Seventh Circuit expressed uncertainty as to whether that concession was correct, suggesting that the doctrine might apply if cell-site simulators could be analogized to pen registers, but also that it might not apply if the better analogy were to GPS trackers. *Id*. at 543-44. Thus, as of April 4, 2017, *Caira*'s passing description of the third-party doctrine as a "bright-line" rule did not specifically authorize the warrantless acquisition of long-term historical GPS data.

That leaves the Fourth Circuit's decision in *Graham* and the Sixth Circuit's later-reversed decision in *Carpenter*. The Sixth Circuit held in *Carpenter* that the government did not conduct a Fourth Amendment search when it acquired CSLI from the defendants' wireless carriers, reasoning that the third-party doctrine "diminish[ed] the defendants' expectation of privacy" in their location information. 819 F.3d at 888-89. In so holding, the Sixth Circuit expressly distinguished GPS data, explaining that the CSLI at issue there was "far less precise" than GPS data and thus could not tell a similarly revealing story of the target's activities. *Id*. at 884, 889. Like *Caira*, then, *Carpenter* did not specifically authorize the GPS search here.

The Fourth Circuit in *Graham* expressed a more expansive view of the third-party doctrine, describing it as "[a] *per se* rule that it is unreasonable to expect privacy in information

voluntarily disclosed to third parties" regardless of the amount or precision of the information shared. 824 F.3d at 436-37 ("If individuals lack *any* legitimate expectation of privacy in information they share with a third party, then sharing *more* non-private information with that third party cannot change the calculus."); *see also id*. at 426 n.3 (noting that CSLI is less precise than GPS tracking, but rejecting the notion that "the applicability of the Fourth Amendment hinges on the precision of CSLI"). So, if *Graham* counts as binding appellate precedent, its view of the third-party doctrine arguably authorized the Hinsdale police's GPS search at the time it was conducted in April 2017. The Seventh Circuit has not definitively resolved whether decisions from other circuits can be "binding appellate precedent" for purposes of the *Davis* good-faith exception. *See United States v. Brown*, 744 F.3d 474, 478 (7th Cir. 2014) (declining to decide "whether precedent from Circuit A could be deemed 'binding' (for the purpose of *Davis*) when the search occurs in Circuit B, where the issue remains unresolved"); *United States v. Martin*, 712 F.3d 1080, 1082 (7th Cir. 2013) (expressing doubt that *Davis* "allow[s] police officers to rely on a diffuse notion of the weight of authority around the country" where "there was no binding appellate precedent" in the circuit where the search took place, but declining to "definitely resolve this point"). In this court's view, the answer is no.

It is axiomatic that decisions from one circuit, while deserving respectful consideration, are not binding on district courts in another circuit. *See United States v. Glaser*, 14 F.3d 1213, 1216 (7th Cir. 1994) ("Nothing the eighth circuit decides is 'binding' on district courts outside its territory. Opinions 'bind' only within a vertical hierarchy. A district court in Wisconsin must follow [the Seventh Circuit's] decisions, but it owes no more than respectful consideration to the views of other circuits."). No reason has been offered, and none is apparent, why that understanding of "binding" precedent should apply to district courts but not to law enforcement

officers who operate in the same circuit. It follows that "binding appellate precedent" for purposes of *Davis* is precedent "governing the jurisdiction in which [the officers] are acting"—that is, Supreme Court decisions and that jurisdiction's circuit decisions. *United States v. Barraza-Maldonado*, 732 F.3d 865, 867-68 (8th Cir. 2013) (holding that the *Davis* good-faith exception applied where the officers conducted a search in the Ninth Circuit "in objectively reasonable reliance on binding Ninth Circuit precedent"); *see also United States v. Lustig*, 830 F.3d 1075, 1082-83 (9th Cir. 2016) (holding that decisions from outside the circuit where the police acted are not "binding appellate precedent" for *Davis* purposes); *United States v. Aguiar*, 737 F.3d 251, 261-62 (2d Cir. 2013) (holding that "'binding precedent' refers to the precedent of this Circuit and the Supreme Court," and not to cases from other circuits).

In this respect, the *Davis* good-faith exception operates differently from the qualified immunity doctrine. Under *Davis*, the good-faith exception applies "when the police conduct a search in objectively reasonable reliance on binding appellate precedent" that "specifically *authorizes* a particular police practice." *Davis*, 564 U.S. at 241, 249-50; *see also Jenkins*, 850 F.3d at 918 (same). Qualified immunity, by contrast, protects officers from damages liability under 42 U.S.C. § 1983 unless "it was objectively *unreasonable* for [them] to believe that [their conduct] was lawful"—that is, unless their conduct violated "clearly established" law. *Williams v. Ind. State Police Dep't*, 797 F.3d 468, 473 (7th Cir. 2015) (emphasis added); *see also Mullenix v. Luna*, 136 S. Ct. 305, 308 (2015) ("[E]xisting precedent must have placed the statutory or constitutional question beyond debate.") (internal quotation marks omitted). In the face of silence from the circuit in which an officer acted, it is entirely consistent to say that cases from other circuits authorizing a practice (1) suggest that the practice did not violate clearly established law, thereby entitling the officer to qualified immunity, but (2) do not constitute

"binding appellate precedent [that] specifically authorizes" the practice, *Davis*, 564 U.S. at 241 (emphasis omitted), and so do not support invocation of the good-faith exception.

Thus, even if the Fourth Circuit's decision in *Graham* and the Sixth Circuit's decision in *Carpenter* specifically authorized the warrantless acquisition of long-term historical GPS data from a third party, they were not binding appellate precedent in the Seventh Circuit. It follows that the *Davis* good-faith exception does not save the GPS search here. *See Jenkins*, 850 F.3d at 920.

Finally, even if all of the above-stated reasons for rejecting the government's *Davis* argument are wrong—that is, even if *Carpenter*'s expressed understanding of the third-party doctrine's pre-*Carpenter* scope could be set aside, even if *Caira* reached GPS tracking, and even if out-of-circuit authority were binding—the good-faith exception still would not apply. The reason is that neither Diggs nor Adams "voluntarily turn[ed] over" the GPS data to Headers, and the government has not identified any decision specifically authorizing law enforcement to gather information from a third party to which the information was not voluntarily provided. *Carpenter*, 138 S. Ct. at 2216 (quoting *Smith*, 442 U.S. at 744); *see also id*. at 2220 (holding that the "voluntary exposure" rationale for the third-party doctrine does not "hold up when it comes to CSLI" because individuals have no meaningful choice as to whether to generate CSLI).

The government maintains that the GPS data was voluntarily provided to Headers because Adams's "contract with Headers alerted her to the potential presence of an electronic tracking device." Doc. 55 at 7-8. The contract states in pertinent part: "If your vehicle has an electronic tracking device, you agree that we may use this device to find the vehicle." Doc. 55-1 at 4. While acknowledging that this provision "indicate[s] that the information would be used only to locate the Lexus, not to determine its prior movements," the government contends that

the third-party doctrine applies "even if the information is revealed on the assumption that it will be used only for a limited purpose." Doc. 55 at 7-8 (emphasis and internal quotation marks omitted). Yet by authorizing Headers to "use [the] device to find the vehicle," Doc. 55-1 at 4, Adams did not also give Headers permission to continuously track the vehicle, and thus did not voluntarily turn historical GPS information over to Headers for *any* purpose. Given that the provision appears in a contract for the sale of a vehicle on credit, the only plausible reading is that it permits Headers to activate the GPS to determine the vehicle's current location if, for example, the buyer defaults and Headers exercises its right to repossess or if the vehicle is reported stolen. *See ibid*. (Indiana choice-of-law provision); *Vesuvius USA Corp. v. Am. Commercial Lines LLC*, 910 F.3d 331, 333 (7th Cir. 2018) ("In Indiana, the general rules of contract interpretation are that, unless the terms of a contract are ambiguous, they will be given their plain and ordinary meaning. … [W]e must construe the contract as a whole and consider all provisions of the contract, not just the individual words, phrases, or paragraphs.") (alteration and internal quotation marks omitted). As the government recognizes by distinguishing between "locat[ing] the Lexus" and "determin[ing] its prior movements," Doc. 55 at 7, the continuous monitoring through which Headers in fact generated the GPS data had nothing to do with "finding" the vehicle in any ordinary sense of that word, and thus went beyond the kind of location monitoring that the contract authorized. *See BMD Contractors, Inc. v. Fid. & Deposit Co. of Md.*, 679 F.3d 643, 656 n.8 (7th Cir. 2012) (applying Indiana law and rejecting an "unnatural" reading of a contract).

It follows that Diggs did not "voluntarily assume the risk of turning over a comprehensive dossier of his physical movements," *Carpenter*, 138 S. Ct. at 2220 (alteration and internal quotation marks omitted), thus precluding reliance on the third-party doctrine even if

pre-*Carpenter* decisions extended it to historical GPS location data. While binding appellate precedent held that the third-party doctrine reached information "revealed [to a third party] on the assumption that it will be used only for a limited purpose," *id*. at 2216 (quoting *Miller*, 425 U.S. at 443), the government points to no decision holding that the doctrine also applies when a third party is authorized to collect only a limited amount of information but exceeds its authorization and collects much more.

The government invokes no other exception to the exclusionary rule, thus forfeiting any such argument. *See Stanbridge*, 813 F.3d at 1038; *Nichols*, 755 F.3d at 600; *Alioto*, 651 F.3d at 721. The GPS data is therefore suppressed. *See United States v. Conrad*, 673 F.3d 728, 732 (7th Cir. 2012) ("The Supreme Court has long recognized the need to exclude evidence obtained in violation of the Constitution's protections. Indeed, unless one of the various exceptions applies, exclusion will run not only to the unconstitutionally obtained evidence, but also to the fruits of that evidence—the so-called fruit of the poisonous tree.") (citation omitted).

Conclusion

Diggs's suppression motion is granted. The GPS data obtained by the Hinsdale police is suppressed. Further proceedings are necessary to determine whether the GPS data yielded any unlawful fruits and, if so, whether suppression of those fruits is warranted. Doc. 49 at 3 n.2 (Diggs contending that the government used the GPS data to support its successful applications for search warrants for DNA and social media records); Doc. 49-1 at 2-4 (the search warrant application for the collection of a saliva sample from Diggs for DNA testing).

May 13, 2019

Gary Feinerman
United States District Judge