

In the
United States Court of Appeals
For the Seventh Circuit

No. 21-1614

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DEWAYNE LEWIS,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Indiana, Fort Wayne Division.
No. 1:15-CR-00010-TLS-SLC-1 — **Theresa L. Springmann**, *Judge.*

ARGUED MAY 16, 2022 — DECIDED JUNE 21, 2022

Before EASTERBROOK, BRENNAN, and ST. EVE, *Circuit Judges.*

ST. EVE, *Circuit Judge.* Dewayne Lewis appeals the denial of his motion to suppress large quantities of cash and drugs found in his hotel room. Lewis was a distributor in a drug-trafficking operation whose leader fled to Mexico. An FBI informant passed along Lewis's cell phone number, and the government obtained a tracking order pursuant to the Stored Communications Act, 18 U.S.C. § 2703(d). Cell-site location

information (“CSLI”) from Lewis’s cell phone provider showed that his phone was within a 1,099-meter radius of Greenwood, Indiana. From there, officers searched parking lots and hotels where a deal might take place. Officers eventually saw a woman resembling Lewis’s wife enter a room at a hotel, drop off a duffel bag, and drive away in a car registered in Lewis’s name. After a drug-sniffing dog alerted at the room, officers applied for a search warrant, and the team executed the warrant the same day. Inside the room, officers found Lewis, \$2 million in cash, and 19.8 kilograms of cocaine.

After a bench trial, the district court found Lewis guilty of possession with intent to distribute five kilograms or more of cocaine. Lewis argues that the dog sniff violated his reasonable expectation of privacy. In the alternative, he argues that the application for the § 2703(d) order lacked probable cause. Assuming that the court should have suppressed the evidence in his hotel room, Lewis further argues that the evidence presented at trial was insufficient to convict him.

We affirm. Lewis lacked a reasonable expectation of privacy in the exterior hallway of his hotel, where the dog sniff occurred. And regardless of whether the government’s use of real-time CSLI amounted to a search, the good-faith exception applies. Because the district court correctly denied the motion to suppress, we do not assess the sufficiency of the remaining evidence.

I. Background

A. The Drug-Distribution Operation

Lewis reported to a man named Allan Bates. In December 2014, Bates introduced Lewis to Thomas “TJ” Boyle. Lewis drove a black Mercedes SUV to the meeting and gave Bates

\$125,000 in cash. Unbeknownst to Bates and Lewis, Boyle was actually an FBI informant. Boyle had agreed to provide the FBI with evidence of Bates's drug operation in exchange for working off a probation revocation. The FBI considered Boyle very reliable because his information previously led to the seizure of \$400,000 from Bates's right-hand man, Larry Norton. Boyle also passed on information about a barn near Butler, Indiana, where the drug-trafficking operation stored cash and drugs in a hidden compartment.

On January 27, 2015, the FBI served search warrants in Indiana, Ohio, and Texas in connection with its investigation of Bates's operation. Bates fled, and Lewis helped him escape to Mexico. On February 1, 2015, Bates told Lewis that he and an associate, Chris Cook, needed to retrieve over \$1 million and 20 kilograms of cocaine from the Butler barn. Lewis and Cook did as Bates instructed, and Lewis told Bates that there were only 19 kilograms, not the expected 20. At Bates's direction, Cook kept \$60,000 in cash, and Lewis transferred the remaining cash and drugs to his car.

Meanwhile, the FBI obtained search warrants to review text messages on a phone that Bates was using in Mexico. On January 29, Bates texted Lewis and asked him to check on Boyle. Bates also told Boyle that "Nap" in Indianapolis (meaning Lewis) could help Boyle get cash and a rental car so he could flee to Texas. Crucially, Bates gave Boyle Nap's cell phone number.

B. The Tracking Order

Boyle passed along the cell phone number to FBI Agent Keszei. FBI Staff Operations Specialist Graff researched the number and determined that it was assigned to a Sprint

phone owned by “Dewayne Lewis.” The phone was pre-paid, so there was no billing address. Graff searched for Dewayne Lewises in Indianapolis and found one who was born in 1977, had a prior drug conviction, and was wanted on an outstanding warrant (the “1977 Lewis”). The 1977 Lewis is *not* the Defendant, who was born in 1974 and did not have an outstanding warrant at the time. Complicating matters, Boyle incorrectly identified a photograph of the 1977 Lewis as “Nap.” Both the 1977 Lewis and Defendant Lewis are black.

On January 30, 2015, an officer with the U.S. Marshals’ Violent Fugitive Task Force applied for and received a court order under the Stored Communications Act, 18 U.S.C. § 2703(d). The application sought precision location-based information for Nap’s cell phone, including cell-site activations, “twenty-four hour a day assistance ... to triangulate target location,” and “[h]istorical call detail records for 30 days,” among other things. In support of the application, Officer Harshman wrote:

Applicant certifies that the information sought is relevant and material to a *fugitive investigation*, to wit: that the INDIANA STATE POLICE [and] US MARSHALS SERVICE are conducting an investigation to locate DEWAYNE LEWIS, a *fugitive from justice*. DEWAYNE LEWIS has an *active warrant* for a PAROLE VIOLATION on an original charge of DEALING COCAINE, IC: 35-48-4-1. On January 30, 2015, Trp. Brian Harshman was contacted by FBI S/A James Keszei reference [sic] assisting in locating and arresting DEWAYNE LEWIS. DEWAYNE LEWIS has an *active warrant* out of the Indiana Department of

Corrections for a parole violation. S/A Keszei advised that he is currently involved in an investigation involving a drug trafficking organization in which DEWAYNE LEWIS is involved. S/A Keszei advised that during the course of the investigation it has been learned through informants and additional investigations that DEWAYNE LEWIS is utilizing a cellular telephone with an associated number of (317)507-8010. TFO Harshman was able to utilize law enforcement contacts within the Sprint Wireless Law Enforcement Compliance Department that [sic] (317)507-8010 does indeed belong to their company. Since DEWAYNE LEWIS is utilizing this cellular phone with associated number (317)507-8010, it is believed that the requested records and information will assist officers in locating and arresting DEWAYNE LEWIS.

(emphases added). On January 30, an Indiana state court judge granted the application “for the period of January 1, 2015 to the present and extending thirty (30) days past the date of this Order.” In doing so, the judge found “that the information likely to be obtained is relevant and material to an ongoing criminal investigation.”

Sprint began providing location information for the cell phone sometime on the morning of February 3, 2015. Sprint’s data showed that Nap’s phone was within a 1,099-meter radius (roughly two-thirds of a mile) of Greenwood, a suburb of Indianapolis. After 11:34 a.m., the phone was no longer connected to Sprint’s network, possibly because the phone had been turned off. The phone reconnected to the network at

3:59 p.m. By that point, as explained below, officers had already zeroed in on Lewis's likely location. Between 3:59 p.m. and 4:21 p.m., Sprint reported that the phone was still within the same area of Greenwood, but Officer Harshman was no longer receiving email updates from Sprint. In any event, after approximately 3:00 p.m., Officer Harshman did not review the location data because he and the other officers were following another lead.

C. The Dog Sniff

On February 3, 2015, in reliance on the Sprint location data, eight to ten Marshals' Task Force Officers checked parking lots across Greenwood for a black Mercedes SUV. They also asked clerks at five local hotels if a black male had recently checked in. Sometime after 2:00 p.m., Officer Jason York checked a police database and discovered that Defendant Lewis lived in Greenwood and had two cars registered in his name: a black Mercedes and a white Cadillac Escalade. Officer York realized for the first time, however, that there was a discrepancy between Defendant Lewis's birth year and the birth year of the man whose outstanding arrest warrant had provided the basis for the § 2703(d) order. Officer Harshman emailed FBI Task Force Officer Martinez about the discrepancy at 2:23 p.m. Officer Martinez told Officer Harshman that the date of birth in the police database might be wrong, but he was confident that the vehicle description was correct, so the Marshals should locate Lewis and take him into custody.

Around 3:00 p.m., an officer on the team learned that a "Michael Jackson" of Evansville, Indiana had checked into Room 211 of the Greenwood Red Roof Inn at 10:10 a.m. (Jackson is a real person, but Defendant Lewis had apparently checked in using his name.) Room 211 is on the second floor

of the hotel and is accessible via an exterior hallway and staircase leading directly to the parking lot. Sometime after 3:00 p.m., an officer on the team saw a white Cadillac Escalade drive into the Red Roof Inn parking lot. The driver was a woman who resembled a picture of Lewis's wife from the Indiana Bureau of Motor Vehicles. A license plate check confirmed that the car was registered to Lewis. The woman took a duffel bag out of the car, brought it inside Room 211, and left the room less than five minutes later.

At 3:35 p.m., about twenty minutes after the woman left, several officers approached Room 211 and knocked on the door. No one answered. At 3:41 p.m., a K-9 handler walked a trained drug-detection dog up the exterior staircase and along the second-floor hallway. After passing seven other doors, the dog alerted at Room 211. Based on the dog sniff, a Greenwood police sergeant applied for a search warrant for Room 211. A local judge approved the warrant at 4:50 p.m., and officers executed the warrant at 5:05 p.m. The officers found Lewis, \$2 million in cash, and 19.8 kilograms of cocaine in duct-taped packages. Lewis later confessed to his role in the drug-trafficking organization.

On the morning of February 4, 2015, one day after Sprint began providing location information for Lewis's cell phone, the Marshals emailed Sprint to discontinue the tracking order.

D. Procedural History

After his arrest, Lewis waived his right to counsel and generally proceeded pro se. A magistrate judge construed Lewis's motion to dismiss the indictment as a motion to suppress evidence resulting from the dog sniff. In February 2016, the magistrate conducted a two-day evidentiary hearing

focused primarily on the dog sniff, followed by a supplemental hearing in January 2017 focused on the § 2703(d) order. The magistrate recommended that the district court suppress all evidence from the hotel room and Lewis's subsequent confession, reasoning that the dog sniff violated the Fourth Amendment. *United States v. Lewis*, No. 1:15-CR-00010-TLS-SLC, 2017 WL 9565360, at *8–9 (N.D. Ind. May 24, 2017) (citing *United States v. Whitaker*, 820 F.3d 849, 853 (7th Cir. 2016)).

In a July 2017 opinion—before *Carpenter v. United States*, 138 S. Ct. 2206 (2018)—the district court rejected that recommendation and denied the motion to suppress. The district judge noted that the Supreme Court had distinguished *Kyllo v. United States*, 533 U.S. 27 (2001) in *Illinois v. Caballes*, 543 U.S. 405 (2005), meaning that dog sniffs do not necessarily infringe reasonable expectations of privacy. The district court further distinguished this court's decision in *Whitaker*, which held that a warrantless dog sniff in the interior hallway of an apartment building violated the Fourth Amendment. 820 F.3d at 853. In the district court's view, the dog sniff in this case did not invade the curtilage, so there was no Fourth Amendment violation. The district court further concluded that any error in the application for the § 2703(d) order was harmless because the officers were not relying on cell-site location information after 11:34 a.m., when Sprint stopped reporting data.

Lewis waived his right to a jury trial. After a three-day bench trial, the district court found him guilty of possessing more than five kilograms of cocaine with the intent to distribute. The judge expressly found that, even if the evidence from the hotel room and Lewis's cell phone had been suppressed, Lewis was still guilty beyond a reasonable doubt. The court

also found that Bates and Cook testified credibly and consistently as to Lewis's involvement in the operation. The government had presented text messages between Lewis and Bates discussing the quantity of drugs stored at the barn and a ledger showing large payments from Bates to Lewis. This evidence showed beyond a reasonable doubt that Lewis knew the packages he and Cook retrieved on February 1, 2015, contained more than five kilograms of cocaine.

II. Discussion

When a defendant appeals the denial of a motion to suppress, we review the district court's legal conclusions de novo and its factual findings for clear error. *United States v. Hammond*, 996 F.3d 374, 383 (7th Cir. 2021).

A. The Dog Sniff

The Fourth Amendment safeguards "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Generally, a law enforcement officer may not perform a search without a warrant supported by probable cause, unless an exception to the warrant requirement applies. *Lange v. California*, 141 S. Ct. 2011, 2017 (2021). Conversely, if something is not a search, then there is no need for a warrant. *Illinois v. Caballes*, 543 U.S. 405, 408 (2005) ("Official conduct that does not compromise any legitimate interest in privacy is not a search subject to the Fourth Amendment.") (internal quotation marks omitted).

Two lines of precedent govern whether officer conduct amounts to a search. Under the property-based approach, a search occurs when an officer enters a constitutionally protected area, such as the home, for the purpose of gathering evidence against the property owner. *Florida v. Jardines*, 569

U.S. 1, 6 (2013) (explaining that the curtilage is the area “immediately surrounding and associated with the home” and is “part of the home itself for Fourth Amendment purposes”) (quoting *Oliver v. United States*, 466 U.S. 170, 180 (1984)). This approach derives from common-law trespass. *United States v. Jones*, 565 U.S. 400, 405–06 & n.3 (2012) (“Where ... the Government obtains information by physically intruding on a constitutionally protected area, [] a search has undoubtedly occurred.”).

Alternatively, under the privacy-based approach, courts ask whether a person has a legitimate expectation of privacy in a given situation. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining that the Fourth Amendment applies when “a person [has] exhibited an actual (subjective) expectation of privacy and ... the expectation [is] one that society is prepared to recognize as ‘reasonable’”). The privacy-based approach also limits the government’s ability to exploit technological advances. *Kyllo v. United States*, 533 U.S. 27, 34–35 (2001) (holding that the use of a thermal imager to detect heat radiating from a home was a search).

The Supreme Court has sometimes held that the use of drug-sniffing dogs constitutes a search. Compare *Jardines*, 569 U.S. at 11–12 (dog sniff for drugs on front porch of home is a search), with *Caballes*, 543 U.S. at 410 (dog sniff for drugs during a lawful traffic stop is not a search because the sniff “reveals no information other than the location of a substance that no individual has any right to possess”); *United States v. Place*, 462 U.S. 696, 707 (1983) (dog sniff of luggage in an

airport is not a search because it “discloses only the presence or absence of narcotics, a contraband item”).¹

In *Jardines*, officers brought a drug-sniffing dog onto the front porch of a home whose owner they suspected of growing marijuana. Justice Scalia’s majority opinion reasoned that the front porch is the “classic exemplar” of the curtilage, meaning that it is part of the home for Fourth Amendment purposes. 569 U.S. at 7. Visitors to a home have an implied license “to approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave.” *Id.* at 8. But the officers in *Jardines* exceeded the scope of that license by bringing a drug-sniffing dog into the curtilage. *Id.* at 9–10. Justice Kagan’s concurrence explained that the same outcome would follow under the privacy-based approach in *Kyllo* and *Katz*. *Id.* at 13 (Kagan, J., concurring). In her view, the case was a straightforward application of *Kyllo* because the officers used “a ‘device ... not in general public use’ (a trained drug-detection dog) to ‘explore details of the home’ (the presence of certain substances) that they would not otherwise have discovered without entering the premises.” *Id.* at 14–15 (quoting *Kyllo*, 533 U.S. at 40).

Lewis argues that the dog sniff outside his hotel room constituted a search. He asks that we extend this court’s decision in *Whitaker*, which held that a dog sniff for drugs in the interior hallway of an apartment building constituted a search.

¹ This case involves a dog sniff for controlled substances, not explosives. Even the dissenters in *Caballes* recognized that “[a] dog sniff for explosives, involving security interests not presented here, would be an entirely different matter.” *Caballes*, 543 U.S. at 423 (Ginsburg, J., dissenting). “[T]he immediate, present danger of explosives would likely justify a bomb sniff under the special needs doctrine.” *Id.* at 425.

820 F.3d at 852–54. Notably, we did not conclude in *Whitaker* that the area outside the defendant’s apartment door amounted to curtilage. *Id.* at 853 (observing that defendant lacked the right to exclude people from the hallway). Instead, the court drew upon Justice Kagan’s concurring opinion in *Jardines* and reasoned that apartment residents have a reasonable expectation of privacy in the area outside their doors. We also distinguished the facts in *Whitaker* from *Caballes* and *Place* because those sniffs occurred in public places rather than a home.

1. Property-Based Approach

The key question under the property-based approach is whether the area outside Lewis’s hotel room door was constitutionally protected. *Jardines*, 569 U.S. at 6. Recall that the hallway of this particular hotel was open-air and accessible via an exterior staircase that led directly to a parking lot. Unlike the homeowner in *Jardines*, Lewis lacked the right to exclude members of the public from passing through the exterior hallway. And as noted above, the *Whitaker* court did not even conclude that the interior hallway of an apartment building amounts to curtilage. *Whitaker*, 820 F.3d at 853. The exterior hallway of the Red Roof Inn is even farther afield from a front porch than an interior apartment hallway, so there was no search under the property-based approach.

2. Privacy-Based Approach

Lewis fares no better under the privacy-based approach. Justice Harlan’s formulation of that approach asks (1) whether “a person [has] exhibited an actual (subjective) expectation of privacy,” and (2) whether “the expectation [is] one that society is prepared to recognize as ‘reasonable.’”

Katz, 389 U.S. at 361 (Harlan, J., concurring). Even assuming that Lewis had a subjective expectation of privacy, the Supreme Court's decisions in *Caballes* and *Place* demonstrate that his expectation was not reasonable.

In *Place*, the Court explained that exposing luggage to a drug-sniffing dog in an airport was not a search, in large part because "the sniff discloses only the presence or absence of narcotics, a contraband item." 462 U.S. at 707. Unlike an officer "rummaging through the contents of the luggage," a dog sniff "does not require opening the luggage" and "does not expose noncontraband items that otherwise would remain hidden from public view." *Id.* Similarly, in *Caballes*, the Court reasoned that "any interest in possessing contraband cannot be deemed legitimate, and thus, governmental conduct that *only* reveals the possession of contraband compromises no legitimate privacy interest." *Caballes*, 543 U.S. at 408 (internal quotation marks omitted). *Caballes* also distinguished *Kyllo*, which involved a thermal-imaging device "capable of detecting lawful activity," including "intimate details in a home." *Id.* at 409–10. "The legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent's hopes or expectations concerning the nondetection of contraband in the trunk of his car." *Id.* at 410.

This is not to say that Lewis had no reasonable expectation of privacy whatsoever inside his hotel room. Lewis is correct that the Fourth Amendment extends to temporary dwelling places, such as hotel and motel rooms. *Finsel v. Cruppenink*, 326 F.3d 903, 907 (7th Cir. 2003) (citing *Stoner v. California*, 376 U.S. 483, 490 (1964)). A hotel guest has a reasonable expectation, for example, that there is not a hidden camera in her

room. But that does not mean an expectation of privacy that is reasonable in a home (i.e., to be free of warrantless dog sniffs) is necessarily reasonable in a hotel room. In that respect, the exterior hallway of a hotel adjacent to a parking lot is much closer to the public settings in *Caballes* and *Place* than the front porch in *Jardines*.

Lewis was also a mere guest, not a resident. While it is true that hotel guests have some legitimate expectations of privacy, they cannot exclude others from entering a hallway—particularly where, as here, an exterior hallway is accessible from a staircase leading directly to the parking lot. Indeed, the Supreme Court in *Stoner* recognized that “when a person engages a hotel room he undoubtedly gives implied or express permission to such persons as maids, janitors or repairmen to enter his room in the performance of their duties.” *Stoner*, 376 U.S. at 489 (internal quotation marks omitted). If hotel guests have only a limited right to exclude hotel staff from a room, then it is hard to see how guests at the Red Roof Inn could reasonably expect to be free of dog sniffs in the exterior hallway.

B. The § 2703(d) Order

Section 2703 of the Stored Communications Act authorizes courts to “order cell-phone providers to disclose non-content information” in response to a governmental entity’s request. *Hammond*, 996 F.3d at 384–85 (citing 18 U.S.C. § 2703(c)(1)(B)). Prior to the Supreme Court’s decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the government could obtain a court order by “offer[ing] 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.” 18 U.S.C. § 2703(d) (emphasis added).

Cell-site location information (“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). “Because cell phones are in constant communication with the nearest cell site—often affixed to a cell tower—they can collect CSLI as frequently as several times a minute.” *Id.* (citing *Carpenter*, 138 S. Ct. at 2211–12). “The precision of this information depends on the size of the geographic area covered by the cell site.” *Carpenter*, 138 S. Ct. at 2211. In dense urban areas, CSLI might be very precise, but CSLI is generally less precise than GPS tracking.

Courts distinguish between historical CSLI and real-time CSLI: historical CSLI allows law enforcement to retrace a defendant’s physical movements, while real-time CSLI shows (roughly) where a defendant’s cell phone is currently located. *Hammond*, 996 F.3d at 387; *Carpenter*, 138 S. Ct. at 2220 (expressing no opinion on “real-time CSLI”). “As with GPS information, [historical CSLI] 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 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

In *Carpenter*, the Supreme Court held that the collection of historical CSLI over the course of a substantial period of time (127 days) was a search. *Carpenter*, 138 S. Ct. at 2217. Because § 2703(d)’s “reasonable grounds” language poses a lower bar than probable cause, the government can no longer rely on

the language of the statute alone. *Id.* at 2221 (“[A]n order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records.”). Instead, the government must generally obtain a warrant to access those records, subject to common-sense exceptions for emergencies. *Id.* at 2222–23.

1. *The Good-Faith Exception*

The exclusionary rule is a judicially created remedy to deter violations of criminal defendants’ constitutional rights. *Davis v. United States*, 564 U.S. 229, 236–37 (2011); *Curtis*, 901 F.3d at 849. A defendant may invoke the rule to prevent tainted evidence from being used against him at trial, but 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.’” *Hammond*, 996 F.3d at 384 (quoting *Davis*, 564 U.S. at 236–37).

The Supreme Court has emphasized that the exclusionary rule does not apply when it would serve no deterrent function. *United States v. Leon*, 468 U.S. 897, 922 (1984) (good-faith reliance on a facially valid warrant); *Illinois v. Krull*, 480 U.S. 340, 356–57 (1987) (good-faith reliance on then-valid statute); *Davis*, 564 U.S. at 232 (good-faith reliance on then-binding circuit precedent). In *Curtis*, this court concluded that the good-faith exception applies to historical CSLI obtained via a § 2703(d) order before the *Carpenter* decision. The *Curtis* court reasoned that under *Krull*, the exclusionary rule does not apply to the fruits of evidence obtained in good-faith reliance on a subsequently invalidated statute. 901 F.3d at 848 (citing *Krull*, 480 U.S. at 349–50); *see also United States v. Rosario*, 5 F.4th 706, 711–12 (7th Cir. 2021); *Hammond*, 996 F.3d at 386; *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019).

The government contends Lewis forfeited his argument that the § 2703(d) order lacked probable cause by failing to raise it below.² We will nonetheless consider it for several reasons. Lewis was pro se below, and he did move to suppress the fruits of the § 2703(d) order on the grounds that it relied on inaccurate information (the outstanding warrant for the 1977 Lewis). In any event, his argument lacks merit because the good-faith exception applies.

a. Historical CSLI

The tracking order in this case seems to have granted the government permission to obtain historical CSLI between January 1, 2015, and “thirty (30) days past the date of this Order,” which was entered on January 30, 2015. At oral argument, however, the government clarified that it did not rely on historical CSLI either to find Lewis or to prosecute him for possession with intent to distribute. Indeed, both parties agree that Sprint did not begin sending data to law enforcement until February 3, 2015, the day of his arrest. Because the government did not use historical CSLI or the fruits of such information against Lewis at trial, there is nothing to exclude. *See Wong Sun v. United States*, 371 U.S. 471, 487–88 (1963); *Hammond*, 996 F.3d at 383 (“[T]here is no need to exclude evidence never admitted at trial or used improperly to obtain additional evidence.”).

² Not to be outdone, Lewis argues the government forfeited reliance on the good-faith exception by not raising it in the district court. This counterattack is unpersuasive because, when the district court ruled on the motion to suppress in 2017, neither *Carpenter* nor *Curtis* had been issued, so there was no basis for raising a good-faith exception argument.

Moreover, this court has repeatedly held that the good-faith exception applies to historical CSLI collected pursuant to a § 2703(d) order pre-*Carpenter*. See *Rosario*, 5 F.4th at 711–12; *Hammond*, 996 F.3d at 386; *Curtis*, 901 F.3d at 849. The mere act of applying for a § 2703(d) order suggests that Officer Harshman made a good-faith attempt to comply with a then-valid statute. Cf. *United States v. Matthews*, 12 F.4th 647, 653 (7th Cir. 2021) (“Although it is the Government’s burden to demonstrate that the officer was acting in objective good faith, an officer’s decision to obtain a warrant is prima facie evidence of his good faith.”). And there is no evidence that Officer Harshman knowingly or recklessly misled the judge or that the affidavit was facially invalid at the time he filed it. *United States v. Rees*, 957 F.3d 761, 771 (7th Cir. 2020).

b. Real-time CSLI

In *Hammond*, we declined to categorically extend *Carpenter* to real-time CSLI. *Hammond* involved three different types of CSLI: (1) historical CSLI collected pursuant to a § 2703(d) order, (2) historical CSLI collected pursuant to a § 2702 request, and (3) real-time CSLI collected pursuant to a § 2702 request. *Hammond*, 996 F.3d at 383. A § 2702 request “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.’” *Id.* at 386 (quoting 18 U.S.C. § 2702(c)(4)). Although the real-time CSLI in *Hammond* was obtained via a § 2702 request rather than a court order, any distinction between §§ 2702 and 2703 did not affect our analysis of how *Carpenter* applies to real-time CSLI.

Law enforcement in *Hammond* used real-time CSLI for several hours on a single day to track the defendant across Indiana. *Hammond*, 996 F.3d at 381. Of relevance here, the *Hammond* court held that a request for real-time CSLI did not amount to a search because the defendant was “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.” *Id.* at 392. On those facts, the defendant had no reasonable expectation of privacy, so evidence stemming from the use of real-time CSLI to arrest Hammond did not have to be suppressed. *Id.* at 391. In the alternative, we concluded that the good-faith exception applied to the collection of real-time CSLI pursuant to a § 2702 request. *Id.* at 392–93.

In light of *Hammond*, even assuming the use of real-time CSLI in this case amounted to a search, the good-faith exception applies. The officers here relied on § 2703(d)’s “reasonable grounds” requirement when seeking a court order. Prior to *Carpenter*, good-faith reliance on this provision for the collection of *historical* CSLI was reasonable. *Curtis*, 901 F.3d at 848. Historical CSLI raises grave privacy concerns because it allows the government to retrace a person’s movements over time. *Carpenter*, 138 S. Ct. at 2217. Real-time CSLI, while still implicating privacy interests, is more analogous to tracking a suspect on public roads. *Cf. United States v. Knotts*, 460 U.S. 276 (1983) (holding that the use of a beeper in a drum of chloroform to track a suspect’s car on public roads was not a search); *Hammond*, 996 F.3d at 389–90 (discussing *Knotts*). It follows that the good-faith exception applies not only to

historical CSLI collected under § 2703(d), but also to real-time CSLI. We leave for another day whether the collection of real-time CSLI after *Carpenter* ever amounts to a search.

2. *Errors in the § 2703(d) Affidavit*

Alternatively, Lewis argues that the officers should have ceased their investigation when they learned that the intended target was not born in 1977. The mix-up was potentially material to Officer Harshman's § 2703(d) application because the 1977 Lewis, unlike the Defendant, had an outstanding warrant for a parole violation. Indeed, Officer Harshman's affidavit emphasized that information from Lewis's cell phone was critical to a "fugitive investigation" and that Lewis was a "fugitive from justice." Around 2:00 p.m. on February 3, Officer York learned that Defendant Lewis was born in 1974, and Officer Harshman emailed FBI TFO Martinez about the discrepancy at 2:23 p.m. Officer Martinez asked the team to continue looking for Lewis, in part because the black Mercedes registered in Lewis's name corroborated the tip from Boyle. It is unclear from the record when the officers learned that Defendant Lewis did not have any outstanding warrants. It is also unclear when or if Officer Harshman pieced together that Boyle's incorrect photo identification of the 1977 Lewis as "Nap" undermined Boyle's credibility.

Lewis is correct that officers must cease executing a search warrant when they learn of a material error in a probable cause affidavit. See *Maryland v. Garrison*, 480 U.S. 79, 86 (1987); *Muhammad v. Pearson*, 900 F.3d 898, 904 (7th Cir. 2018) ("Officers executing warrants ... may violate the Fourth Amendment if they know or should know, before execution, that the warrant has an error or critical ambiguity that risks a search of the wrong location."). We are skeptical, however, that the

facts that were then known to the officers materially undermined the basis for the § 2703(d) order. From what we can tell, the only discrepancy that the officers knew of on the afternoon of February 3 was Lewis's birth year—not the fact that he lacked outstanding warrants or that Boyle had incorrectly identified Nap. A three-year difference in birth year, alone, did not require them to stop searching and report to the magistrate judge.

Regardless, any belatedly discovered errors in the § 2703(d) affidavit were attenuated from the events that led to Lewis's eventual arrest. *See Wong Sun*, 371 U.S. at 487–88; *United States v. Green*, 111 F.3d 515, 520–21 (7th Cir. 1997). Sprint was not sending any information to law enforcement between 11:34 a.m. and 3:59 p.m., possibly because Lewis's phone was turned off. Between 3:00 p.m. and 3:41 p.m., officers saw a woman resembling Lewis's wife drop off a bag in Room 211, the woman drove away in a car registered in Lewis's name, and a drug-sniffing dog had alerted at the door. Thus, by the time Sprint began sending information again, the officers were already in the process of seeking a search warrant for Room 211.

III. Conclusion

For the foregoing reasons, the district court's denial of the motion to suppress is

AFFIRMED.