RECOMMENDED FOR PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 24a0022p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ROBERT ZENAS WHIPPLE, III,

Defendant-Appellant.

No. 23-5126

Appeal from the United States District Court for the Eastern District of Tennessee at Knoxville.
No. 3:20-cr-00031-1—Katherine A. Crytzer, District Judge.

Argued: December 6, 2023

Decided and Filed: February 8, 2024

Before: BATCHELDER, CLAY, and GIBBONS, Circuit Judges.

COUNSEL

ARGUED: Joshua D. Hedrick, WHITT, COOPER, HEDRICK & WOJCIK, Knoxville, Tennessee, for Appellant. Samuel R. Fitzpatrick, UNITED STATES ATTORNEY'S OFFICE, Knoxville, Tennessee, for Appellee. **ON BRIEF:** Joshua D. Hedrick, WHITT, COOPER, HEDRICK & WOJCIK, Knoxville, Tennessee, for Appellant. Samuel R. Fitzpatrick, UNITED STATES ATTORNEY'S OFFICE, Knoxville, Tennessee, for Appellee.

OPINION

ALICE M. BATCHELDER, Circuit Judge. Robert Whipple appeals the denial of his motions to suppress evidence. Whipple argued that law enforcement violated his Fourth Amendment rights when officers subpoenaed Walmart for his purchase history, searched his

phone after the expiration of the warrant for his phone, and impermissibly seized his car. The district court denied Whipple's motions. Finding no merit to these claims, we **AFFIRM**.

I. Background and Procedural History

a. Background

Between March 5 and 7 of 2020, three Knoxville, Tennessee, banks were robbed. The first two robberies were committed by a "a heavy-set white male" who "wore a thin red rain poncho, light-colored shorts, white shoes, and disposable gloves." The robber used a manila envelope to write his demand letters for each robbery. The third robbery was committed by a large white male, this time wearing "a tan jacket, a curly wig, blue jeans, and white sneakers." But he still wrote his demand letter on a manila envelope.

On March 7, FBI agents contacted a nearby Walmart, asking specifically about recent purchases of red rain ponchos and tan Dickies-brand jackets. Walmart security personnel responded that a purchase was made using the "Walmart Pay app" on March 2 at 10:15 a.m. for "a red rain poncho, markers, and manila envelopes." The agents reviewed Walmart's security footage from that day and time, and they observed a large white male, wearing white sneakers, leave Walmart in a yellow Dodge Challenger. Agents then subpoenaed Walmart's transactional data and subscriber information for that specific purchase and obtained information including an email copy of the specific transaction and Robert Whipple's name, address, and telephone number that were associated with the Walmart Pay account. Agents also pulled Whipple's Tennessee driver's license records. They observed that Whipple's photograph, height, and weight resembled that of the robber on the banks' surveillance footage. The records also revealed that Whipple owned a yellow Dodge Challenger with license plate number CLN097.

Later that day, after a police officer observed Whipple's Challenger at a Red Roof Inn in Knoxville, FBI agents went to the hotel. The hotel clerk told them that Whipple was in room 354 and provided them with a key to that room. The agents then forced entry into the room, arrested Whipple, and secured the room while FBI Agent Leatham obtained a federal search warrant for the room. It was issued at 10:58 p.m., and it was executed that night. Agents arrested Whipple, impounded his car, and on March 10, obtained a search warrant for it. Agent

Leatham later testified that agents had probable cause to believe that Whipple used his car in the commission of his robberies, having observed Whipple via surveillance video enter that car after the Walmart purchase. Agent Leatham also testified that the agents did not want the car to be stolen or moved within the hotel parking lot because the lot was an open and unsecured space. The car was searched on March 11 pursuant to the warrant. Inside, agents found a red rain poncho, a brown wig-and-beard costume kit, a manila envelope with a demand note, an opened package of manila envelopes, black pens, a tan Dickies jacket, suspected crack cocaine, and bank receipts.

Agents seized Whipple's phone during his arrest and obtained a warrant for it on March 10. On March 11, Agent Leatham requested that the FBI Computer Analysis Response Team (CART) search Whipple's phone. On March 13, CART examiner, Leyton Adams attempted to access the phone. Examiner Adams removed both the SIM and SD cards from Whipple's phone and extracted data from them. Examiner Adams then found that the cellphone was passcode protected. After determining that he could not enter Whipple's phone himself, Examiner Adams requested that the FBI's Electronic Device Analysis Unit (EDAU) unlock the phone.[1] He submitted that request on March 13. Examiner Adams received an email from EDAU eight months later, on November 13, stating that he could send the phone to the Tennessee Valley Regional Computer Forensics Laboratory in Huntsville, Alabama for unlocking. Examiner Adams believed that the March to November timeline was not unusual, given the COVID-19 pandemic and staff shortages. On November 19, Examiner Adams received the cellphone's data and analyzed it.

b. Procedural History

A federal grand jury charged Whipple with bank robbery for the March 5 through 7 bank robberies. Whipple moved to suppress any evidence found as a result of the administrative

[1]Examiner Adams explained that too many incorrect attempts at unlocking a cellphone could lock or break the phone. And he stated that reprogramming the phone would likely wipe the data therein.

subpoena, the seizure of his car, and the search of his phone.[2] The motions were consolidated and referred to the magistrate judge for recommendation.

The magistrate judge recommended that the district court deny Whipple's motion to suppress the Walmart subpoena because it was reasonable in scope, seeking only one transaction and the identity of that purchaser's name, address, and telephone number. Whipple objected to the magistrate judge's report and recommendation both factually and legally. Factually, Whipple argued that the subpoena was too broad in scope. The district court explained that the agents sought a specific transaction and the Walmart-Pay-app account-holder's identifying information, not a general sweep of purchasing history. Therefore, the court overruled the factual objection. The court overruled the legal objection as well. Relying on the third-party doctrine, the court reasoned that Whipple voluntarily chose to put his information on the Walmart Pay app and to use the app to complete his in-store purchase. Whipple analogized his situation to that in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), but the district court noted that *Carpenter* was a narrow decision that did not call into question conventional surveillance tools or the use of business records, such as purchase receipts.

The magistrate judge also examined "whether the officers could seize and impound . . . Whipple's car without a warrant and hold the car for three days, while obtaining a search warrant for the car." Applying the automobile exception, the magistrate judge recommended that Whipple's motion to suppress be denied. Whipple objected. The district court agreed with the magistrate judge and concluded that the automobile exception applied to this situation. The district court reasoned that where there is probable cause to believe that a car is associated with criminal activity, a warrantless seizure is appropriate even if a warrant could have been obtained. The district court overruled Whipple's objection.

The magistrate judge recommended that Whipple's motion to suppress the evidence found in his cellphone be denied as well. The magistrate judge applied the reasonable-continuation rule, explaining that a more detailed search of a device may occur even months or years after the initial warrant's expiration, so long as the later search does not exceed the

[2]Whipple also moved to reopen his suppression hearing. That issue is not before this Court.

probable cause in the initial warrant. Whipple factually and legally objected to this recommendation. The district court agreed with the magistrate judge, stating that Whipple never had the opportunity to regain his phone after incarceration and that the months-later search of his phone was a continuation of the search from the initial warrant.

In sum, the district court overruled Whipple's objections to the magistrate judge's recommendation, adopted the relevant portions of the recommendation, and denied Whipple's motions. Whipple entered a guilty plea pursuant to a plea agreement, but he reserved the right to appeal the denial of his motions to suppress.

II. Legal Standard

When reviewing district court decisions on motions to suppress, we review factual findings for clear error and legal conclusions de novo. *United States v. Cleveland*, 907 F.3d 423, 430 (6th Cir. 2018). Because the district court denied the motions to suppress evidence, we review the evidence in a light most favorable to the government. *Id.*

III. Discussion

On appeal, Whipple raises three legal issues related to (1) the subpoena to Walmart, (2) the seizure and subsequent search of his car pursuant to a warrant, and (3) the unlocking of his cellphone after the initial warrant for it expired. We affirm.

a. Whipple's Specific Walmart Purchase

The entirety of Whipple's purchase history at Walmart was *neither* accessed *nor* sought by the administrative subpoena. However, Whipple argues that his Walmart-Pay-app purchasing history and subscriber information is subject to a reasonable expectation of privacy, meaning that the government needs a warrant before it can access that history.[3] This argument fails because the subpoena was narrowly tailored and because of our application of the third-party doctrine to Whipple's voluntary actions.

[3]Law enforcement officers never sought Whipple's entire purchase history, nor did they gain access to it. Instead, they sought a specific transaction associated with consumer information that was provided by the consumer on the Walmart application.

It is the defendant's burden to show that he had a reasonable expectation of privacy in the area searched or items seized. *United States v. Mathis*, 738 F.3d 719, 729 (6th Cir. 2013). The defendant must exhibit by his conduct (1) an actual, subjective expectation of privacy that (2) society is willing to recognize as reasonable. *Id.* (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)); *see also Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Whipple exhibits neither.

We recognize subjective expectations of privacy for placing trash in an opaque garbage bag. *California v. Greenwood*, 486 U.S. 35, 39 (1988). We also recognize the same when a defendant sets up elaborate security systems and high fences to obstruct street-level view into a property. *See Dow Chem. Co. v. United States*, 476 U.S. 227, 229, 237–39 (1986); *California v. Ciraolo*, 476 U.S. 207, 211 (1986). Furthermore, letters and emails have a subjective, as well as objective, expectation of privacy. *United States v. Warshak*, 631 F.3d 266, 285, 287–88 (6th Cir. 2010). The key to these subjective expectations of privacy is that those defendants showed their subjective expectations through conduct, doing more than just making statements during litigation about their expectations. *See Mathis*, 738 F.3d at 730.

Through his conduct, Whipple did not show that he had a subjective expectation of privacy in the purchase of "a red rain poncho, markers, and manila envelopes," which were used in the bank robberies, or in his subscriber information. He went to Walmart to make his purchase, *in-store*. And instead of using a more private purchasing method, Whipple chose to use the Walmart Pay app after he actively and voluntarily disclosed his name, address, and payment information to the Walmart Pay app.[4] Moreover, he was seen on Walmart surveillance video leaving the store in his not-so-subtle yellow Dodge Charger. We will not recognize Whipple's litigation statements as demonstrating his subjective expectation of privacy in his

[4]Post-*Carpenter*, at least four of our sister circuits have recognized that law enforcement can still use subpoenas to obtain a suspect's personal internet traffic data, i.e., internet protocol (IP) addresses—something that is arguably more private than subscriber information voluntarily stored on an application. *See, e.g., United States v. Soybel*, 13 F.4th 584, 592 (7th Cir. 2021); *United States v. Trader*, 981 F.3d 961, 967–68 (11th Cir. 2020); *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019); *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018). And one of our district courts has held that subscriber information is subject to subpoena, based on this reasoning and differentiating subscriber information from the geolocation data at issue in *Carpenter*. *United States v. Maclin*, 393 F. Supp. 3d 701, 708 (N.D. Ohio 2019) ("Subscriber information requires an individual's active participation."). We find the same here. Whipple's subscriber information was subject to the administrative subpoena for his active and voluntary disclosure of that information.

specific purchase and subscriber information when his actions do not indicate that he tried to keep this specific purchase private.

Nor do we find that society is willing to recognize as reasonable an expectation of privacy such as Whipple claims here. Walmart's tracking of purchasing history, particularly as related to one specific purchase, is an example of a business record, which is not subject to a reasonable expectation of privacy. *See, e.g.*, *United States v. Miller*, 425 U.S. 435, 440, 443 (1976). Therefore, the third-party doctrine still applies to business records that might reveal information such as telephone numbers and bank records, and *Carpenter* does not suggest otherwise. 138 S. Ct. at 2220, 2222.[5]

Whipple attempts to analogize his information to cellphone geolocation data, invoking the application of the third-party doctrine in *Carpenter*. There, the Supreme Court held that an individual maintains a reasonable expectation of privacy for information captured by his cellphone's geolocation. 138 S. Ct. at 2217. The Court explained that the automatic, *involuntary* disclosure of cellphone-geolocation data is not subject to the third-party doctrine, *id.* at 2217–18, 2219–20, but the Court was careful not to disturb the application of the traditional third-party doctrine to voluntary disclosures. *Id.* at 2219–20. In other words, what a person knowingly exposes to the public is not subject to Fourth Amendment-warrant protection. *See Katz*, 389 U.S. at 351; *Miller*, 425 U.S. at 443 (explaining that when someone reveals his affairs to another, he can no longer expect that such information will remain private).[6] This means that "[t]he

[5]Whipple cited a California Law Review article to suggest that society recognizes that purchasing history is subject to a reasonable expectation of privacy. Whipple's law review citation faces three problems. First, law enforcement officers sought information about one specific transaction. Second, precedent which binds us today demonstrates that specific purchasing history and subscriber information are akin to business records. *Carpenter*, 138 S. Ct. at 2220, 2222; *Miller*, 425 U.S. at 440, 443. Third, as we explained, Whipple's actions did not demonstrate that he had a legitimate expectation of privacy for this one specific transaction.

[6]There are numerous cases dealing with knowing and voluntary disclosures as related to the third-party doctrine: *Sanchez v. L.A. Dep't of Transp.*, 39 F.4th 548, 559–60 (9th Cir. 2022) (explaining the "knowing[] and voluntar[y]" disclosure of location data when the plaintiff used a third party's (Lyft's) e-scooter); *United States v. Gratkowski*, 964 F.3d 307, 311–13 (5th Cir. 2020) (explaining the affirmative actions required to partake in Bitcoin's blockchain and transactions on Coinbase, which diminish a reasonable expectation of privacy in the related information); *United States v. Caira*, 833 F.3d 803, 809 (7th Cir. 2016) (holding that "[b]ecause [the defendant] voluntarily shared his I.P. addresses with Microsoft, he had no reasonable expectation of privacy in those addresses"); *United States v. Bah*, 794 F.3d 617, 633 (6th Cir. 2015) (explaining that the information stored on a credit or debit card's magnetic strip is subject to a warrantless search because that data "is *intended* to be read by third parties") (emphasis in original) (citation omitted).

Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations." *Carpenter*, 138 S. Ct. at 2222.

Unlike what occurred in *Carpenter*, Whipple's information was not automatically disclosed by virtue of his shopping at Walmart. Here, agents asked Walmart about specific purchases of items such as those used in the bank robberies. Walmart security personnel identified a single purchase, which included a red rain poncho, markers, and manila envelopes—all items used by the bank robber. That purchase had been made just three days prior to the first bank robbery. In turn, agents subpoenaed Walmart's records for that specific purchase and identifying information related to the purchaser related to it. Walmart's business records showed Whipple as the man behind the purchase, and identified information such as his name and address.[7] Whipple had voluntarily disclosed information to Walmart, via the Walmart-Pay-app. Moreover, he was seen on surveillance footage at Walmart. *See United States v. Knotts*, 460 U.S. 276, 282–83 (1983) (explaining that no expectation of privacy extends to visual observation from public places of one's whereabouts). Whipple's actions were not demonstrative of a legitimate or reasonable expectation of privacy. Therefore, the third-party doctrine applies, and the agents did not violate Whipple's Fourth Amendment rights by subpoenaing Walmart's records for the specific purchase and subscriber information related to it.[8]

---

[7]Whipple also argues that the authorities *could have* gone through the entirety of Whipple's purchasing history at Walmart, citing *Kyllo v. United* States, 533 U.S. 27, 38 (2001). This argument is inapposite for two reasons. First, the assertion only tangentially supports Whipple's argument. The thermal imaging at issue in *Kyllo* could have revealed more than heat signatures. Indeed, there was no way to limit the scope of what the thermal imaging would reveal. Here, the authorities limited what they were looking at: Whipple's single transaction regarding items like those used in the bank robberies. Second, and relatedly, the authorities did not go through all of Whipple's purchasing history. They narrowed the subpoena and the information collected from it to a specific transaction tied to a specific account.

[8]Whipple alternatively argues in briefing that even if law enforcement could use a subpoena to get Whipple's purchasing history and subscriber information, they did not follow the proper procedure. Blue Br., Pg. 31. Here, Whipple relies on the Right to Financial Privacy Act (RFPA). *Id.* In relevant part, the RFPA requires that a government authority only obtain "financial records" by administrative subpoena of customers from "financial institution[s]" if the records are "reasonably described" and they are disclosed to the customer who has an opportunity to quash the subpoena. 12 U.S.C. § 3402(2) & 3405. Whipple faces a major problem: he does not offer any evidence that Walmart is a financial institution for purposes of the RFPA or that his transaction and subscriber information were financial records protected by RFPA. *See* 12 U.S.C. §3401(1), (2). Therefore, this alternative argument fails.

b. Whipple's Car

Whipple argues that the warrantless seizure of his car renders the evidence found within it inadmissible. Whipple's car was impounded by FBI agents and kept by for three days before they procured a warrant and searched the car. Whipple's arguments fail for one reason: the automobile exception to the warrant requirement applies to this situation.[9]

The automobile exception relieves law enforcement officers of the requirement to obtain a warrant before seizing and conducting a search of an automobile where probable cause exists to believe that evidence of a crime will be found in the car. *See Chambers v. Maroney*, 399 U.S. 42, 48 (1970) ("[A]utomobiles and other conveyances may be searched without a warrant . . . provided that there is probable cause to believe that the car contains articles that the officers are entitled to seize."); *Cardwell v. Lewis*, 417 U.S. 583, 593–95 (1974) (holding that the warrantless seizure of a car from a public parking lot, and subsequent impoundment following the defendant's arrest, was "not unreasonable" because there was probable cause that the car constituted evidence of a crime); *United States v. Smith*, 510 F.3d 641, 647–48 (6th Cir. 2007). Ready mobility is one of the principal bases for the automobile exception. *California v. Carney*, 471 U.S. 386, 391 (1985). A car's ready mobility creates exigent circumstances that make "rigorous enforcement of the warrant requirement . . . impossible." *South Dakota v. Opperman*, 428 U.S. 364, 367 (1976). Furthermore, cars have a reduced expectation of privacy because they are subject to "pervasive [travel] regulation." *Id.* at 392.

Here, agents had probable cause to believe that Whipple used his yellow Charger during the bank robberies and that it contained evidence of those crimes. After all, he was seen leaving Walmart, via surveillance footage, in his Charger after purchasing the materials he used to commit the robberies. *See Cardwell*, 417 U.S. at 592, 594–95. Even, as here, when a car has been immobilized because the owner can no longer drive it, the justification for a warrantless seizure of a car does not vanish. *Michigan v. Thomas*, 458 U.S. 259, 261 (1982). What matters

[9]Warrantless searches are presumptively unreasonable. *United States v. Place*, 462 U.S. 696, 701 (1983). However, there are exceptions to that presumption. *See, e.g.*, *Missouri v. McNeely*, 569 U.S. 141, 148–49 (2013) (exigent circumstances); *Maryland v. Buie*, 494 U.S. 325, 333–336 (1990) (warrantless protective sweeps); *Cardwell v. Lewis*, 417 U.S. 583, 594–95 (1974) (automobile exception).

is that the agents had probable cause to search and seize Whipple's car. *Id.*; *Cardwell*, 417 U.S. at 595 ("Assuming that probable cause . . . exist[s], we know of no case or principle that suggests that the right to search on probable cause and the reasonableness of seizing a car under exigent circumstances are foreclosed if a warrant was not obtained at the first practicable moment."); *United States v. Hofstatter*, 8 F.3d 316, 322 (6th Cir. 1993).[10] The district court did not err in holding that both the seizure and the search of the car were lawful.

c. Whipple's Cellphone

Whipple argues that because law enforcement did not complete the search of his phone within fourteen days of the initial search warrant for the cellphone, any evidence found within the phone after the expiration date is inadmissible against him. Whipple's arguments fail because a warrant's execution date does not apply to off-site investigation and analysis of a cellphone's contents. *Cleveland*, 907 F.3d at 430–31.

The "federal rules of criminal procedure give law enforcement the authority to conduct searches of lawfully seized phones after they are seized." *Id.* (quoting *United States v. Castro*, 881 F.3d 961, 969 (6th Cir. 2018)). "The time for executing the warrant . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Fed. R. Crim. P. 41(e)(2)(B). "A substantial amount of time can be involved in the forensic imaging and review of information" on cellphones. *Cleveland*, 907 F.3d at 430 (quoting Fed. R. Crim. P. 41, advisory committee's note to 2009 amendments). In other words, law enforcement is allowed to decode or otherwise analyze data on a seized phone at a later time, even after the initial warrant expires. *Id.* at 431 (citing *United States v. Huart*, 735 F.3d 972, 974 n.2 (7th Cir. 2013)).

[10]Whipple also argues that *United States v. Place*, 462 U.S. 696 (1983), supports his argument that the police should not have warrantlessly seized his car. His reliance on *Place* is misplaced. There, the Court held that the extended seizure of baggage (or a container) *without justification* gave rise to a Fourth Amendment violation. *Place*, 462 U.S. at 709–10. Here, there was justification—probable cause—to seize Whipple's car, and law enforcement may seize an item based on probable cause and later obtain a search warrant for it. *United States v. Respress*, 9 F.3d 483, 486 (6th Cir. 1993). Even after attempting to analogize his situation to Fourth Amendment container cases, Whipple cannot succeed with this argument.

Here, the agents seized Whipple's phone on March 7 while arresting Whipple, and obtained a warrant for his cellphone on March 10. The search was initiated on March 11, and the cellphone was sent to CART on March 13 for examination. *Contra United States v. Sykes*, 65 F.4th 867, 878 (6th Cir. 2023) (explaining that a 31-day delay between a phone's seizure and obtaining a search warrant was unreasonable when the defendant had a possessory interest in the cellphone, and agents failed to exercise diligence (citing *United States v. Pratt*, 915 F.3d 266, 272 (4th Cir. 2019))). After removing the phone's SD and SIM cards, the examiner was not able to crack the cellphone's passcode, so he contacted the FBI EDAU to unlock the cellphone. During the height of the COVID-19 pandemic and staff shortages, the EDAU did not respond until November 13. Ultimately, the cellphone was searched and returned to the examiner on November 19. Although the warrant for Whipple's phone expired on March 24, law enforcement officers began searching the cellphone on March 13, well before the expiration date. Those officers did not unreasonably delay in obtaining a warrant, nor did they delay after obtaining a warrant. Rather, law enforcement officers acted reasonably in this situation. *Cf. Cleveland*, 907 F.3d at 430–31.[11] The district court did not err in denying the motion to suppress the evidence from the cellphone.

CONCLUSION

For the foregoing reasons, we **AFFIRM** the district court's denial of Whipple's motions to suppress evidence.

[11]Further, Whipple had virtually no possessory interest in his phone while he was incarcerated. *Sykes*, 65 F.4th at 879. When there is a reasonable belief that a cellphone contains evidence of a crime, there is greater justification for retention of that cellphone, pursuant to a valid warrant. *Id.* And when there are reasonable excuses for delaying cell-phone-data extraction, searches after the expiration of a warrant have more justification. *Id.*