NOT RECOMMENDED FOR FULL-TEXT PUBLICATION
File Name: 16a0006n.06

Case No. 14-4212

FILED
Jan 07, 2016
DEBORAH S. HUNT, Clerk

**UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT**

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

CHRISTOPHER D. RARICK,

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF OHIO

OPINION

BEFORE: BATCHELDER, GIBBONS, and WHITE, Circuit Judges.

JULIA SMITH GIBBONS, Circuit Judge. Christopher Rarick appeals the district court's denial of his motion to suppress evidence of child pornography found on his smartphone, which was searched pursuant to a warrant after Rarick was arrested for obstructing official business and driving with a suspended license. Rarick challenges the particularity of the warrant and the manner in which it was executed. We affirm.

I.

On February 14, 2013, Christopher Rarick was stopped by Ashland City Police Officer Kim Mager outside a Cheap Tobacco store in Ashland, Ohio, after Officer Mager conducted a LEADS inquiry on the car Rarick was driving and determined the registered owner of the vehicle, Rarick, had a suspended license. Accordingly, Officer Mager stopped Rarick to determine whether he was the registered owner and was thus driving with a suspended license. During the stop, Rarick became argumentative: he challenged the officer's authority to ask his name or run his license plate, and he refused to produce his driver's license, insurance information, or vehicle registration. At some point, Rarick removed his smartphone from his pocket, held it up, approached the officer, and stated that he was recording her. The officer took the phone, placed it on the trunk of Rarick's car, and ordered Rarick to remain in his car while she conducted her work. Rarick grabbed his phone from the trunk and retreated to the passenger seat of his car, whereupon the officer approached him to find out what he was doing. The officer saw that Rarick was manipulating his phone, and she ordered him to stop and to put his hands on the dashboard. Saying that he wanted to record what was happening, Rarick continued to manipulate his phone. Eventually he put the phone down and placed his hands on the dashboard. After backup arrived, Rarick was arrested and taken to jail, where he was cited for obstructing official business and driving with a suspended license. His cell phone—a black Samsung Nexus S 4G model SPH-D720—was seized as evidence.

Rarick refused to consent to a search of his phone. Lieutenant Joel Icenhour then filed an affidavit for a search warrant. In the affidavit, Icenhour stated that he had good cause to believe that evidence relating to the offense of obstructing official business, a violation of Ohio Revised Code § 2921.31, was likely stored in a digital format on Rarick's phone, which had been taken from Rarick at the time of his arrest. Icenhour's affidavit stated that "[t]his belief is based on a traffic stop conducted by Officer Kimberly Mager." Search Warrant Aff. 1, ECF No. 19-1. An Ohio state judge issued a warrant that authorized the search and seizure of, among other things, "[a]ll information within" Rarick's phone, "including but not limited to machine-readable data, all previously erased data, and any personal communications"; "[a]ny and all electronic data contained in the device's memory as well as on other internal, external or removable media to include but not necessarily limited to . . . images, voice memos, photographs, [and] videos"; and "[a]ll other fruits and instrumentalities of crime at the present time unknown." Search Warrant 1–2, ECF No. 19-2.

Icenhour then executed the search warrant by connecting Rarick's phone to a computer that was running Susteen Secure View 3 forensic cell phone data recovery software.[1] Icenhour downloaded the phone's data onto his computer. After the data had been downloaded, Icenhour testified, "a little box show[ed] up" on his computer screen, saying "Do you want to view the report?" Hr'g Tr. 28:24–25, Oct. 15, 2013, ECF. No. 54. Icenhour clicked "View the report," and his computer displayed the downloaded data, which included technical information about the phone itself, call logs, contacts, pictures, audio files, video files, and other data. Hr'g Tr. 28:25–29:8. The report displayed thumbnail images of the pictures and video files; for the video files, the thumbnail image was the first frame of the video. Icenhour acknowledged that it was possible to get an idea of the contents of the pictures and video files by looking at the thumbnails. Icenhour looked for video and audio files because Rarick had told the arresting officer that he was recording her. As Icenhour scrolled down into the section containing video files, he scrolled past the pictures, and he could see from the thumbnails that the pictures contained child pornography. Icenhour then scrolled further down, where he spotted a video with a thumbnail that he thought looked like a beige wall. He testified that he opened the video because he thought that the thumbnail might depict the wall of the Cheap Tobacco store where the stop occurred. It did not—it too contained child pornography.

At this point, Icenhour shut off the video and went to tell his chief of police what he had found. After consulting with the prosecutor's office, they applied for and received a second

[1] The first time Icenhour attempted to execute the warrant, he was thwarted because he did not have the phone's passcode. Icenhour subsequently obtained the passcode from Rarick's father, apparently with Rarick's consent. If Icenhour had been unable to obtain the passcode, he would have sent the phone to the Ohio Bureau of Criminal Investigation to be unlocked.

warrant, this time asserting probable cause to search for evidence of child pornography and several related offenses under Ohio law. Executing the second warrant, Icenhour found numerous pictures and videos containing child pornography, many of which appeared to have been taken with Rarick's phone. The police then arrested Rarick and applied for and received a third search warrant for his vehicle and residence.

A federal grand jury indicted Rarick on two counts of exploiting children in violation of 18 U.S.C. § 2251(a) and one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). Arguing, *inter alia*, that the first search warrant was unconstitutionally broad and had been executed in an unreasonable manner, Rarick moved to suppress all of the evidence found on his smartphone and the fruits obtained from the search. The district court denied his motion. Rarick then pled guilty but preserved his right to appeal the district court's denial of his motion to suppress. The court ordered Rarick incarcerated for concurrent sentences of 188 months on each of the two exploiting-children counts and a concurrent sentence of 120 months on the child-pornography count.

After entry of judgment by the district court, Rarick timely appealed. He argues that the first search warrant failed the Fourth Amendment's particularity requirement and that the manner of the search was unreasonable and unconstitutional.

II.

Where the issue on appeal is a district court's denial of a motion to suppress evidence, we review the district court's findings of fact for clear error and its legal conclusions *de novo*. *United States v. Quinney*, 583 F.3d 891, 893 (6th Cir. 2009). A district court's determination of the particularity of a search warrant is reviewed *de novo*. *United States v. Richards*, 659 F.3d 527, 536 (6th Cir. 2011) (citing *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001)). We consider the evidence in the light most likely to support the district court's denial of the motion to suppress. *United States v. Pritchett*, 749 F.3d 417, 435 (6th Cir. 2014) (quoting *United States v. Adams*, 583 F.3d 457, 463 (6th Cir. 2009)).

III.

A.

The Fourth Amendment generally requires police to obtain a warrant before searching the digital information stored on a cell phone, even when a cell phone is seized incident to arrest. *Riley v. California*, 134 S. Ct. 2473, 2493 (2014). The new rule established in *Riley* applies to cases still pending on direct review, such as Rarick's. *See Griffith v. Kentucky*, 479 U.S. 314, 328 (1987). The Fourth Amendment further requires that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement stems from the Founders' concern with "curb[ing] the abuses of general warrants, devices which provided British officers with broad discretion to search the homes of citizens of the Colonies for evidence of vaguely specified crimes." *Ellison v. Balinski*, 625 F.3d 953, 958 (6th Cir. 2010). The particularity requirement encompasses two issues: "whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take; and . . . whether the category as specified is too broad in the sense that it includes items that should not be seized." *Richards*, 659 F.3d at 537 (quoting *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999)).

Rarick does not dispute the existence of probable cause supporting the first search warrant to the extent that the warrant authorized obtaining evidence of his interaction with the police officer outside the Cheap Tobacco store, for which he was charged with obstructing official business. Rather, he argues that the first search warrant was overly broad because it neither specified the particular electronic evidence sought from the phone nor the particular crime to which the evidence was connected. Although it is true that the text of the warrant did not contain that information, "[t]he particularity requirement may be satisfied through the express incorporation or cross-referencing of a supporting affidavit that describes the items to be seized, even though the search warrant contains no such description." *Richards*, 659 F.3d at 537 (citing *Baranski v. Fifteen Unknown Agents of the Bureau of Alcohol, Tobacco and Firearms*, 452 F.3d 433, 439–40 (6th Cir. 2006) (en banc)). Here, the warrant referred to the supporting affidavit that had been filed by Icenhour. The first sentence of the warrant was "WHEREAS there has been filed with me an affidavit." Search Warrant 1. The warrant then stated, referring to the following paragraphs that named the types of data to be searched, "[t]hese are, therefore, to command you" to search Rarick's cell phone. Search Warrant 1. This language constitutes a sufficient cross-reference of the affidavit. *See Groh v. Ramirez*, 540 U.S. 551, 557–58 (2004).

The question, then, is whether the information contained in the affidavit, to which the warrant referred, was enough to satisfy the particularity requirement. "[T]he degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought." *Greene*, 250 F.3d at 477 (quoting *United States v. Ables*, 167 F.3d 1021, 1033 (6th Cir. 1999)). The description of the things to be seized should, however, be "as specific as the circumstances and the nature of the activity under investigation permit." *Richards*, 659 F.3d at 537 (quoting *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001)). In the context of searches of electronic devices, while recognizing the inherent risk that criminals can easily "hide, mislabel, or manipulate files to conceal criminal activity," we must also take care not to give the Government free rein to essentially do away with the particularity requirement by allowing it to examine every file on the device. *Richards*, 659 F.3d at 538 (quoting *United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011)).

Rarick objects, among other things, to the warrant's expansive language authorizing the search of "any and all electronic data" and "any and all communications," and the warrant's failure to specify the date of the creation of the video at issue. As he sees it, this language swept far more broadly than "the circumstances and the nature of the activity under investigation permit[ted]." *See Richards,* 659 F.3d at 537 (quoting *Leis,* 255 F.3d at 336).

In *Richards*, we held that the search warrant for evidence regarding a child pornography website was not overbroad where it authorized a search beyond the file directory on the server where the evidence was contained. 659 F.3d at 541. There, the broad search of the entire server was necessary because the agents did not know how, where, or in what quantity the evidence would be stored on the server. *Id.* The warrant in *Richards* was specific as to what the agents were searching for and limited the items to be seized to the content of the pornographic website, and business records, email correspondence, and other files related to the website. *Id*. at 535. Here, certain portions of the warrant were not limited to files specific to what the government was searching for—a video or image taken by Rarick on the date and around the time of his arrest. For instance, the warrant authorized Icenhour to examine "all GPS data such as but not limited to locations, waypoints, favorite locations, points of interest and routes of travel." Search Warrant 1. However, the remedy in this circuit is not suppression of all of the items seized under the warrant, but rather severance of the infirm portions "from the remainder which passes constitutional muster." *United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) (quoting *United States v. Blakeney,* 942 F.2d 1001, 1027 (6th Cir. 1991)); *United States v. Cook*, 657 F.2d 730, 735 (5th Cir. 1981)) ("[I]t would be harsh medicine indeed if a warrant which was issued on probable cause and which did particularly describe certain items were to be invalidated in toto merely because the affiant and the magistrate erred in seeking and permitting a search for other items as well." (citation omitted)).[2] Certain portions of the warrant, such as the portion authorizing seizure of "images" and "videos," were specifically targeted to what the officers had probable cause to search, and, therefore, satisfy the particularity requirement. *See* Search Warrant 1. No evidence offered against Rarick was seized pursuant to the overbroad portions of the warrant. Rather, as will be discussed in further detail below, Icenhour executed the warrant as though the infirm portions had been excised, seizing only "images" and "videos" that appeared to be related to the incident at the Cheap Tobacco store. Thus, the district court did not err in denying Rarick's motion to suppress.

B.

Rarick further argues that the manner of the search was unconstitutional because Icenhour did not begin his search by focusing on the places where the evidence was most likely to be. Traditionally, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant—subject of course to the general Fourth Amendment protection 'against unreasonable searches and seizures.'" *Dalia v. United States*, 441 U.S. 238, 257 (1979) (footnote omitted). In the context of searches of electronic devices, this court and other courts have recognized that the methodology of a search matters in determining whether it is constitutionally reasonable. *See, e.g.*, *Richards*, 659 F.3d at 538–39; *Stabile*, 633 F.3d at 237–40; *United States v. Burgess*, 576 F.3d 1078, 1094–95 (10th Cir. 2009). While it is true that "[a]s the description of . . . places and things becomes more general . . . the search method must be tailored to meet allowed ends," eventually, "there may be no practical substitute" for actually examining most or even all potential repositories, particularly when the search is for image files. *Richards*, 659 F.3d at 539

[2] The dissent urges us to reverse for want of probable cause. However, Rarick has never argued, either in the district court or here, that there was no probable cause to arrest for or search for evidence of a violation of Ohio Revised Code § 2921.31.

(quoting *Burgess*, 576 F.3d at 1094). Due to "the practical difficulties inherent in implementing universal search methodologies," most federal courts, including this circuit, have taken the approach of determining the reasonableness of the search on a case-by-case basis. *Id.* at 538. For instance, in *Burgess*, the agent searching the defendant's computer used the "preview feature" to examine reduced size photos in search of "trophy photos" evidencing drug use. *Burgess*, 576 F.3d at 1084. The Tenth Circuit held that this search methodology was reasonable because the agent's search was properly targeted to search for "trophy photos," he immediately stopped his search when he found evidence of a second crime, which was outside the scope of the warrant, and it was likely, given the risk of deceptive labelling of file names, that he would have eventually found the evidence of that second crime using an alternative search method. *Id.* at 1094–95. In the end, there was "no practical substitute" for this methodology. *See id.* at 1094.

While Rarick would have us declare that, to be reasonable, the search here should have at least been commenced by using a date filter before expanding the search, we will not get involved in the minutiae of determining specifically what methodologies should be taken, but will rather examine whether the search executed under the facts of this case was reasonable. Searching by date may have been *one* reasonable search methodology, but it was not the *only* reasonable one. The facts of this case lead us to conclude that the search conducted by Icenhour was executed in a reasonable manner. Though, under certain portions of the warrant, Icenhour was given leave to search virtually the entire contents of Rarick's phone, the record establishes that he did not do so. Rather, he targeted his search to where he reasonably believed the recording was most likely to be found—among the audio and video files. Icenhour testified that he scrolled through the thumbnails of the files on Rarick's phone. Though he observed the child pornography photos during this search, he continued to scroll through the files until he found an image of a beige wall that he thought could be the start of the video recorded outside of the Cheap Tobacco store. Rather than continue to search after discovering that this beige wall was a part of a video containing more pornography, he turned off the video and proceeded to get a second warrant. Although the recording could have been found by first searching for data recorded on February 14, 2013, the date of Rarick's arrest, Icenhour's approach of searching by scrolling through all of the thumbnails, rather than just those on the date of Rarick's arrest, and taking care not to closely examine more than the target of the search warrant was not unreasonable.

IV.

For the reasons explained above, we affirm the district court's denial of Rarick's motion to suppress.

ALICE M. BATCHELDER, Circuit Judge, concurring in part and dissenting in part. Had we considered this case as it was framed for us on appeal, it would have led not only to the conclusion that the warrant was overbroad, but also that it lacked probable cause and that no amount of trimming could save it. I therefore respectfully concur in part and dissent in part.

I.

It is true that severing the "infirm portions" of a warrant is an acceptable legal remedy when dealing with an overbroad warrant. But the government never made this argument. Instead, it contended that, even if the warrant were overbroad, suppression would be inappropriate because Icenhour's search fell within the good faith exception set forth in *United States v. Leon*, 468 U.S. 897 (1984). Our next step should have been to consider whether the *Leon* exception applies here. *See Richards*, 659 F.3d 527, 542 (6th Cir. 2001). A glance at *Leon* reveals that the good-faith exception does not apply when an officer relies "on a warrant based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'" *Leon*, 468 U.S. at 923 (quoting *Brown v. Illinois*, 422 U.S. 590, 611 (1975) (Powell, J., concurring in part)).

The majority was able to avoid discussing good faith, and thus the latent probable cause issue, only by doing the very thing it finds objectionable in this dissent: raising an argument that was not before us. And it seems to me more appropriate to consider an argument that was raised, albeit without much elaboration, than one that was not raised at all.

II.

A review of the record reveals that probable cause was sorely lacking in this case. Officer Icenhour's affidavit notes that the offense at issue is obstructing official business in violation of Ohio Revised Code § 2921.31. "[A] police officer is expected to tolerate a certain level of uncooperativeness, especially in a free society in which the citizenry is not obliged to be either blindly or silently obeisant to law enforcement," and the obstruction must therefore be more than "mere argument." *State v. Stayton*, 709 N.E.2d 1224, 1227 (Ohio Ct. App. 1998). Thus, with the exception of fighting words, "a citizen's verbal assault on a police officer does not, standing alone, constitute criminal conduct." *Id.*[1] Further, "refusal to cooperate with police and provide identification upon request does not constitute obstructing official business." *State v. Prestel*, No. 20822, 2005 WL 2403941, at *2 (Ohio Ct. App. Sept. 30, 2005); *see also Cleveland Heights v. Lewis*, 933 N.E.2d 1146, 1151 (Ohio Ct. App. 2010).

Recording the police is of course an "affirmative act," but it is fully legal in Ohio. *See* Ohio Rev. Code § 2933.52(B)(4). And there is no indication that Rarick's recording hampered Officer Mager in any way. Allowing the police to arrest someone for obstructing official business simply because that person was legally recording them goes against the plain language of § 2933.52(B)(4) and raises serious First Amendment concerns. *See Am. Civil Liberties Union of Illinois v. Alvarez,* 679 F.3d 583, 607 (7th Cir. 2012).

In any event, the state would still have had to show that Rarick acted "with an intent to obstruct the officers," and that he "succeeded in actually hampering or impeding them." *State v. Crowell*, 938 N.E.2d 1115, 1117–18 (Ohio Ct. App. 2010) (internal quotation marks omitted). But nothing in the record before us suggests that Rarick in any way interfered with the performance of Officer Mager's duties or that the video evidence would have shown as much.[32]

[1] Rarick's statement "I have killed people" was perhaps threatening, but it did not constitute fighting words. *See Greene v. Barber*, 310 F.3d 889, 896 (6th Cir. 2002) (citing *Houston v. Hill*, 482 U.S. 451, 462 (1986)).

[2]

[3] That Rarick recorded the interaction appears, if anything, to have helped speed along the arrest, as "Christopher's demeanor changed once he got the phone in record mode" and he was "subsequently arrested."

When a warrant lacks probable cause, the applicability of "the [good faith] exception turns on whether a reasonable officer would know that the affidavit failed to establish probable cause." *United States v. Helton*, 314 F.3d 812, 824 (6th Cir. 2003). Under *Leon*, we presume that "officers . . . have a reasonable knowledge of what the law prohibits." *Leon*, 468 U.S. at 919 n.20. "This burden is even greater when the officer executing the warrant prepares the affidavit in support of the warrant, drafts the warrant, and applies for the warrant." *United States v. Watson*, 498 F.3d 429, 433 (6th Cir. 2007). Ohio's obstruction law applies to the workaday interactions of police officers with the public, and its meaning is well settled. Officer Icenhour should have known that this warrant lacked probable cause.

III.

Having reached this conclusion (a conclusion that the majority does not disagree with except on procedural grounds), it is manifest that no amount of trimming can save the warrant. The evidence should have been suppressed. From the majority's holding to the contrary I respectfully dissent.