In the

United States Court of Appeals

For the Seventh Circuit

No. 15-2443

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DAMIAN PATRICK,

Defendant-Appellant.

Appeal from the United States District Court
for the Eastern District of Wisconsin.
No. 13-CR-234 — **Rudolph T. Randa**, *Judge*.

ARGUED MAY 24, 2016 — DECIDED NOVEMBER 23, 2016

Before WOOD, *Chief Judge*, and EASTERBROOK and KANNE, *Circuit Judges*.

EASTERBROOK, *Circuit Judge*. Police in Wisconsin arrested Damian Patrick while he was in a car on a public street and found him armed. That led to this federal prosecution, because Patrick's criminal record made it unlawful for him to possess firearms. 18 U.S.C. §922(g)(1). The district court denied his motion to keep the gun out of evidence. 2015 U.S.

Dist. LEXIS 1421 (E.D. Wis. Jan. 7, 2015), approving a magistrate judge's recommendation, 2014 U.S. Dist. LEXIS 179522 (E.D. Wis. Sept. 30, 2014). Patrick pleaded guilty but reserved the opportunity to contest the validity of his arrest, and thus the validity of the gun's seizure. He now appeals from the 57-month sentence he received.

Patrick was serving a term of parole that followed his release from state prison. He did not comply with the conditions of his release, and a warrant was issued for his arrest. (He does not contest that warrant's validity.) In an effort to find Patrick, Milwaukee's police obtained a second warrant, which authorized them to locate Patrick using cell-phone data. Patrick's cell phone revealed his location, which enabled the police to find him.

Patrick attempts to undermine the validity of the location-tracking warrant by contending that his person was not contraband or the proceeds of a crime, and that it therefore was off limits to investigation. That sounds like an attempt to resurrect the "mere evidence" doctrine that the Supreme Court disapproved in *Warden v. Hayden*, 387 U.S. 294 (1967). *Hayden* authorized the use of warrants to get evidence to locate a wanted person. See also *Steagald v. United States*, 451 U.S. 204 (1981) (search warrant to enter house to look for person to arrest). Police were entitled to use a warrant to obtain data that would help them track down Patrick's location.

Indeed, they were entitled to arrest him without a warrant of any kind, let alone the two warrants they had. *United States v. Watson*, 423 U.S. 411 (1976), holds that probable cause alone is enough for an arrest in a public place. A warrant is necessary only when the police need to enter a private area to capture the wanted person. See *Payton v. New York*,

445 U.S. 573 (1980). Because Patrick was visible to the general public, he did not have any privacy interest in his location at the time.

More: the Supreme Court recently held that a valid arrest warrant precludes the suppression of evidence seized in an arrest, even if the arrest was set in motion by officers who had neither probable cause nor knowledge of the warrant. *Utah v. Strieff*, 136 S. Ct. 2056 (2016). *Strieff* tells us that, if the police had stopped Patrick's car for no reason at all and learned only later that he was a wanted man, the gun would have been admissible in evidence. The officers who nabbed Patrick, by contrast, had both probable cause to believe that he was a fugitive from justice and knowledge of the arrest warrant. The gun cannot be less admissible than in *Strieff*, even if we knock out the means used to track his location.

Because Patrick was arrested in a public place, and the arrest was supported by both probable cause and a valid arrest warrant that had been issued before any effort to learn his location (an effort that therefore could not "taint" the arrest in the parlance of the exclusionary rule), we need not resolve some difficult issues posed by a fact that came to light while the case was in this court. After Patrick filed his opening brief, the prosecutor revealed that Patrick's location had been pinned down using data from a cell-site simulator. That device (often called a Stingray, the trademark of one brand) pretends to be a cell-phone access point and, by emitting an especially strong signal, induces nearby cell phones to connect and reveal their direction relative to the device. Here is a description from the Department of Justice:

> Cell-site simulators … function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices

> in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.
>
> A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.
>
> By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. §3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015) at 2. See also the Wikipedia entry at <en.wikipedia.org/wiki/Stingray_phone_tracker>.

If the Department's description is accurate (a question not explored in this litigation) law-enforcement officials get the

same sort of information that a phone company could provide using its own facilities, and they get it in real time rather than waiting for the phone company to turn over data. But instead of collecting information on just one person, as the warrant in this proceeding entitled the police to learn Patrick's location, a cell-site simulator collects the relative location of *everyone* whose phone is induced to connect to the simulator—though it may discard that information before alerting officials to the presence of the sought-after person (just as the phone company, which has location data about all of its customers, would disclose only one person's location).

One potential question posed by use of a cell-site simulator would be whether it is a "search" at all, or instead is covered by *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Knotts*, 460 U.S. 276 (1983). The former holds that a pen register is not a search because it reveals the making of a call, and the number called, but not the call's communicative content. The latter holds that the use of a beeper is not a search, because it reveals a suspect's location but nothing else. Recent decisions such as *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc), and *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), apply these principles to hold that tracking a person via data from phone companies is not a search within the scope of the Fourth Amendment. (*Graham* involved historical cell-tower location information and *Carpenter* involved "transactional records" from phone companies, so both cases dealt with the sort of information covered by the location warrant in this proceeding.) Police freely use databases, containing information such as the addresses associated with automobile license plates and persons licensed to drive, to track down suspects; they search

trash for credit card receipts showing where he made purchases; they consult a suspect's relatives and friends (and sometimes his enemies) to learn his whereabouts; no one thinks that those methods require a search warrant.

A contrary line of argument analogizes cell-site simulators to GPS locators, which are treated as searches when police enter private property to install them, see *United States v. Jones*, 132 S. Ct. 945 (2012), and may be searches when used for extended durations even if installed with a vehicle owner's consent, *id*. at 954–64 (concurring opinions of Sotomayor and Alito, JJ.). If a cell-site simulator is like a GPS tracker, and if the approach of the concurring opinions in *Jones* is adopted, then it would be necessary to know how long the police used a simulator while searching for Patrick and just how accurate is the location information it provides. (Is it information that leaves uncertainty about where in several city blocks a suspect may be, such as the beeper in *Knotts*, or is it closer to the precise location supplied by a GPS tracker?) Cf. *Kyllo v. United States*, 533 U.S. 27 (2001) (thermal image of the inside of a house is a search, given a person's strong privacy interest in his dwelling).

The United States has conceded for the purpose of this litigation that use of a cell-site simulator is a search, so we need not tackle these questions. The parties join issue, however, on the significance of the fact that police did not reveal to the state judge who issued the location-tracking warrant that they planned to use a cell-site simulator—indeed, implied that they planned to track him down using his phone company's data. Patrick says that leaving the judge in the dark (perhaps misleading the judge by omitting a potentially material fact) makes the location-tracking warrant invalid.

This poses the question whether a judge is entitled to know how a warrant will be executed.

The Fourth Amendment requires that warrants be based "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Supreme Court stated in *Dalia v. United States*, 441 U.S. 238, 256 (1979), that neither constitutional text nor precedent suggests that "search warrants also must include a specification of the precise manner in which they are to be executed." The manner of search is subject only to "later judicial review as to its reasonableness." *Id.* at 258. And the Justices added in *Richards v. Wisconsin*, 520 U.S. 385 (1997), that courts cannot limit a warrant so as to foreclose a particular means of execution. In *Richards* the police sought a warrant that would have authorized a no-knock entry to conduct a search. The judge denied that request but issued a warrant for a regular search. After the police conducted a no-knock entry anyway, the Court held that this was proper because it was reasonable to carry out the search that way under the circumstances.

This means that the police could have sought a warrant authorizing them to find Patrick's cell phone and kept silent about how they would do it. Or affidavits and the warrant itself might have said that "electronic means that reveal locations of cell phones" will be used. Professor Kerr has concluded from *Dalia* and *Richards*, and other considerations, that the Fourth Amendment *forbids* judges to attempt to regulate, *ex ante*, how a search must be conducted, and confines the judiciary to *ex post* assessments of reasonableness. Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1260–71 (2010).

We can imagine an argument that it will often be unreasonable to use a cell-site simulator when phone company data could provide what's needed, because simulators potentially reveal information about many persons other than the suspects. (The contrary argument is that data from simulators is current, while data relayed through phone-companies' bureaucracies may arrive after the suspect has gone elsewhere.) But if the problem with simulators is that they are too comprehensive, that would not lead to suppression—though it might create a right to damages by other persons whose interests were unreasonably invaded. Patrick is not entitled to invoke the rights of anyone else; suppression is proper only if the defendant's own rights have been violated. See, e.g., *United States v. Payner*, 447 U.S. 727 (1980).

Patrick contends that, even if *ex ante* authorization of the method is unnecessary, the police must be candid with the judiciary when they mention potential methods of executing a search warrant. He seeks, at a minimum, a remand to explore those questions, after the fashion of a *Franks* hearing (see *Franks v. Delaware*, 438 U.S. 154 (1978)), at which the court would decide whether the warrant still would have issued if the affidavits had been more forthcoming.

But for the reasons given earlier we conclude that the answers do not control this appeal. A person wanted on probable cause (and an arrest warrant) who is taken into custody in a public place, where he had no legitimate expectation of privacy, cannot complain about how the police learned his location. Recall that the cell-site simulator (unlike the GPS device in *Jones*) was not used to generate the probable cause for arrest; probable cause to arrest Patrick predated the effort to locate him. From his perspective, it is all the same whether

a paid informant, a jilted lover, police with binoculars, a bartender, a member of a rival gang, a spy trailing his car after it left his driveway, the phone company's cell towers, or a device pretending to be a cell tower, provided location information. A fugitive cannot be picky about how he is run to ground. So it would be inappropriate to use the exclusionary rule, even if the police should have told the judge that they planned to use a cell-site simulator to execute the location warrant.

The Department of Justice announced last September that in the future it would ordinarily seek a warrant, plus an order under the pen-register statute, 18 U.S.C. §3123, before using a cell-site simulator, but it has not conceded that this is constitutionally required. Questions about whether use of a simulator is a search, if so whether a warrant authorizing this method is essential, and whether in a particular situation a simulator is a reasonable means of executing a warrant, have yet to be addressed by any United States court of appeals. We think it best to withhold full analysis until these issues control the outcome of a concrete case.

AFFIRMED

WOOD, *Chief Judge*, dissenting. This case raises serious issues about the use of cell-site simulators to track down the location of a target person. That is how police found Damian Patrick, for whom an arrest warrant had been issued for parole violations. My colleagues see no serious Fourth Amendment issues in Patrick's case, because they believe that a defendant has no interest in the manner in which a warrant is executed. They also question whether the use of a cell-site simulator is a "search" at all, noting that *Smith v. Maryland*, 442 U.S. 735 (1979), holds that the use of a pen register is not a "search," and that *United States v. Knotts*, 460 U.S. 276 (1983), says the same thing about the use of a beeper. Finally, they note that Patrick was arrested in a "public place," by which they mean sitting in the passenger seat of a parked car. All of this matters greatly to Patrick, because if his initial arrest was invalid, then the gun that the police spotted in plain view in the car should have been suppressed as "fruit of the poisonous tree," see *Wong Sun v. United States*, 371 U.S. 471, 488 (1963), and Patrick's conviction under 18 U.S.C. §§ 922(g)(1) and 924(a)(2) for being a felon in possession of a firearm would need to be revisited. If the arrest complied with the Fourth Amendment, the gun was lawfully found and seized and his conviction must be affirmed. Because I believe that the panel opinion underestimates the relevant technology's capabilities and extends *Utah v. Strieff*, 136 S. Ct. 2056 (2016), too far, I dissent.

This is the first court of appeals case to discuss the use of a cell-site simulator, trade name "Stingray." We know very little about the device, thanks mostly to the government's refusal to divulge any information about it. Until recently, the government has gone so far as to dismiss cases and withdraw evidence rather than reveal that the technology was used. See

Memorandum Agreement between Amy S. Hess, Assistant Director, Operational Technology Division, FBI, and David Salazar, Chief of Police, MPD (Aug. 13, 2013) (agreeing to dismiss cases rather than disclose use of Stingray). Indeed, in this case, the government appears to have purposefully concealed the Stingray's use from the issuing magistrate, the district court, defense counsel, and even this court. It ultimately admitted its use of the device only in response to an *amicus curiae* brief filed during this appeal.

Although, as we all agree, Patrick does not have standing to challenge any location information gathered from other persons' cell phones, see *Jones v. United States*, 362 U.S. 257, 261 (1960), *overruled on other grounds by United States v. Salvucci*, 448 U.S. 83 (1980), he is entitled to challenge the use of the Stingray itself, along with the gathering of any non-location information from his cell phone.

The record is painfully—indeed fatally—inadequate with respect to critical details about the way the Stingray was used. We are thus not in a position to determine whether (1) its use was sufficiently outside the scope of the warrant to merit blanket suppression; and whether (2) Patrick's arrest (putting the warrant to one side) was based in whole or in part on information gathered in violation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–20 (if, as it may, that statute applies). Even if the Stingray revealed no information beyond Patrick's location, we must know how it works and how the government used it before we can judge whether it functions in a manner sufficiently different from the location-gathering methods specified in the warrant that it amounted to a search outside the warrant's scope.

The majority offers a long quote from the Department of Justice Policy Guidance manual on the use of cell-site simulator technology, *ante* at 3–4, but that information is contestable. We are given no reason to think that a municipal police department such as MPD was bound in any way to the guidance offered by the DOJ, or that the MPD chose to follow the DOJ Guidance as a matter of internal policy. There is another side to the story, but because of the government's furtiveness, Patrick never had the chance to present it.

With certain software (known as "Fishhawk" and "Porpoise"), the Stingray is much more than a high-tech pen register. It can capture the "emails, texts, contact lists, images," and other data disclaimed by the last paragraph of the majority's excerpt of the Policy Guidance. It can eavesdrop on telephone conversations and intercept text messages. See Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 11–12 (2014) ("Depending on the particular features of the surveillance device and how they are configured by the operator, IMSI catchers can be used to identify nearby phones, locate them with extraordinary precision, intercept outgoing calls and text messages, as well as block service, either to all devices in the area or to particular devices." (footnotes omitted)). Because many third-party apps automatically send and receive data through the subscriber's network, it is reasonable to assume that a Stingray can collect other information from a cell phone, as well.

We know nothing about the way in which the Stingray used in Patrick's case was configured, nor do we know the extent of its surveillance capabilities. The majority properly

notes that DOJ's description may or may not be accurate, either in general or for particular cases. It is worth underscoring how inaccurate that description may be and how important it is, both for Patrick and as a matter of Fourth Amendment jurisprudence and public policy, that these questions be explored.

In this case, the location warrant authorized only methods of fixing Patrick's location that involved gathering information that would reveal his phone's connection with cell-phone towers. The Supreme Court has recognized that a search of cell-phone data requires a warrant. See *Riley v. California*, 134 S. Ct. 2473, 2494–95 (2014) (associating a warrantless search of a cell phone with the "reviled 'general warrants' and 'writs of assistance'" against which the Fourth Amendment was aimed). The authorization of the collection of location data cannot be expanded to permit a search of the contents of Patrick's cell phone. If the Stingray gathered information from the phone that went beyond his location, such a "search" of his phone would have been unauthorized, and suppression of the additional information (which might have pinpointed Patrick's location) would likely be required. See *United States v. Foster*, 100 F.3d 846, 850–51 (10th Cir. 1996) (applying blanket suppression where agents performed general search of residence and seized "anything of value" even though warrant authorized only search for four firearms and marijuana).

Title III may also be pertinent here, depending on what the facts reveal about the device that was used. It seems clear that if the MPD intercepted any cell-phone conversations, text messages, or data, Title III covered those interceptions. Under section 2511(a), any person who "intentionally intercepts …

any wire, oral, or electronic communication" without following the proper procedures is liable under the statute. "Title III now applies to the interception of conversations over both cellular and cordless phones." *Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001). The Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). Text messages and cell-phone data transmissions easily fit that definition. None of the relevant exceptions to that definition applies, see *id.*, and there is no reason to think that the interception of text messages or data transmissions would otherwise be excluded from it. See *Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995) ("The principal purpose of the [Electronic Communications Privacy Act] amendments to Title III was to extend to 'electronic communications' the same protections against unauthorized interceptions that Title III had been providing for 'oral' and 'wire' communications via common carrier transmissions."); see also *Joffe v. Google, Inc.*, 746 F.3d 920, 930 (9th Cir. 2013) (electronic information transmitted over Wi-Fi network does not fit 18 U.S.C. § 2511(g) exceptions).

The MPD concededly never followed the procedures required for an order for electronic surveillance. See 18 U.S.C. § 2518. Any interception of the substance of Patrick's communications would thus almost certainly be illegal. The remedy for a Title III violation is normally the suppression of the illegally intercepted communications and any evidence derived from them. 18 U.S.C. § 2515. If such evidence is relevant to Patrick's conviction, Title III might require suppression and,

in the absence of the suppressed evidence, a reversal of the conviction.

Even if the Stingray did not gather any information from Patrick's cell phone other than its location, its use still might be problematic. The court order authorized "cellular telephone global positioning system (GPS) location information … if available," and the "identification of the physical location of the target cellular telephone." But that is not all it said: it specified in some detail the manner in which that information was to be collected—from the service provider. "Such service provider," it stated, "shall initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available[.]" It "[a]pprove[d] the release of information," not the use of a device that would allow the MPD to track Patrick's phone on its own. While it also "authorize[d] the identification of the physical location of the target cellular phone," the context implied that the identification would be derived from information released by a service provider. I take these limitations, built into the warrant, seriously; they circumscribe the authority granted by the warrant just as surely as a physical limitation to the house but not the garage, or vice versa, would do.

At oral argument, the government argued that the warrant authorized it to obtain Patrick's location with no restrictions on how it went about accomplishing that task. It relies on *Dalia v. United States*, 441 U.S. 238, 257 (1979), which held that a warrant was not defective for lack of particularity where it authorized police officers to install an electronic listening device in the defendant's office but did not specify that the officers would covertly enter the premises to do so. *Dalia* noted

that "the specificity required by the Fourth Amendment does not generally extend to the means by which warrants are executed." *Id.* But that statement must be understood in context. Here, the device itself is what is at issue. Because of its capabilities, the way it was used could affect the scope and location of the search itself.

We are in all likelihood not looking at two interchangeable tools for gathering exactly the same information. If the facts ultimately show that the MPD had gathered the identical information in the same manner that Sprint would have used, I would concede that there is no problem. In such a case, the only difference between using the Stingray and obtaining the information from Sprint would be *who* gathered the information. And the majority may even be correct that the government's regrettable lack of candor about the manner of the search is not enough by itself to render the search unconstitutional. Under these circumstances, there would be no additional privacy intrusion from the use of the Stingray, and the misrepresentation would not affect whether there was probable cause for the search. See *United States v. Mittelman*, 999 F.2d 440, 444 (9th Cir. 1993) (holding that because "only false statements that are material in causing the warrant to issue will invalidate it," "misstatements regarding the manner of a search do not bear on the issue of whether the search itself was justified" under the Fourth Amendment (quoting *United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985))); see also *Franks v. Delaware*, 438 U.S. 154, 156 (1978) (warrant based in part on false statements is void if "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause"). This means that the critical questions in a case such as this one, where a much more sophisticated device is used, are how the Stingray was

used, how it works, and whether, conceptually, it "searched" Patrick's phone in the same manner that Sprint would or much more intrusively.

According to extra-record information provided by *amici*, the Stingray is different in kind, not just in degree. On this record, we do not have sufficient information to say whether that is right or wrong. We do not know whether the warrant's authorization of *Sprint* to "initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonable available" also describes the working of the *Stingray* that was used. If so, perhaps all is well. If the Stingray works in a different manner—for instance, by forcing the cell phone to transmit location data housed inside the cell phone rather than using a signal to locate the cell phone on the Sprint network—it might not. See C. Justin Brown & Kasha M. Leese, *Stingray Devices Usher in A New Fourth Amendment Battleground*, 39 CHAMPION 12, 14 (2015) (arguing that cell-site simulators engage in "electronic … intrusion" possibly constituting trespass because they force cell phones to transmit information that they would not otherwise). The relevant point is that a location warrant does not (without saying more) authorize a search of the contents of the cell phone itself. If that is the right way to describe what the Stingray did, its use would constitute an impermissible search, and the gun would be fruit of the poisonous tree. At this point, we do not have the facts to say.

My colleagues finally dismiss my concerns for a different reason: they contend that the existence of a warrant for Patrick's arrest brings this case under the rule of *Utah v. Strieff*,

136 S. Ct. 2056 (2016), and precludes the application of the exclusionary rule. In *Strieff*, the Supreme Court held that a valid, pre-existing arrest warrant could attenuate the link between an unlawful investigatory stop and evidence seized as a result of that stop. *Id.* at 2062. But I do not read *Strieff* so broadly.

It is critical in this connection to recall that *Strieff* rests on the idea of a break in the causal chain, and it is that break that attenuates any Fourth Amendment concerns. In *Strieff*, the officer stopped the defendant without reasonable suspicion and then conducted a warrant check; based on the warrant he discovered, he arrested the defendant. *Id.* at 2060. The drugs at issue were found by the search incident to that arrest. *Id.* As a result, the causal chain between the officer's illegal action—the initial, unjustified *Terry* stop—and the search was "brok[en]" by the intervening discovery of the warrant. *Id.* at 2063. The arrest warrant was "downstream" of the tainting action, and "upstream" of the search.

Our case presents a different sequence. The arrest warrant here (and the relevant officers' awareness of it) preceded both the potentially illegal action and the potentially valid search—it was "upstream" of both. The MPD got the arrest warrant, got the location warrant, used the Stingray to locate Patrick, and then found the gun in plain view in the process of arresting him. The arrest warrant is therefore not an intervening cause, at least in the temporal sense. One could perhaps argue that the arrest warrant resurfaced in the causal chain at the moment the MPD located Patrick, and then moved to apprehend him. (Ironically, in this case, an arrest warrant was not even necessary to authorize the finding of the gun, which was in plain view.) But any causal connection

in this case between a potentially illegal search and the discovery of Patrick's gun had to do with the *timing* of the search—not whether the search could be conducted at all. As a result, the arrest warrant did not do anything to attenuate the potential taint.

I recognize that *Strieff* contains language that could be stretched to suggest that a warrant's existence, regardless of the actual causal chain, is sufficient attenuation. See *id*. at 2062 ("The *Segura* Court suggested that the existence of a valid warrant favors finding that the connection between unlawful conduct and the discovery of evidence is 'sufficiently attenuated to dissipate the taint.' That principle applies here." (citation omitted)). But elsewhere in the opinion the Court emphasized not only that the "warrant was valid" and "predated [the officer's] investigation," but also that it "was *entirely unconnected* with the stop," and that the officer's decision to arrest the defendant was "a ministerial act that was independently compelled by the pre-existing warrant." *Id*. (emphasis added). Here, the use of the Stingray led to the arrest, and neither the arrest nor the search was a ministerial act.

It oversimplifies *Strieff* to focus solely on whether an intervening circumstance can be identified. That is important, but it is not enough by itself. *Strieff*, like all attenuation cases, also rests on two other factors: (1) the "temporal proximity" between the potentially unlawful action and the "search," and (2) the culpability of the police misconduct. *Id.* As in *Strieff*, the relative temporal proximity in our case between the potentially illegal conduct and the search weighs against attenuation. But unlike the situation in *Strieff*, the facts here do not permit us to say that the MPD's conduct was merely negli-

gent: the police knew what they were doing. Purposeful evasion of judicial oversight of potentially illegal searches is exactly the kind of "police misconduct … most in need of deterrence." *Id.* at 2063 (noting that exclusion should be applied where misconduct is "purposeful or flagrant"). I would find that all three factors identified in *Strieff* weigh against finding attenuation in this case.

None of the other doctrines that might counsel against use of the exclusionary rule applies here. Although the independent-source doctrine precludes the operation of the exclusionary rule, see *Murray v. United States*, 487 U.S. 533, 537 (1988), there was no alternate source here that enabled the MPD to find Patrick. Nor is this case a likely candidate for the inevitable-discovery rule. See *Nix v. Williams*, 467 U.S. 431, 444 (1984) (exclusionary rule does not apply if "prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means"). Patrick's gun was found because it was in the car where he was sitting at the time of his apprehension. If not for the Stingray, he might not have been apprehended in his vehicle, or he might have been apprehended at a time when the gun was not located in his vehicle.

Neither would the good-faith exception apply. "The good-faith exception precludes application of the exclusionary rule when law enforcement reasonably and in good faith believed that a search was lawful." *United States v. Tomkins*, 782 F.3d 338, 349 (7th Cir. 2016) (citing *United States v. Leon*, 468 U.S. 897, 922 (1984)). The contents of the search warrant application, the warrant itself, and the government's litigation of this case all tend to show that the officers deliberately deceived

the issuing judge about how they planned to execute the warrant. While the test for the exception is "an objective one," *Leon*, 468 U.S. at 919 n.20, that fact is designed to safeguard the Fourth Amendment's substantive protections, not to limit them. See *id.* at 915 n.13. Deception of the issuing magistrate is just the kind of misconduct "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009). *Leon* specifically noted that the good-faith exception should not apply "when the affiant misleads the magistrate with a reckless or knowing disregard for the truth." *United States v. Glover*, 755 F.3d 811, 818 (7th Cir. 2014) (citing *Leon*, 468 U.S. at 914 (suppression appropriate where officers dishonest in preparing affidavit)).

A number of other courts have suggested that bad faith, especially when manifested by insufficient candor to the issuing magistrate, may justify suppression. See *United States v. Sells*, 463 F.3d 1148, 1161 n.7 (10th Cir. 2006) (noting that "a number of courts have concluded that the severance doctrine is not applicable where the Government has added particularized descriptions of items to be seized for which probable cause exists as a pretext to support an otherwise unlawful search and seizure"); *United States v. Woerner*, 709 F.3d 527, 534 (5th Cir. 2013) (collecting cases for principle that suppression is appropriate where the "officer applying for the warrant knew or had reason to know that the information was tainted and included it anyway without full disclosure and explanation"); *United States v. Reilly*, 76 F.3d 1271, 1281 (2d Cir. 1996) (rejecting application of good-faith exception "when the officers are themselves ultimately responsible for the defects in the warrant"). Although these cases are about

affidavits supporting probable cause, their logic applies equally to the execution of the search. After all, the *Leon* exception was meant to prevent the "[p]enalizing [of] the officer for the magistrate's error," *Leon*, 468 U.S. at 921, and to "allow some latitude for honest mistakes." *Maryland v. Garrison*, 480 U.S. 79, 87 (1987). If the MPD misled the magistrate or reasonably should have known that the warrant did not cover a Stingray, neither concern applies here.

Even if my colleagues' reading of *Strieff* were correct or another doctrine precluding the exclusionary rule applied, those facts would not resolve any potential Title III issues discovery could reveal. Our sister circuits disagree about whether the Title III suppression remedy is affected by the judge-made exclusionary rule. Compare *United States v. Rice*, 478 F.3d 704, 711 (6th Cir. 2007) (good-faith exception does not apply); *United States v. Spadaccino*, 800 F.2d 292, 296 (2d Cir. 1986) (using this same rationale and reaching the same conclusion in analyzing whether the *Leon* good-faith exception applied to a state wiretapping statute); *United States v. Vest*, 813 F.2d 477, 484 (1st Cir. 1987) (rejecting judicially created exception); with *United States v. Moore*, 41 F.3d 370, 376 (8th Cir. 1994) (good-faith exception applies); *United States v. Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988) (same, although without analysis); *United States v. Brewer*, 204 Fed. App'x 205, 208 (4th Cir. 2006) (same). No court of appeals has found that the attenuation rule applies to the Title III suppression remedy. In fact, *United States v. Giordano*, 416 U.S. 505, 528 (1974), seems to suggest it does not. Unless we are prepared to weigh in on this question without knowing whether it is before us, we should remand for further fact-finding.

It is time for the Stingray to come out of the shadows, so that its use can be subject to the same kind of scrutiny as other mechanisms, such as thermal imaging devices, GPS trackers, pen registers, beepers, and the like. Its capabilities go far beyond any of those, and cases such as *Riley* indicate that the Supreme Court might take a dim view of indiscriminate use of something that can read texts and emails, listen to conversations, and perhaps intercept other application data housed not just on the target's phone, but also on those of countless innocent third parties. Governmental entities, including the Justice Department itself, see DOJ Policy Guidance, *ante* at 3–4, and the State of Illinois, see Citizen Privacy Protection Act, Pub. Act 099-0622 (2016) (delineating court order, disclosure, and minimization requirements for police use of cell-site simulators), have recognized the weighty Fourth Amendment concerns the device provokes. It is possible that discovery could reveal that none of those concerns is triggered in this case. But before we dismiss them, we should have all the facts before us. For that reason, I would remand this case for further fact-finding. I respectfully dissent.