DISTRICT OF COLUMBIA COURT OF APPEALS

No. 15-CF-322

PRINCE JONES, APPELLANT,

v.

UNITED STATES, APPELLEE.

Appeal from the Superior Court
of the District of Columbia
(CF1-18140-13)

(Hon. Jennifer M. Anderson, Trial Judge)

(Argued April 18, 2017 Decided September 21, 2017)

Stefanie Schneider, Public Defender Service, with whom *Samia Fam* and *Jaclyn Frankfurt*, Public Defender Service, were on the brief, for appellant.

Lauren R. Bates, Assistant United States Attorney, with whom *Channing D. Phillips*, United States Attorney, and *Elizabeth Trosman*, *John P. Mannarino*, and *Jodi S. Lazarus*, Assistant United States Attorneys, were on the brief, for appellee.

Nathan Freed Wessler, American Civil Liberties Union, with whom *Arthur B. Spitzer* and *Scott Michelman*, American Civil Liberties Union, and *Jennifer Lynch*, Electronic Frontier Foundation, were on the brief, for American Civil Liberties Union of the Nation's Capital and Electronic Frontier Foundation, *amicus curiae*, in support of appellant.

Before THOMPSON and BECKWITH, *Associate Judges*, and FARRELL, *Senior Judge*.

Opinion by *Associate Judge* BECKWITH for the court, except as to Part II.E.3.

Opinion by *Senior Judge* FARRELL, concurring in part and concurring in the judgment, at page 47.

Dissenting opinion by *Associate Judge* THOMPSON, at page 54.

BECKWITH, *Associate Judge*: A jury found appellant Prince Jones guilty of various offenses arising out of two alleged incidents of sexual assault and robbery at knifepoint.[1] Mr. Jones appeals his convictions on the ground that much of the evidence offered against him at trial was the direct or indirect product of a warrantless—and thus, Mr. Jones argues, unlawful—search involving a cell-site simulator or "stingray."[2] Mr. Jones presented this Fourth Amendment claim to the trial court in a pretrial motion to suppress, but the trial court denied it under the

[1] Mr. Jones was convicted of two counts of first-degree sexual abuse while armed, D.C. Code §§ 22-3002 (a)(1)–(2), -3020 (a)(5), -3020 (a)(6), -4502 (2012 Repl.); two counts of kidnapping while armed, *id.* §§ 22-2001, -4502; four counts of robbery while armed, *id.* §§ 22-2801, -4502; and one count of threats, *id.* § 22-1810.

[2] The "StingRay" is a popular cell-site simulator produced by the Harris Corporation. *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, 14 (2014). The name has become a generic term for a cell-site simulator. Kim Zetter, *Hacker Lexicon: Stingrays, the Spy Tool the Government Tried, and Failed, to Hide*, Wired (May 6, 2016), https://www.wired.com/2016/05/hacker-lexicon-stingrays-spy-tool-government-tried-failed-hide/. The record in this case does not reveal the name of the device used against Mr. Jones; in the suppression hearing, the trial court sustained the government's objection to a question about the name of the device.

inevitable-discovery doctrine[3] and did not reach the question whether the government violated Mr. Jones's rights. We agree with Mr. Jones that the government violated the Fourth Amendment when it deployed the cell-site simulator against him without first obtaining a warrant based on probable cause. Further, we reverse the trial court's inevitable-discovery ruling and reject the government's argument (not resolved by the trial court) that the good-faith doctrine[4] precludes applying the exclusionary rule in this case. Because the admission at trial of the evidence obtained as a result of the unlawful search was not harmless beyond a reasonable doubt, we reverse Mr. Jones's convictions.

I. Background

A. Investigation and Arrest of Mr. Jones

At the suppression hearing in this case, Detective Rachel Pulliam, a member of the Sexual Assault Unit of the Metropolitan Police Department (MPD), testified that she investigated a sexual assault that occurred around 12:30 a.m. on October 9, 2013, and another that occurred around 1:30 a.m. on October 11. The two sexual-

[3] *See Nix v. Williams*, 467 U.S. 431 (1984).

[4] *See United States v. Leon*, 468 U.S. 897 (1984).

assault complainants were women who had advertised escort services on the classified-advertising website Backpage. Detective Pulliam testified that on each occasion, the perpetrator[5] contacted the complainant by telephone in response to an advertisement and arranged to pay the complainant for sexual services. According to Detective Pulliam, when each complainant arrived at the arranged meeting place, the perpetrator "forced [her] to perform oral sex on [him] at knifepoint" and robbed her of her cellphone and other property. Detective Pulliam testified that on one of the two occasions, the perpetrator also robbed the complainant's cousin, who had been waiting in a car outside the meeting location.

Detective Pulliam testified that in the morning following the second incident, she and her colleagues obtained telephone records for the sexual-assault complainants. The telephone records revealed a possible suspect: Both complainants had received calls from the same number during the relevant time periods. Detective Pulliam sought the assistance of the MPD's Technical Services Unit (TSU) to track the suspect's and the complainants' phones.

[5] Detective Pulliam referred to the perpetrator as "the defendant," but Mr. Jones was not known to the police at the time the complainants reported the crimes and only became known after the police tracked him down using the cell-site simulator.

Sergeant Todd Perkins, a supervisor in the TSU, testified about his office's efforts to track the phones that morning. He testified that he and his team sought "subscriber information" for the suspect's number from the provider associated with that number but were unsuccessful—the cellphone "was just a generic prepaid" with "no subscriber information whatsoever." The TSU also sought and obtained information about the locations of the suspect's and complainants' cellphones from the relevant telecommunication providers.[6] According to Sergeant Perkins, the TSU received updated location information from the providers every fifteen minutes. The information came in the form of geographic coordinates—latitude and longitude—with a "degree of uncertainty" specified in meters.

Sergeant Perkins testified that the real-time location information they received that morning had a high degree of uncertainty—"several hundred meter[s]"—indicating that the phones' GPS capabilities were inactive. He explained that "if it [had been] true GPS," his team would have been "getting two meter, three meter, five meter hits." Despite the lack of precision in the location information, Sergeant Perkins and his team were able to "tell that . . . one of the

[6] Officer Perkins testified that the TSU "declared an exigent situation" and was therefore "able to obtain the [real-time location] information without getting a warrant." Officer Perkins admitted at the suppression hearing that his team had been operating under an erroneous belief that there had been a string of three sexual assaults by the same perpetrator within the preceding twenty-four hours.

[complainants'] phones and the [suspect's] phone were traveling in the same general direction . . . as if they were together." The location information suggested that the two phones stopped in the general vicinity of the Minnesota Avenue Metro Station.

Based on this information, Sergeant Perkins and other TSU officers took a truck equipped with a cell-site simulator to the area of the Minnesota Avenue Metro station and used the device to track the suspect. Sergeant Perkins could not remember whether he and his team used the cell-site simulator to track the suspect's phone or the complainant's phone that they believed was traveling with it,[7] but whichever signal they were tracking led them, at around 11:30 a.m., to a parked Saturn. Inside the Saturn were Mr. Jones and Mr. Jones's girlfriend, Nora Williams. The police arrested Mr. Jones and recovered evidence from Mr. Jones's person and his car and from Ms. Williams, including a folding knife and the

[7] As explained in the testimony summarized below, a cell-site simulator interferes with the target phone's ability to communicate with the cellular network. Records for the complainant's phone show that there was a single communication error around the time the TSU officers were operating the cell-site simulator, and Sergeant Perkins inferred from this—and from other circumstantial information—that his team had probably been tracking the complainant's phone. Other evidence, however, suggested that the TSU may have been tracking the suspect's phone. In particular, records for the suspect's phone—which turned out to be Mr. Jones's phone—show seven failed calls during the relevant time period, and a data dump of the phone revealed that during that time period Mr. Jones sent a text message which said, "Our call dropped."

complainants' and the suspect's cellphones. Mr. Jones also made an incriminating statement to the police. Ms. Williams later testified against Mr. Jones at trial.

B. Cell-Site Simulator

Sergeant Perkins testified at the suppression hearing about "how [the cell-site simulator they used] works," "based on the information that's publicly available." He explained that his team engages the cell-site simulator by programming into it a unique identifier—an MIN or IMSI number[8]—associated with the target phone.[9] The simulator then begins "listening for [the target] phone," which, as part of its normal operation, is "constantly transmitting to and receiving from a tower." The officers operating the cell-site simulator drive around and "as soon as [the simulator] comes across [the target phone's signal], it

[8] These identifying numbers are distinct from the seven- or ten-digit number that a person dials when he or she places a call. Sergeant Perkins testified that the TSU receives these numbers by requesting "subscriber information" for a phone number. He explained that "MIN" stands for "mobile identification number" and is the identifying number used by "Verizon, Cricket and Sprint" and that "IMSI" stands for "international mobile subscriber identification" and is used by "T-Mobile and AT&T."

[9] Sergeant Perkins testified that it is also possible to enter multiple identifying numbers into the cell-site simulator. In this operating mode, he explained, "the equipment will just let us know one of those phones is present in the area" but will not provide location information.

grabs it and it holds on to it." Once the cell-site simulator "grabs" the target phone, the simulator begins reporting "general location information and signal strength" that can be used to locate the target phone's exact location.[10] Sergeant Perkins testified that once the cell-site simulator "grabs" the target phone, the target phone is prevented from communicating "with an actual . . . tower."

Further information about the cell-site simulator was provided by Ben Levitan, an expert on "cellular telephone networks and systems" called by the defense.[11] According to Mr. Levitan, cell phones are "dumb devices" that "generally connect themselves to the strongest cell tower signal that they detect." Mr. Levitan explained that a cell-site simulator "act[s] as a portable cell tower," which, "when turned on or brought into an area, may appear to be a stronger signal and cause [a] phone[] to break its connection with the cell phone network and

---

[10] Sergeant Perkins explained the search process thus:

> [T]here is a directional antenna, . . . so we're driving this way, the directional antenna knows the signal is coming from over here, so we know the phone's coming over there. And then it also measures the signal strength from the phone, so if the signal strength is real, real low, it's probably somewhere behind you.

[11] The defense also submitted an affidavit by Mr. Levitan, which Mr. Levitan "adopt[ed] . . . as part of [his] testimony," without objection by the government.

reattach itself to the newly found . . . simulator."[12] Mr. Levitan testified that when the cellphone "attach[es]" itself to the cell-site simulator, it "identifies itself by phone number and various codes," including its IMSI number.[13] Although Mr. Levitan had never used the type of cell-site simulator utilized by law enforcement, he testified that he had used similar devices working within the telecommunications industry and that the devices allow the user to determine the target phone's direction and distance relative to the simulator device.[14] Moreover, because the cell-site simulator is not a true cell tower connected with the cellular network, any cellphone connected to the cell-site simulator will not be able to communicate with the network: "[Y]our call doesn't go through[,] period.

---

[12] Mr. Levitan testified that a cell-site simulator causes not only the target phone, but "[a]ll cell phones that are in the vicinity," to "attach . . . to the newly found . . . simulator."

[13] Cell-site simulators are sometimes referred to as "IMSI catchers." Pell & Soghoian, *supra* note 2, at 11.

[14] Mr. Levitan testified that when a cellphone is communicating with a legitimate cellular tower, it communicates with a particular sector antenna of the tower, and that the provider can thus determine "what side of the cell tower" the cellphone is on. Mr. Levitan indicated that cell-site simulators measure direction through a similar method. But see *supra* note 10 (Sergeant Perkins describing a somewhat different method of determining direction). And Mr. Levitan testified that a cell-site simulator can determine distance through a "trick" in which it "send[s] . . . a signal [to the phone] and ask[s] it to send . . . the signal back." By "measur[ing] th[e] round trip time," the distance between the cell-site simulator and the phone can be determined.

Nothing happens."[15]

C. Trial Court's Ruling on the Motion To Suppress

In ruling on Mr. Jones's motion to suppress, the trial court did not decide whether the use of a cell-site simulator was a search within the meaning of the Fourth Amendment or whether the government was required to obtain a warrant to use the cell-site simulator. Instead, the trial court focused on the issues of standing, exigent circumstances, and inevitable discovery.

---

[15] We note that both witnesses' testimony about the cell-site simulator is consistent with information in a Department of Justice memorandum on such devices. *See* Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download. The memorandum explains:

> 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.

Id. at 2. Once the target cellphone is identified, the cell-site simulator "provide[s] . . . the relative signal strength and general direction" of the phone. *Id.* The memorandum notes that the cell-site simulator can cause "cellular devices in the area [to] experience a temporary disruption of service from the service provider." *Id.* at 5.

On the issue of standing, the trial court stated that the suppression-hearing record did not reveal "with any great degree of certainty" which phone—Mr. Jones's or the complainant's—the police had tracked using the cell-site simulator. The court believed that the burden was on the government to show that the police did not track Mr. Jones's phone and found that the government had failed to meet this burden. The government did not take issue with this allocation of the burden of proof and agreed with the court's determination.[16]

The trial court rejected the government's argument that there were exigent circumstances justifying noncompliance with any otherwise applicable warrant requirement—though, again, the trial court did not determine whether there *was* a warrant requirement. The court noted that significant time (around ten hours) had passed between the sexual assault and the arrest of Mr. Jones on October 11, during which time "the detectives could have been getting a warrant."

The trial court agreed with the government's argument that regardless of whether there had been a Fourth Amendment violation, the inevitable-discovery

[16] The government has reversed course in this appeal and is now arguing that Mr. Jones bore the burden of proving that the government searched his phone and failed to meet this burden. But because the government affirmatively—and repeatedly—conceded the standing issue in the trial court, the government has waived this argument.

doctrine rendered the exclusionary rule inapplicable. The court found that "even if [the police] were using [Mr. Jones's] phone on the cell site simulator, . . . had they switched over . . . to use the [complainant's] number instead, . . . they would have eventually gotten to the exact same place because the phones were together[a]nd it's the same technology." The court thus agreed with the government's assertion that "there[was] a separate lawful means" by which the government "would have gotten to the exact same place."

II. Discussion

Mr. Jones claims that the government's use of a cell-site simulator violated his Fourth Amendment rights and that the trial court erred in failing to grant his motion to suppress. In deciding this Fourth Amendment claim, we defer to the trial court's factual findings and review them only for clear error, but we review the trial court's legal conclusions de novo. (*Albert*) *Jones v. United States*, 154 A.3d 591, 594 (D.C. 2017). The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and thus we turn first to the threshold question whether the government's use of the cell-site simulator to locate Mr.

Jones's cellphone[17] constituted a search or seizure.

A. Fourth Amendment Search

Government conduct is a "search" within the meaning of the Fourth Amendment if it invades "an actual (subjective) expectation of privacy . . . that society is prepared to recognize as reasonable." *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (internal quotation marks omitted); *see also Kyllo v. United States*, 533 U.S. 27, 33 (2001); *Napper v. United States*, 22 A.3d 758, 767 (D.C. 2011). In deciding whether a particular expectation of privacy is "reasonable," this court aims to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34. "To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." *Id.*

Our analysis begins with the obvious fact that most people have a cellphone

[17] We consider it conceded that the government deployed the cell-site simulator on Mr. Jones's phone rather than on one of the complainants' phones. See *supra* notes 7 & 16, as well as the accompanying text.

and carry it with them practically everywhere they go.[18] One consequence of this is that locating and tracking a cellphone using a cell-site simulator has the substantial potential to expose the owner's intimate personal information. First, "cell phone tracking can easily invade the right to privacy in one's home or other private areas." *Tracey v. State*, 152 So. 3d 504, 524 (Fla. 2014); *see also State v. Earls*, 70 A.3d 630, 642 (N.J. 2013) ("[C]ell phones . . . blur the historical distinction between public and private areas because [they] emit signals from both places."). When this occurs, there is a "clear[] . . . Fourth Amendment violation." *Tracey*, 152 So. 3d at 524; *see also United States v. Karo*, 468 U.S. 705, 714 (1984) ("[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."). And second, even a person's public movements, as observed by a cell-site simulator or other means of cellphone tracking, can reveal sensitive information about the person's "familial, political, professional, religious, and sexual associations." *United States v.* (*Antoine*) *Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

---

[18] *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("[I]t is the person who is not carrying a cell phone . . . who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time . . . .").

Another consequence of cellphones' "pervasiveness"[19] is that a cell-site simulator can be used by the government not merely to *track* a person but to *locate* him or her. *See State v. Andrews*, 134 A.3d 324, 348 (Md. Ct. Spec. App. 2016). Police have always had the capacity to visually track a suspect from some starting location, and electronic tracking devices like those used in *United States v. Knotts*, 460 U.S. 276 (1983), and *Karo*, 468 U.S. 705, have augmented this preexisting capacity. But although the kind of device used in *Knotts* and *Karo* is probably more reliable than a human tracker—less prone to discovery than a human and harder to elude—at their core these devices merely enable police officers to accomplish the same task that they could have accomplished through "[v]isual surveillance from public places." *Knotts*, 460 U.S. at 282; *see also Karo*, 468 U.S. at 713. This is because the tracking device must be physically installed on some object that the target will later acquire or use. *See, e.g.*, (*Antoine*) *Jones*, 565 U.S. at 402–03 (GPS tracker placed on the defendant's wife's car); *Karo*, 468 U.S. at 708 (tracker placed in container of chemicals the defendant had purchased); *Knotts*, 460 U.S. at 276 (same). These devices do not enable police to locate a person whose whereabouts were previously completely unknown.

With a cell-site simulator, however, police no longer need to track a person

[19] *Riley*, *supra* note 18, 134 S. Ct. at 2490.

visually from some starting location or physically install a tracking device on an object that is in, or will come into, his or her possession. Instead, they can remotely activate the latent tracking function of a device that the person is almost certainly carrying in his or her pocket or purse: a cellphone. As the present case demonstrates, police officers first obtain subscriber information and real-time location information from the target's telecommunications provider to narrow down the search area.[20] They then proceed to that area with a cell-site simulator,

[20] Mr. Jones has not argued in this appeal that the government violated his Fourth Amendment rights when it obtained real-time cell-site location information (CSLI) for his phone from his telecommunications provider. Also not involved in this case is historical CSLI—location information maintained by cellular companies in the ordinary course of business. Some courts have held that the Fourth Amendment protects real-time CSLI, *e.g.*, *Tracey*, 152 So. 3d at 523, but many have held that the Fourth Amendment does not protect historical CSLI, *e.g.*, *United States v. Graham*, 824 F.3d 421, 427–28 (4th Cir. 2016) (en banc). *See generally* Eric Lode, Annotation, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (2015). The Fourth Amendment analysis for real-time and historical CSLI disclosed by a telecommunications provider is complicated by uncertainty about the applicability and scope of the third-party doctrine. *Compare Graham*, 824 F.3d at 427–28 ("Each time Defendants made or received a call, or sent or received a text message—activities well within the 'ordinary course' of cell phone ownership—[their provider] generated a record of the cell towers used . . . . Having 'exposed' the CSLI to [their provider], Defendants here, like the defendant in *Smith*, 'assumed the risk' that the phone company would disclose their [historical CSLI] to the government." (quoting *Smith v. Maryland*, 444 U.S. 735, 744 (1979))), *with In re United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011) ("[T]he court concludes that established normative privacy considerations support the conclusion that the reasonable expectation of privacy is preserved here, despite the fact that cell-site-location records [are] (continued…)

which they use to force the person's cellphone to identify itself and reveal its exact location. It is in this sense that a cell-site simulator is a locating, not merely a tracking, device: A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will.

A final consideration is that when the police use a cell-site simulator to locate a person's cellphone, the simulator does not merely passively listen for transmissions sent by the phone in the ordinary course of the phone's operation. Instead, the cell-site simulator exploits a security vulnerability in the phone—the fact that cellphones are, in the words of the defense expert, "dumb devices," unable to differentiate between a legitimate cellular tower and a cell-site simulator masquerading as one[21]—and actively induces the phone to divulge its identifying information. Once the phone is identified, it can be located. So far as the present record reveals, the only countermeasure that a person can undertake is to turn off

---

(…continued)
disclosed to cell-phone service providers."). The third-party doctrine has no application in the present case, however, because the police's use of a cell-site simulator is "*direct* government surveillance." *Graham,* 824 F.3d at 426 & n.4.

[21] *See also* Pell & Soghoian, *supra* note 2, at 12 (explaining that active surveillance devices exploit the lack of an authentication mechanism in the 2G phone protocol design).

his or her cellphone or its radios (put it in "airplane mode"), thus forgoing its use as a communication device.

The preceding considerations lead us to conclude that the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search. First, given the potential for location information gathered by a cell-site simulator or other device to reveal sensitive personal facts, people justifiably seek to keep such information private. This is insufficient, in itself, to support our conclusion that the government invaded a legitimate expectation of privacy: Supreme Court precedent makes clear that certain forms of tracking do not invade a reasonable expectation of privacy. *See Knotts*, 460 U.S. at 282 (holding that the use of an electronic device to track a suspect's movements in public spaces did not invade a reasonable expectation of privacy);[22] *see also Karo*, 468 U.S. at 719 (holding that the unlawful use of a device to track movements inside a residence did not necessarily taint the otherwise lawful use of the same device to track the suspects in public).

[22] *But see* (*Antoine*) *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques."); *id.* at 430 (Alito, J., concurring in judgment) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

But in addition to the fact that people reasonably value and hope to protect the privacy of their location information, what necessitates our conclusion is the *method* by which the government obtained the location information in this case. *See Kyllo*, 533 U.S. at 35 n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment."); *United States v. Maynard*, 615 F.3d 544, 566 (D.C. Cir. 2010) ("[W]hen it comes to the Fourth Amendment, means do matter."), *aff'd on other grounds by* (*Antoine*) *Jones*, 565 U.S. 400. Unlike in a situation in which the government determines a person's location through visual surveillance or by employing the older generation of tracking devices, *see Karo*, 468 U.S. at 719; *Knotts*, 460 U.S. at 282, it cannot be argued that "the information obtained by [the government] in this case was . . . readily available and in the public view," *Andrews*, 134 A.3d at 348. The cell-site simulator employed in this case gave the government a powerful person-locating capability that private actors do not have and that, as explained above, the government itself had previously lacked—a capability only superficially analogous to the visual tracking of a suspect.[23] And

[23] We are accordingly unpersuaded by one court's suggestion that using cellular technology to track a suspect is analogous to using "dogs . . . to track a fugitive . . . [by] his scent." *United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012). And our dissenting colleague's suggestion that the search here was permitted under the automobile exception to the Fourth Amendment, see *post* at 86–88, is similarly unconvincing. The dissent argues that under the automobile

(continued…)

the simulator's operation involved exploitation of a security flaw in a device that most people now feel obligated to carry with them at all times. Allowing the government to deploy such a powerful tool without judicial oversight would surely "shrink the realm of guaranteed privacy" far below that which "existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34. It would also place an individual in the difficult position either of accepting the risk that at any moment his or her cellphone could be converted into tracking device or of forgoing "necessary use of" the cellphone. *Tracey*, 152 So. 3d at 523. We thus conclude that under ordinary circumstances, the use of a cell-site simulator to locate a person through his or her cellphone invades the person's actual,[24] legitimate, and

---

(…continued)
exception, police officers could have searched Mr. Jones's car without a warrant and seized "any cell phones in it that might have been contraband or evidence of the crime." *Post* at 88. From this, the dissent claims, it follows that the police had the right to use the cell-site simulator to search or seize Mr. Jones's phone. This argument glosses over the fact that what the cell-site simulator obtained was Mr. Jones's location information. When police search a car under the automobile exception, by contrast, they do not obtain location information—they already *know* the car's location if they are searching it. The dissent also glosses over the fact that the police need probable cause to search a car under the automobile exception. *Tuckson v. United States*, 77 A.3d 357, 366 (D.C. 2013). The police here did not have probable cause to believe that there was evidence of a crime inside Mr. Jones's car until they used the cell-site simulator to locate Mr. Jones's cellphone.

[24] Ordinarily, a person need not do anything affirmative to exhibit an actual subjective expectation that he or she will not be located and tracked by a cell-site simulator. In *Katz*, the defendant was "entitled to assume" that his phone conversation was private based purely on the fact that he had "occupie[d] [the (continued…)

reasonable expectation of privacy in his or her location information and is a search.

The government's argument to the contrary is unpersuasive. The government contends that because a cellphone "must continuously broadcast a signal," a person who carries or uses a cellphone is engaging in "conduct [that] is not calculated to keep [his] location private and . . . thus[] has no reasonable expectation of privacy in his location." The government cites for support *United States v. Wheeler*, 169 F. Supp. 3d 896 (E.D. Wis. 2016), in which the court found that "today, when many Americans own some sort of cell phone and carry it frequently, an individual's expectation that the government could not track his whereabouts over time is [not] reasonable." *Id.* at 908; *see also id.* ("The media is rife with information—and sometimes warnings—about the fact that one's location can be tracked from one's cell phone.").[25] This line of reasoning rests on a

---

(…continued)
phone booth], shut[] the door behind him, and pa[id] the toll." 389 U.S. at 352. Likewise, in *Kyllo*, the Supreme Court found that the use of a thermal imager on the defendant's home violated an expectation of privacy, without any discussion about whether the defendant had taken measures to thwart the effectiveness of the device. 533 U.S. at 40. But in fact in the present case, there was some evidence that Mr. Jones affirmatively sought to keep his location information private: His phone's GPS feature (to the extent it existed) had been disabled.

[25] The government also cites *United States v. Caraballo*, 831 F.3d 95 (2d Cir. 2016), *cert. denied*, 137 S. Ct. 654 (2017), a case in which the police obtained real-time cell-site location information without a warrant. See *supra* note 20. The court approved the officers' actions under the exigency exception. *Caraballo*, 831
(continued…)

misreading of the *Katz* expectation-of-privacy test that construes the test as involving a probabilistic inquiry (an inquiry into whether it is likely—or the public thinks it is likely—that the government *can* access the information in question) rather than a normative one (an inquiry into whether it is consistent with the nation's traditions and values that the government *should* have unfettered access to the information).[26] Contrary to the government's argument, *Katz* makes clear that

---

(…continued)
F.3d at 106. The court stated that "any expectation of privacy that [the defendant] had in his cell-phone location was dubious at best." *Id.* at 105. But this remark was part of a broader exigency analysis, and the court's primary justification for it was the lack of decisive authority on the question. *See id.* at 106 ("[T]he fact that the question of the degree of privacy that adheres to these sorts of information, to date, divides those Circuit courts that have spoken to the issue reinforces the conclusion that the intrusion here was not to an established, core privacy value.").

[26] Moreover, the factual premise of the government's argument is erroneous. The events at issue in this case occurred in 2013, and at that time cell-site simulators were relatively unknown to the public. Law-enforcement agencies around the country that acquired the device had been required (and, for all we know, still continue to be required) to sign nondisclosure agreements with the Federal Bureau of Investigation. *See* Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times, Mar. 15, 2015, https://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html; Pell & Soghoian, *supra* note 2, at 38. Indeed, amici curiae have provided us with a redacted copy of a nondisclosure agreement that the MPD signed. By signing this agreement, the MPD agreed that, among other things, "the equipment/technology and any information related to its functions, operation, and use shall . . . [not be] disclos[ed] . . . to the public in any manner including but not limited to: in press releases, in court documents, during judicial hearings, or during other public forums." *See also Andrews*, 134 A.3d at 338 (detailing a similar agreement signed by the Baltimore City Police Department). There is no evidence in the record that Mr. Jones was aware of the government's secret use of the cell-site simulator and
(continued…)

a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government's capacity to invade his or her privacy. When *Katz* was issued, the public and the courts were well aware of the government's capacity to wiretap and eavesdrop through technological means, yet the Supreme Court did not find this fact determinative of the question whether individuals possess a reasonable expectation of privacy in their conversations. *See Katz*, 389 U.S. at 352 (citing *Olmstead v. United States*, 277 U.S. 438 (1928) (wiretapping), and *Goldman v. United States*, 316 U.S. 129 (1942) (bugging)); *see also* Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. 3, 28 ("In the several years preceding *Katz*, the public had learned of rampant illegal wiretapping from numerous influential books, scholarly articles, and newspaper accounts."). A person's awareness that the government can locate and track him or her using his or her cellphone likewise should not be sufficient to negate the person's otherwise legitimate expectation of privacy. *See also Smith v. Maryland*, 442 U.S. 735, 741 n.5 (1979) ("[W]here an individual's subjective expectations ha[ve] been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection

---

(…continued)
little reason to believe that the public was widely aware of it.

[is].”); 1 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 2.1 (d) (5th ed. 2016) (“[W]hat is involved here is ‘our societal understanding’ regarding what deserves ‘protection from government invasion.’” (quoting *Oliver v. United States*, 466 U.S. 170, 178 (1984))).

The government’s use of the cell-site simulator to locate Mr. Jones was therefore a search.[27] The government did not obtain a warrant and has not argued

[27] We need not rule on Mr. Jones’s alternative argument that the government’s conduct here constituted a search under (*Antoine*) *Jones*, 565 U.S. 400, where the court held that a trespass used to obtain information constitutes a Fourth Amendment search. Mr. Jones makes a plausible argument that the government’s conduct constituted a trespass to his chattel—that is, that the government “intentionally . . . us[ed] or intermeddl[ed]” with his chattel, his cellphone. Restatement (Second) of Torts § 217 (Am. Law Inst. 1965). The government, through the cell-site simulator, coopted Mr. Jones’s phone, forcing it to do something Mr. Jones surely never intended it to do: reveal its identifying and location information to an entity other than a telecommunications provider. Moreover, it is a natural consequence of a cell-site simulator’s use that it will disrupt the operation of the target phone, and there is reason to believe that this happened here, given the records showing Mr. Jones’s seven failed calls. See *supra* note 7. And numerous courts have held that computer hacking and interference with electronic resources can satisfy the elements of common-law trespass to chattels. *See generally* Marjorie A. Shields, Annotation, *Applicability of Common-Law Trespass Actions to Electronic Communications*, 107 A.L.R.5th 549 (2003).

But the question whether the holding of (*Antoine*) *Jones* extends beyond physical trespasses is still an open one. It is unclear, first of all, whether the holding of (*Antoine*) *Jones* depends on “the law of trespass as it existed at the time of the adoption of the Fourth Amendment” or whether new forms of the tort are relevant. 565 U.S. at 426 (Alito, J., concurring in judgment). Assuming that the former is the case, it is also not clear whether “the[] recent decisions [recognizing

(continued…)

that the search "f[ell] within a specific exception to the warrant requirement," and therefore the search was unlawful under the Fourth Amendment. *United States v. Riley*, 134 S. Ct. 2473, 2482 (2014); *see also United States v. Lewis*, 147 A.3d 236, 239 (D.C. 2016) (en banc) ("A search conducted without a warrant is per se unreasonable under the Fourth Amendment unless it falls within a few specific and well-established exceptions." (quoting *United States v. Taylor*, 49 A.3d 818, 821 (D.C. 2012))).[28]

(…continued)
electronic trespass to chattels] represent a change in the law or simply the application of the old tort to new situations." *Id.* at 426–27 (Alito, J., concurring in judgment). Mr. Jones's counsel pointed out during oral argument that courts recognized forms of nonphysical trespass on chattels long before the electronic age, suggesting a possible answer to the second of these questions. *See, e.g.*, *Cole v. Fisher*, 11 Mass. 137 (1814) (holding that the plaintiff could sue for trespass to chattels where the sound of the defendant's gunshot frightened the plaintiff's horse, resulting in damage to the plaintiff's carriage); *see also* W. Page Keeton et al., *Prosser and Keeton on Torts* § 14 n.8 (5th ed. 1984) (citing other cases). Yet we do not have to answer these "vexing" questions today. (*Antoine*) *Jones*, 565 U.S. at 426 (Alito, J., concurring in judgment).

[28] Arguing that "bystanders[']s . . . phones [can be] ensnared by the cell site simulator," see *supra* notes 12 and 15, amici curiae ask us to adopt a requirement that "any cell site simulator warrant must include provisions to minimize collection, retention, and use of bystanders' data." *See In re Application of the United States for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *3–4 (N.D. Ill. Nov. 9, 2015); *In re Search Warrant*, 71 A.3d 1158, 1170 (Vt. 2012) ("Warrants for electronic surveillance routinely set out 'minimization' requirements—procedures for how and under what conditions the electronic surveillance may be conducted—in order to 'afford similar protections to those that are present in the use of conventional warrants authorizing
(continued…)

Our conclusion that the government violated Mr. Jones's Fourth Amendment rights is not the end of our inquiry. We must decide whether Mr. Jones is entitled to a remedy, and if so what the scope of that remedy should be. As a general matter, the "[e]xclusionary rule . . . forbids the use of improperly obtained evidence at trial." *Herring v. United States*, 555 U.S. 135, 139 (2009). "[T]his judicially created rule is 'designed to safeguard Fourth Amendment rights generally through its deterrent effect.'" *Id.* at 139–40 (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)). The government argues that the exclusionary rule does not apply in this case, invoking the inevitable-discovery doctrine, good-faith exception, and a change in its policies concerning the use of cell-site simulators. The government also argues that much of the evidence that Mr. Jones wants excluded does not fall within the scope of the exclusionary rule—that it is not "fruit of the poisonous tree." *Wong Sun v. United States*, 371 U.S. 471, 488 (1963). We first address the inevitable-discovery doctrine.

B. Inevitable-Discovery Doctrine

(…continued)
the seizure of tangible evidence.'" (quoting *Berger v. New York*, 388 U.S. 41, 57 (1967)) (brackets removed)). The issue of interference with third parties' phones is not before us in this appeal, however.

The inevitable-discovery doctrine "shields illegally obtained evidence from the exclusionary rule if the government can show, by a preponderance of the evidence, that the evidence 'ultimately or inevitably *would* have been discovered by lawful means.'" *Gore v. United States*, 145 A.3d 540, 548 (D.C. 2016) (quoting *Hicks v. United States*, 730 A.2d 657, 659 (D.C. 1999)); *see also Nix v. Williams*, 467 U.S. 431 (1984). To avail itself of the inevitable-discovery doctrine, the government must prove two distinct elements: (1) that "the lawful process which would have ended in the inevitable discovery . . . ha[d] commenced before the constitutionally invalid seizure," and (2) that there is a "'requisite actuality' that the discovery would have ultimately been made by lawful means." *Hicks*, 730 A.2d at 659 (quoting *Douglas-Bey v. United States*, 490 A.2d 1137, 1139 n.6 (D.C. 1985), and *Hilliard v. United States*, 638 A.2d 698, 707 (D.C. 1994)) (brackets and ellipsis removed).

The trial court found that "had [the police] switched [the cell-site simulator] over to use the [complainant's phone] . . . they would have eventually gotten to the exact same place because the phones were together." Assuming for the sake of argument that the hearing evidence supports this finding,[29] we agree with the trial

[29] Mr. Jones argues that this finding was clearly erroneous because "[t]he government presented no expert testimony about the functioning of the cell site (continued…)

court that this finding justifies a conclusion that there was a separate lawful means by which the police *could* have captured Mr. Jones and recovered the evidence used against him at trial.[30] The finding is insufficient, however, to support a conclusion that the police *would* have captured Mr. Jones—which is what the inevitable-discovery doctrine requires.

The undisputed evidence in the record shows that the MPD possessed only a single operating cell-site simulator,[31] and that it could only be used to locate a single phone at a time. The police used it to search for Mr. Jones's cellphone. Thus, the police's search for the complainant's cellphone—the lawful process—never occurred. If the lawful search never occurred, it did not "commence[] before

---

(…continued)
simulator, choosing instead to present only lay testimony [by Sergeant Perkins] about how the field operators use the device." In Mr. Jones's view, "there is no evidence in the record about the failure rate of the cell site simulator or whether it statistically works better with certain models of phones or on certain networks."

[30] In this regard, we note that not only did Mr. Jones concede that he lacked standing to contest a search involving the complainant's phone, but also the record suggests that the complainant consented to the police's tracking of her phone. *See United States v. Johnson*, 380 F.3d 1013, 1017 (7th Cir. 2004) (holding that to rely on the inevitable-discovery doctrine the government must prove a lawful means by which it would have obtained the evidence, and that it is insufficient to prove merely that "the evidence would have been discovered as a consequence of [an] illegal search of [a third party], to which [the defendant] could not object").

[31] The MPD owned another unit, but it was not working properly the day of the search.

the constitutionally invalid seizure" of Mr. Jones. *Hicks*, 730 A.2d at 659 (quoting *Douglas-Bey*, 490 A.2d at 1139 n.6).

The government disagrees with this conclusion and argues that because the police had tracked the complainant's phone using real-time location information from the provider and had obtained her phone's identifying information, they "had begun the process necessary to locate her phone with the cell-[s]ite simulator." Even if we agreed that these steps constituted the commencement of a lawful process, we would nonetheless find the second element of the inevitable-discovery test—the "requisite actuality" that the process would have led to the discovery of Mr. Jones—lacking. This is because the police either suspended or abandoned the purported lawful process when they chose to deploy the only operational cell-site simulator in their possession on Mr. Jones's phone.

This court has found the inevitable-discovery doctrine applicable in cases in which the police engaged in lawful and unlawful processes in parallel. *See Pinkney v. United States*, 851 A.2d 479, 495 (D.C. 2004); *McFerguson v. United States*, 770 A.2d 66, 74–75 (D.C. 2001); *Hicks*, 730 A.2d at 662. Had the unlawful process not occurred in these cases, the lawful one would inevitably have produced the same evidentiary result. But here the government is asking us to find inevitable discovery where the police had mutually exclusive options and, for whatever

reason, chose the option that turned out to be unlawful. The inevitable-discovery doctrine does not apply in this type of situation. *See Gore*, 145 A.3d at 549 n.32 ("[T]he argument that 'if we hadn't done it wrong, we would have done it right' is far from compelling." (quoting 6 LaFave, *supra*, § 11.4 (a)) (internal quotation marks omitted)).[32]

---

[32] Unlike our dissenting colleague, we are not persuaded by the government's alternative argument that because Mr. Jones was carrying the stolen phones, which could have been located and tracked lawfully (it is assumed), Mr. Jones had no expectation of privacy in his location. This argument was not raised in the initial briefing or in the trial court—it was first raised at oral argument before this court in response to questions from the bench. Although after oral argument we requested supplemental briefing on this argument, we ultimately conclude that the government's failure to present it at an earlier stage constitutes a waiver of the argument under the circumstances of this case. *See Tuckson v. United States*, 77 A.3d 357, 366 (D.C. 2013); *Rose v. United States*, 629 A.2d 526, 535 (D.C. 1993); *see also Greenlaw v. United States*, 554 U.S. 237, 244 (2008) ("We wait for cases to come to us, and when they do we normally decide only questions presented by the parties. Counsel almost always know a great deal more about their cases than we do, and this must be particularly true of counsel for the United States, the richest, most powerful, and best represented litigant to appear before us." (quoting *United States v. Samuels*, 808 F.2d 1298, 1301 (8th Cir. 1987) (Arnold, J., concurring in denial of rehearing en banc))). In any case, the argument is unpersuasive because, as we have explained above, "[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Kyllo*, 533 U.S. at 35 n.2; *see also Maynard*, 615 F.3d at 566. And as amici have cogently argued in their supplemental submission, "[c]onsidering as part of the reasonable-expectation-of-privacy inquiry the availability of alternative means to gather information would collapse inevitable discovery into the reasonable-expectation question in a manner that would radically transform both doctrines." As amici explain, were we to adopt the government's—and the dissent's—novel theory of

(continued…)

C. Good-Faith Exception

We turn next to the government's argument that application of the exclusionary rule here "would not meaningfully deter police misconduct" because the use of the cell-site simulator to locate Mr. Jones was "not the type of 'flagrant' abuse for which the exclusionary rule was designed." In support of this argument, the government notes that Sergeant Perkins and his team believed "exigent circumstances existed" and asserts that "at the time of this incident, no court had held that using a simulator to locate a phone violates the Fourth Amendment." The government further points out that the police received judicial approval for various secondary searches of the evidence recovered from Mr. Jones and Ms. Williams at the time of Mr. Jones's arrest. Specifically, the police obtained warrants to search Mr. Jones's Saturn and the phones they recovered from Mr. Jones and Ms. Williams, and secured a court order to take a buccal swab from Mr. Jones.

Although it does not explicitly say so, the government is invoking the

---

(…continued)
affirmance, "the contours of the inevitable discovery doctrine, a carefully crafted exception to the exclusionary rule with strict requirements, would be subject to end-runs, because the possibility of an alternative means of discovery could often be repackaged as a reason to reject an expectation of privacy in the first place" (citation omitted).

"good-faith exception." *Davis v. United States*, 564 U.S. 229, 239 (2011). The Supreme Court first recognized this exception in *United States v. Leon*, 468 U.S. 897 (1984), holding that "evidence obtained [by the police] in objectively reasonable reliance on a subsequently invalidated search warrant" is not subject to the exclusionary rule. *Id.* at 922. This holding was based on the premise that "the deterrence rationale [for exclusion] loses much of its force" "when the police act with an objectively reasonable good-faith belief that their conduct is lawful." *Davis*, 564 U.S. at 252; *id.* at 238 (quoting *Leon*, 468 U.S. at 909, 919) (internal quotation marks omitted). The Court has since extended the good-faith exception to apply in various other situations involving nonculpable or merely negligent law-enforcement conduct. *See, e.g.*, *id.* at 239–40 (holding that the good-faith exception applies "when the police conduct a search in objectively reasonable reliance on binding judicial precedent"); *Herring*, 555 U.S. at 136 (holding that the good-faith exception applied to evidence obtained in a search incident to arrest where the officer "reasonably believe[d] there [wa]s an outstanding arrest warrant" for the defendant, but where "that belief turn[ed] out to be wrong because of a negligent bookkeeping error by another police employee").

The Supreme Court has not, however, recognized the applicability of the good-faith exception in a situation remotely like the present one—where the

police, not acting pursuant to a seemingly valid warrant, statute, or court opinion, conducted an unlawful search using a secret technology that they had shielded from judicial oversight and public scrutiny. See *supra* note 26. Indeed, assuming the police believed the warrantless use of the cell-site simulator to be lawful, they could not have reasonably relied on that belief, given the secrecy surrounding the device and the lack of law on the issue.[33] And the government does not argue that the police officers' mistaken belief that exigent circumstances existed was reasonable or cite any case law that would support such an argument.

The fact that some of the evidence was obtained in secondary searches pursuant to warrants and a court order does not change things. The police's reliance on the warrants and order was not objectively reasonable because the warrants and order were based on information obtained in violation of Mr. Jones's Fourth Amendment rights. *See Evans v. United States*, 122 A.3d 876, 886 (D.C. 2015) ("The subsequent issuance of [a] search warrant . . . , based on information [illegally] obtained . . . , d[oes] not operate to attenuate the [original] illegality.").[34]

---

[33] The Supreme Court has implicitly foreclosed the government's argument that police can reasonably conclude from the complete lack of judicial precedent that their conduct is lawful. *See Davis*, 564 U.S. at 248 (suggesting that the good-faith exception for police reliance on binding judicial precedent would not apply where "the precedent is distinguishable").

[34] The government cites *United States v. McClain*, 444 F.3d 556 (6th Cir.

(continued…)

Thus, the evidence the police obtained through their warrantless use of the cell-site simulator is not subject to the good-faith exception.

D. Change in Department of Justice Policy

The government's final argument for not applying the exclusionary rule is that a change in Department of Justice (DOJ) policy has diminished the likelihood that excluding the evidence in this case will deter misconduct in the future. The government asserts that the MPD is bound by a new DOJ policy to "obtain a search warrant supported by probable cause" before deploying a cell-site simulator. Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology at 3–4 (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download.

(…continued)
2006), in which the court declined to apply the exclusionary rule where officers conducted a search pursuant to a warrant based in large part on information that had been illegally gathered. This court's holding in *Evans* precludes us from following *McClain*. And in any case, *McClain* is distinguishable because there the "warrant affidavit fully disclosed to a neutral and detached magistrate the circumstances surrounding the initial [illegal] search." *Id.* at 566. Here, by contrast, the police did not disclose in their applications for the warrants and order that they had deployed a cell-site simulator to locate Mr. Jones. Indeed, in the otherwise lengthy affidavit for the warrants, the officers' search for Mr. Jones is described in a single sentence: "[T]he Defendant was located by members of the Washington, D.C. Metropolitan Police Department . . . ." The government cannot rely on the *Leon* good-faith exception when the police have not been "frank with the magistrate in proceedings to obtain the warrant." *United States v. Reilly*, 76 F.3d 1271, 1273 (2d Cir.), *on reh'g*, 91 F.3d 331 (2d Cir. 1996).

The government did not develop this argument in the trial court—and could not have, as the DOJ policy had not yet been issued—and we do not find it persuasive. The government has not cited any case in which a court has declined to apply the exclusionary rule based on the government's representation that it will not engage in unlawful conduct in the future. The government cites *Blair v. United States*, 114 A.3d 960 (D.C. 2015), but in that case we relied on a change in a statute that eliminated the need to deter subsequent violations, not a mere change in policy. *Id.* at 973–74. And given that the DOJ policy memorandum does not describe any sort of enforcement mechanism that would ensure compliance with the policy, and given that the present administration or a subsequent one may well revise this policy, we are not convinced that the need to deter future constitutional violations is lacking.

E. Fruit of the Poisonous Tree

Having decided that the exclusionary rule applies in this case, we must now decide which evidence should be excluded as "fruit of the poisonous tree" of the illegal search.[35] *Wong Sun*, 371 U.S. at 488. In deciding whether evidence

[35] In the trial court, Mr. Jones specifically moved to "[s]uppress [i]dentifications, [s]tatements, and [t]angible evidence" resulting from the illegal search. The evidence and testimony that Mr. Jones identifies as fruits of the (continued…)

constitutes fruit of the poisonous tree, the critical inquiry is whether "the evidence . . . has been come at by exploitation of th[e] illegality or instead by means sufficiently distinguishable to be purged of the primary taint." *Wong Sun*, 371 U.S. at 488 (quoting John Maguire, *Evidence of Guilt* 221 (1959)); *see also Wilson v. United States*, 102 A.3d 751, 753 (D.C. 2014). The court considers "[t]he temporal proximity of the [illegality] and the [acquisition of the evidence], the presence of intervening circumstances, and, particularly, the purpose and flagrancy of the official misconduct." *Brown v. Illinois*, 422 U.S. 590, 603–04 (1975) (citations and footnote omitted); *see also Gordon v. United States*, 120 A.3d 73, 85 (D.C. 2015).

Mr. Jones argues that the following evidence and testimony should have been excluded as fruits of the poisonous tree: his knife, a statement he made to the

---

(…continued)
poisonous tree in this appeal clearly fall within these categories, and the government could not have reasonably doubted that Mr. Jones intended to have them suppressed. The government had a "full and fair opportunity" in the trial court to litigate this matter. *Barnett v. United States*, 525 A.2d 197, 200 (D.C. 1987). And the record before us is "of amply sufficient detail and depth" to permit us to decide the scope of the exclusionary rule as a matter of law. *Brown v. Illinois*, 422 U.S. 590, 604 (1975). We thus (except as to the testimony of Ms. Williams, see *infra* note 41) decline the government's request that we remand the case so that the trial court can "hold hearings, make factual findings of fact, and reach legal conclusions on the application of the fruit-of-the-poisonous-tree doctrine."

police at the scene of his arrest, cellphones recovered from Ms. Williams's purse at the scene of the arrest, evidence (including cellphones) recovered from his car (the Saturn) pursuant to a warrant, data extracted from the various cellphones pursuant to warrants, the testimony of Ms. Williams, the later photo-array identification of Mr. Jones by one of the complainants, a DNA profile generated from a buccal swab of Mr. Jones (a month after his arrest), and a photograph of Mr. Jones's groin.[36] The government "agrees that some, but not all, of the . . . evidence [identified by Mr. Jones] is a fruit of the alleged poisonous tree." The government only specifically objects to classifying (1) Mr. Jones's statement to the police, (2) the cellphones recovered from Ms. Williams's purse, and (3) Ms. Williams's testimony as fruits of the poisonous tree.

1. Prince Jones's Statement

Mr. Jones made an incriminating statement to the police at the scene of the arrest: When asked what his address was, Mr. Jones gave the address of one of the sexual-assault complainants. The government argues that this statement should not be suppressed as a fruit of the unlawful cell-site-simulator search because "[i]t

[36] One of the complainants testified at trial about the appearance of Mr. Jones's genital area, and the photograph of Mr. Jones's groin was admitted in evidence at trial.

would make little sense to suppress evidence obtained merely as part of a routine booking procedure." *See Thomas v. United States*, 731 A.2d 415, 421 (D.C. 1999) (recognizing "a routine booking question exception" to the rule of *Miranda v. Arizona*, 384 U.S. 436 (1966)). We reject this argument. That the question about Mr. Jones's address was otherwise proper does not negate the fact that very little time and no substantial intervening circumstances separated the illegal search from Mr. Jones's incriminating response. *See United States v. Olivares-Rangel*, 458 F.3d 1104, 1112 (10th Cir. 2006). Mr. Jones's statement was a direct product of the unlawful search and is thus excludable as fruit of the poisonous tree.

2. Cellphones from Nora Williams's Purse

When the police located Mr. Jones and Ms. Williams, they searched Ms. Williams's purse and found several cellphones, including two of the complainants' phones and Mr. Jones's phone. The government argues that the contents of Ms. Williams's purse are not fruits of the poisonous tree because Mr. Jones did "not have a reasonable expectation of privacy in the contents of Ms. Williams's purse" and because "Ms. Williams gave the officers consent to search her purse."

Preliminarily, Mr. Jones's expectation of privacy (or lack thereof) in Ms. Williams's purse is not a material consideration in the fruit-of-the-poisonous-tree

analysis. As one court has explained, "[w]hile the fruit of the poisonous tree doctrine applies only when the defendant has standing regarding the Fourth Amendment *violation* which constitutes the poisonous tree, the law imposes no separate standing requirement regarding the *evidence* which constitutes the fruit of that poisonous tree."[37] *Olivares-Rangel*, 458 F.3d at 1117 (citation omitted); *see also* 6 LaFave, *supra*, § 11.4 ("If the defendant [has] standing with respect to the poisonous tree, that alone suffices . . . .").

The factors in *Brown*, 422 U.S. at 604, moreover, compel a conclusion that the contents of Ms. Williams's purse are fruits of the poisonous tree. First, as the search of Ms. Williams's purse occurred at the scene of Mr. Jones's apprehension and arrest, very little time passed between the police's unlawful cell-site-simulator search and their recovery of the evidence from Ms. Williams's purse.

---

[37] *United States v. Bowley*, 435 F.3d 426, 430–31 (3d Cir. 2006), and *United States v. Pineda-Chinchilla*, 712 F.2d 942, 943–44 (5th Cir. 1983), cited by the government, stand only for the narrow proposition that a defendant cannot suppress the contents of his immigration file even if the prosecuting authority's discovery of that file or its connection to the defendant was based on evidence gathered in an illegal search or seizure. Thus, even if we were to find these cases persuasive, *but see* 6 LaFave, *supra*, § 11.4 & n.22, they would not support the proposition that a defendant must always—or even usually—have standing in a particular item of evidence to have it suppressed as a fruit of an illegal search or seizure.

Second, Ms. Williams's supposed consent was not a significant intervening circumstance. According to Detective Pulliam, Ms. Williams consented only after the police presented her with the following options: the police "would either have to take the purse and put it into police custody until [they] could get a search warrant and then search it or . . . she could give [the police] consent to search it." Given this threat and the fact that her boyfriend, Mr. Jones, had just been arrested in her presence, Ms. Williams's consent was not sufficiently "the product of free will [to] break . . . the causal connection between the illegality and the" search of the purse. *Brown*, 422 U.S. at 603; *cf. Utah v. Strieff*, 136 S. Ct. 2056, 2062 (2016) (holding that a valid arrest warrant "entirely unconnected with the [illegal] stop" was a sufficient intervening circumstance); 4 LaFave, *supra*, § 8.2 (c) (explaining that a person's consent to a search may be involuntary where the police, "'trading on' a prior Fourth Amendment violation," have "threat[ened] to seek a warrant").[38]

And third, although the police officers' warrantless use of the cell-site

[38] The proper inquiry here is not whether Ms. Williams's consent was a valid waiver of her own rights, but rather whether it constituted an intervening circumstance sufficient to purge the taint of the illegal search. Thus, we need not decide whether Ms. Williams could have had the evidence excluded had she herself been tried. *See generally* 4 LaFave, *supra*, § 8.2 (c) (discussing Fourth Amendment cases in which "the police have obtained consent to search after threatening that if consent were not given they would proceed to seek or obtain a search warrant").

simulator here was not flagrant misconduct,[39] recovery of Mr. Jones's cellphone and the complainants' phones was undoubtedly one of the officers' purposes in deploying the cell-site simulator. The cell-site simulator is used to locate and track *phones* after all. The contents of Ms. Williams's purse thus "bear a . . . close relationship to the underlying illegality." *Gordon*, 120 A.3d at 85 (quoting *New York v. Harris*, 495 U.S. 14, 19 (1990)).[40]

3. Nora Williams's Testimony[41]

Mr. Jones argues that Ms. Williams should have been barred from testifying

---

[39] But see *supra* text accompanying note 33.

[40] The government contends that even if the cellphones in Ms. Williams's purse are fruits of the poisonous tree, the "call detail records and location information obtained from the provider" for the cellphones "are not subject to exclusion." Mr. Jones has not argued otherwise, and we see no reason for classifying this information as fruit of the poisonous tree.

The government also represents in its brief that "the government received an unsolicited offender hit from the FBI's Combined DNA Index System ('CODIS') indicating that a sample obtained from [Mr. Jones] in connection with [a] prior Maryland conviction matches the crime scene sample obtained in this case." Assuming that the government can demonstrate this in the trial court, we agree with the government that it "should not be precluded from seeking another buccal swab [from Mr. Jones] based on the independent and untainted CODIS hit." This CODIS hit would not be a fruit of the illegal search.

[41] This part does not constitute the opinion of the court, as it is not joined by *Associate Judge* THOMPSON or *Senior Judge* FARRELL.

for the government at trial. The government disagrees, arguing that "[t]here was sufficient attenuation between the search and Ms. Williams's testimony to dissipate any taint" and that "the government would have inevitably discovered Ms. Williams through independent sources."

In *United States v. Ceccolini*, 435 U.S. 268 (1978), the Supreme Court recognized factors pertinent to the determination of whether a witness's testimony should be barred as fruit of the poisonous tree: (1) whether "the testimony given by the witness was an act of her own free will in no way coerced," (2) whether evidence gathered or information learned as a result of the illegal search was used to question the witness, (3) whether "[s]ubstantial periods of time elapsed between the time of the illegal search and the initial contact with the witness . . . and between the [initial contact] and the testimony at trial," (4) whether the witness and "her relationship with the [defendant] were well known" to the police before the illegal search, and (5) whether the officers conducting the illegal search did so with the "intent of finding a willing and knowledgeable witness to testify against" the defendant. *Id.* at 279–80; *see also* 6 LaFave, *supra*, § 11.4 (i). These factors weigh in favor of excluding Ms. Williams's testimony.

First, it is undisputed that Ms. Williams was not a willing witness for the government. As the government points out, Ms. Williams was initially "not

forthcoming about her knowledge and use of the . . . items" stolen from the complainants, and only testified after "the government sought and received a court order granting her immunity." Ms. Williams testified at trial that after she was granted immunity, she testified for the grand jury "[b]ecause [she] had no choice." She expressed unhappiness about having to testify against Mr. Jones at trial, stating that she "didn't want to go against him."

Second, the government admits that the police "confronted [Ms. Williams] with the fact that stolen phones and other items were recovered from her purse and from the car." This evidence, as explained above, was the product of the illegal search. The government's attempt to minimize the significance of this fact is unpersuasive. The government contends that the "illegally obtained evidence ultimately did not play a great role in obtaining Ms. Williams's testimony" and that it was the grant of immunity that was the decisive factor. But this argument fails to address the fact that the police questioned Ms. Williams before she was immunized, and is also speculative: It is plausible—indeed, likely—that both the grant of immunity and fact that Ms. Williams was found red-handed with the proceeds of the robberies played significant roles in her decision to testify.

Third, a very short period of time passed between the illegal search and Ms. Williams's first contact with the police. Indeed, Ms. Williams was present at Mr.

Jones's arrest and was questioned at the scene. *See United States v. Ramirez-Sandoval*, 872 F.2d 1392, 1397 (9th Cir. 1989). Approximately a year passed between the police's initial contact with Ms. Williams and her testimony at trial, but a lengthy period between first contact and trial is almost always present in a criminal case, and this time period is less significant than the time period between the search and first contact. Moreover, the witness's initial statements to the police will often significantly constrain the witness's testimony at trial because the initial statements can be used to impeach the witness or bolster his or her testimony. *See* 1 Kenneth S. Broun et al., *McCormick on Evidence* § 34 (7th ed. 2016) (discussing the procedure of impeaching a witness with a prior inconsistent statement); *id.* § 47 (discussing the procedure of supporting a witness with a prior consistent statement).

Fourth, although at trial the government offered in evidence surveillance footage of Ms. Williams using an ATM card stolen from one of the complainants, at the suppression hearing the government neither presented evidence nor argued that the police had this video before they conducted the illegal cell-site-simulator search or that the video would have enabled the police to locate Ms. Williams. Thus, based on the record before the court, it is not possible to conclude that the police were aware of Ms. Williams or her relationship with Mr. Jones before they

located her through the illegal search. See also *supra* note 35.

The remaining factor favors the government. Specifically, there is no reason to believe that the police intended their use of the cell-site simulator to result in the discovery of a witness for the government. Rather, the record before the court suggests that the police were trying to locate Mr. Jones—and, as a necessary consequence of their use of cellphone tracking, Mr. Jones's cellphone. Nonetheless, because the other four factors strongly weigh in favor of suppression, there is "a close[], . . . direct link between the illegality and [Ms. Williams's] testimony." *Ceccolini*, 435 U.S. at 278.

F. Harmless-Error Analysis

The introduction of evidence collected in violation of Mr. Jones's Fourth Amendment right to be free from unreasonable searches and seizures is constitutional error. So we must reverse Mr. Jones's convictions unless the government has "prove[d] beyond a reasonable doubt that the error . . . did not contribute to the verdict." *Chapman v. California*, 386 U.S. 18, 24 (1967). Because we have concluded that the fruits identified by Mr. Jones should have

been excluded at his trial,[42] and because these fruits comprised some of the most damning evidence against him, we need not undertake a detailed analysis to conclude that the erroneous admission of these fruits at trial was not harmless beyond a reasonable doubt. The government does not argue otherwise.

III. Conclusion

For the foregoing reasons, we reverse the judgment of the trial court and remand for further proceedings consistent with this opinion.

[42] To be entirely accurate, we have reached this conclusion with respect to all of the purported fruits except for the testimony of Ms. Williams. See *supra* note 41. The conclusion that the error was not harmless beyond a reasonable doubt nonetheless stands.

FARRELL, *Senior Judge*, concurring in part and concurring in the judgment: I agree with Judge Beckwith that the police' use of the cell-site simulator to discover appellant's precise location violated the Fourth Amendment because it was a "search" requiring a warrant. My analysis of why that is so is more limited than Judge Beckwith's, however. I also agree that the government has not shown that the fruits of the use of the simulator would have been inevitably discovered by lawful means, and that this is not the sort of case in which the Supreme Court has found that suppression of the fruits would serve no deterrent purpose. Further, except that I would not decide whether the testimony of Nora Williams should have been suppressed, I agree that the evidence discussed in part II. E. of Judge Beckwith's opinion was suppressible fruit of the warrantless search. Finally, I explain briefly why I am not persuaded by Judge Thompson's position in dissent that no search at all under the Fourth Amendment took place.

I.

As to inevitable discovery, a key argument by appellee in its original brief, I agree that the government has failed to show the "requisite actuality," *Hicks v. United States*, 730 A.2d 657, 659 (D.C. 1999), that tracking the complainants' cellphones with the simulator, had that taken place, would have led to the same seizure of incriminating evidence. The government in its brief states that

appellant's and the complainants' cellphones "were ultimately found together in appellant's car," and that since "the simulator was close enough to locate one of the phones, it inevitably was close enough to locate the other" (Appellee's Brief at 32). But this analysis is troublesome partly because it relies on the fruits of the actual simulator use. *See* 6 WAYNE R. LAFAVE, *Search and Seizure*: *A Treatise on the Fourth Amendment* § 11.4 (a), at 283 (5th ed. 2016) ("'[T]he fact making discovery inevitable must arise from circumstances other than those disclosed by the illegal search itself.'"). Moreover, the police began using the simulator a considerable length of time after appellant had come into possession of the complainants' cellphones, and even then some 30–45 minutes elapsed before the simulator directed them to appellant's car and cellphone. So there is too much surmise, I submit, in the reasoning that if the police had used the simulator to locate the complainants' phones instead, those phones would still have been in appellant's possession or, if so, in a powered-on condition enabling their detection.

II.

The dispositive issue, then, is whether the use of the cell-site simulator was a "search" requiring the police to have obtained a warrant beforehand (in the now-conceded absence of exigent circumstances). To answer that question it is enough, I believe, to know how the simulator learns of a target cellphone's location. It does

so by effectively commandeering the cellphone as a police investigative tool in the way Judge Beckwith describes, namely, by "actively induc[ing] the phone to divulge its identifying information," *ante* at 17, from which the phone's direction and distance relative to the simulator can be determined. This process of "grabbing" the target phone and making it the instrument of its own locational disclosure explains why the government's primary reliance on the third-party doctrine of *Smith v. Maryland*, 442 U.S. 735 (1979)—"*Smith* . . . is controlling here" (Appellee's Brief at 23)—to argue that appellant had no reasonable expectation of privacy in the police' use of his phone is unpersuasive.

Smith held that an individual enjoys no Fourth Amendment protection "in information he voluntarily turns over to [a] third part[y]." *Id*. at 743–44. The reason is that by "revealing his affairs to another" an individual "takes the risk . . . that the information will be conveyed by that person to the government." *United States v. Miller*, 425 U.S. 435, 443 (1976). Recently the Fourth Circuit applied the third-party doctrine to hold that the government's acquisition of historical cell-site location information (CSLI) from a suspect's cellphone provider is not a search under the Fourth Amendment. *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc). Although that issue remains an open one in this court, and the Supreme Court is expected to decide it this term, *Carpenter v. United States*, No.

16-402, *cert. granted* June 5, 2017, *Graham*'*s* analysis at least serves by comparison to show why the use of a cell-site simulator to locate appellant's phone compels a different conclusion.[1]

Graham distinguished prior Supreme Court cases involving "direct government surveillance" (*e.g.*, *United States v. Karo*, 468 U.S. 705 (1984); *United States v. Jones*, 565 U.S. 400 (2012)) from the situation where the government "obtains, from a third party, the third party's records, which permit the government to deduce location information." 824 F.3d at 426. Because CSLI is information the individual has already "'exposed' . . . to the phone company's 'equipment in the ordinary course of business,'" that person has "'assumed the risk' that the phone company would disclose their information to the government." *Id*. at 427-28 (quoting *Smith*, 442 U.S. at 744). The government thus "does not engage in a Fourth Amendment 'search' when it acquires" CSLI from the cellphone provider. *Id.* at 427. But in contrast to this passive "acquir[ing]" or "obtain[ing]" of CSLI, direct government surveillance of a cellphone does constitute a search, as when — the Fourth Circuit observed by footnote — "the government uses cell-site

[1] The fact that the Supreme Court will take up cell phone technology in relation to the Fourth Amendment is alone reason for us to decide the present issue narrowly and not opine in broad stokes about privacy and electronic information, locational or other.

simulators . . . to *directly* intercept CSLI instead of obtaining CSLI records from phone companies." *Id*. at 426 n.4

When the police seek and obtain locational information by directly interacting with, indeed by taking functional control of, a suspect's cellphone through a simulator, it cannot reasonably be said that the phone user has "voluntarily conveyed" locational information to anyone and thereby relinquished a reasonable expectation of privacy in the information. *Smith*, 442 U.S. at 744. Police requests for cellphone location data held by a third party, however the Supreme Court resolves that privacy issue, are not comparable to forcing a cellphone to disclose its own identifying data. The police located appellant's phone by effectively making it a self-investigative tool. Any reduced expectation of privacy an individual accepts by entering the cellphone world does not extend to co-optation of that kind.

III.

I also agree that suppression of most of the fruits of the unlawful search here will "pay its way," *United States v. Leon*, 468 U.S. 897, 919 (1984), under the "cost-benefit analysis in exclusion cases." *Davis v. United States*, 564 U.S. 229, 238 (2011). As Judge Beckwith points out, the government has not sought to show

that any belief the police had that there was no time to pursue a search warrant was objectively reasonable, albeit mistaken. The record suggests, to the contrary, that the police decided to forgo the warrant process either believing — unreasonably, in the virtual absence of relevant court decisions—that no Fourth Amendment intrusion was involved or to honor a proprietary agreement for secrecy in using the device. See *ante* at 22 n.26. Thus, the search cannot be said to have involved the sort of "'isolated,' 'nonrecurring' police negligence . . . [that] lacks the culpability" required to justify suppression, *Davis*, 564 U.S. at 239 (citing *Herring v. United States*, 555 U.S. 135, 137 (2009)), even if it entailed no "'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights." *Davis*, 564 U.S. at 238. The unlawfulness here was not like the "err[or] in maintaining records in a warrant database," *id.* at 239, involved in both *Arizona v. Evans*, 514 U.S. 1 (1955), *Herring*, *supra*; nor was it comparable to the mistaken but "objectively reasonable reliance on binding judicial precedent" in *Davis*, 564 at 239.

Exclusion of evidence was thus a proper remedy here, except that, unlike Judge Beckwith, I would not decide whether the testimony of Nora Williams should have been suppressed. Her testimony was given more than a year after the illegal search and only after, now represented by counsel, she had received use immunity for her testimony. Those circumstances present a difficult question of

attenuation that we need not reach, because the admission of the immediate fruits of the search was not harmless error and requires reversal. In any new trial the parties can brief and the trial court resolve the issue of the admissibility of Williams' testimony, should the issue arise.

Finally, I am not persuaded by Judge Thompson's position in dissent that no Fourth Amendment search took place because appellant had no "reasonable expectation that the location of his cell phone would remain private while he was traveling *on the public roads with a powered-on, stolen cell phone*." *Post* at 68 (emphasis added). That contention, resting on appellant's presumed awareness of how the police might have located him (via the stolen cell phone) but did not, closely resembles the inevitable discovery argument we have rejected. *See* Appellee's Supp. Brief at 6 ("[A]ppellant has effectively conceded that the use of a cell site simulator to locate the stolen Sprint cell phone *would have been* a 'lawful investigative process'" (emphasis added)). Moreover, the theory appears to assume a conclusion of wrongdoing—that appellant possessed a "stolen" phone—disputed by appellant's not-guilty plea at the time the suppression motion was litigated.[2] It would be unfair to hold that, in moving to suppress the fruits of the

[2] In *McFerguson v. United States*, 770 A.2d 66 (D.C. 2001), this court rejected the argument that "society would [not] impute a reasonable expectation of (continued…)

search of *his* cell phone, appellant assumed the burden of proving that his possession of another's phone was lawful—the issue of guilty possession *vel non* on which the government would have the burden of proof at trial. The dissent's ingenious argument for why no search took place is too fraught with difficulty to provide a basis for admitting in evidence the fruits of the warrantless manipulation of appellant's cell phone.

THOMPSON, *Associate Judge*, dissenting: My colleagues in the majority are "properly and commendably concerned about the threats to privacy that may flow from advances in the technology available to the law enforcement profession."[1] I share their concern, but I am not persuaded to their conclusion in this case, which I believe rests on a too-generic description of the facts surrounding use of the cell-site simulator involved here. My colleagues express concern that "[a] cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will." *Ante* at 17. But this

(…continued)
privacy to a burglar running away from the crime scene carrying in plain view a distinctively marked shopping bag . . . stolen from the burgled residence and filled with the victim's property." *Id.* at 71 (internal quotation marks and ellipses omitted). The government's argument, we said, "assumes the very facts that were to be proved at trial — that [the defendant] was fleeing with goods he had stolen in the burglary." *Id.*

[1] *Kyllo v. United States*, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting).

case is about far more particular and narrow facts, and here, as always, Fourth Amendment analysis must be "extremely fact-specific";[2] "[i]t is important to be clear about what occurred in this case[.]"[3]

Described with the necessary specificity, this case is about the following: Police had near real-time cell-site location information from cell phone providers[4] that a cell phone, which police knew (from a review of victim call records) had been used by the perpetrator of two recent sexual assaults and related robberies to lure his victims, was traveling on the public streets together with a powered-on[5] Sprint cell phone (the "stolen phone") that the perpetrator had stolen from one of the robbery victims, and was in the vicinity of the Minnesota Avenue Metro

---

[2] *In re Application of United States for Historical Cell Site Data*, 724 F.3d 600, 603 (5th Cir. 2013) (internal quotation marks omitted).

[3] *United States v. Jones*, 565 U.S. 400, 404 (2012).

[4] As the majority opinion notes, *ante* at 16 n.20, appellant has not argued in this appeal that his Fourth Amendment rights were violated when the government obtained cell-site location information from cellular providers. *See United States v. Graham*, 824 F.3d 421, 428 (4th Cir. 2016) (joining other circuit courts in holding that "individuals do not have a reasonable expectation of privacy in historical [cell-site location information] that the government obtains from cell phone service providers").

[5] Police Technical Services Unit ("TSU") Sergeant Perkins testified at the suppression hearing in this case that, as long as it's "powered on," a cell phone "is constantly transmitting to and receiving from a tower."

station; and, after driving to the area near that station, law enforcement officers using a cell-site simulator (over a period of 30 to 45 minutes) were led to a row of cars parked on the street near the Metro station and thence to the sole occupied car, in which appellant sat with the stolen cell phone in his possession.[6]

I can agree with my colleagues that "under ordinary circumstances," *ante* at 20, the government's use of a cell-site simulator to locate an individual through the individual's cellphone likely violates the legitimate expectation of privacy we all have in our location information.[7] I would also agree that "individuals have a reasonable expectation of privacy in their location information when they are tracked in a space, like the home, that is traditionally protected or when they are tracked for a longer period of time and in greater detail than society would expect." *Historical Cell Site Data*, 724 F.3d at 608 (describing a contention by the ACLU). But I do not believe it is fair to regard the particular circumstances of this case, which I have described above, as "ordinary circumstances." And as the facts of

[6] Actually, at the time appellant was arrested, he had in his car all four stolen cell phones involved in this case.

[7] I acknowledge that some courts have so held. *See, e.g.*, *United States v. Ellis*, No. 13-CR-00818 PJH, 2017 U.S. Dist. LEXIS 136217, *20 (N.D. Cal. Aug. 24, 2017) ("[C]ell phone users have an expectation of privacy in their cell phone location in real time and . . . society is prepared to recognize that expectation as reasonable.").

this case (1) do not involve the privacy of the home;[8] (2) did not entail long-term tracking that could reveal appellant's private information about the places he frequents;[9] (3) did not entail a physical intrusion or a physical trespass to any

[8] That fact distinguishes this case from cell-site simulator cases on which appellant relies. *See State v. Andrews*, 134 A.3d 324 (Md. Ct. Spec. App. 2016), and *United States v. Lambis*, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016). In *Andrews*, police used a cell-site simulator to locate Andrews, who was wanted on charges of attempted murder, and tracked him to a location inside a residence, where he was arrested. 134 A.3d at 326. The court cited its concern that the cell-site simulator had "been used to obtain information about the contents of a home, not otherwise discernable without physical intrusion." *Id.* at 349. The court stated that "people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement" and "an objectively reasonable expectation of privacy in real-time cell phone location information." *Id.* at 327. In *Lambis*, the Drug Enforcement Administration used a cell-site simulator to locate Lambis's apartment, conduct that the court found to be an unreasonable search because "[t]he home has special significance under the Fourth Amendment." 197 F. Supp. 3d at 609–10. These cases are consistent with the principle that, "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." *Kyllo*, 533 U.S. at 31 (observing that "[a]t the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion" (internal quotation marks omitted)).

In this case, the cell-site simulator alerted the officers that appellant's phone was located in the 4000 block of Minnesota Avenue, N.E., a block on which there were several businesses, a District of Columbia government building, and a Metro station. There appears to be no evidence in the record that there were residential buildings in the block, but *amici* note that a large apartment building is also located on the block, at 4020 Minnesota Avenue. There appears to be no evidence in the record that the cell-site simulator came within range of that apartment building as the officers were "coming down southbound Minnesota [Avenue]."

[9] *See Graham*, 824 F.3d at 435 (noting that in *Jones*, "the concurring justices recognized a line between 'short-term monitoring of a person's movements

(continued…)

property of appellant;[10] and (4) did not involve a search of the contents of

(…continued)
on public streets,' which would not infringe a reasonable expectation of privacy, and 'longer term GPS monitoring,' which would" (quoting *Jones*, 565 U.S. at 430)). The concern is that long-term historic location information can reveal "a wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in judgment) ("[T]he use of longer term GPS monitoring [over a period of twenty-eight days in Jones's case] in investigations of most offenses impinges on expectations of privacy."); *cf. United States v. Riley*, 858 F.3d 1012, 1013 (6th Cir. 2017) (tracking of fugitive's real-time GPS location data for approximately seven hours did not amount to a Fourth Amendment search).

[10] A trespassory search implicating the Fourth Amendment occurs when the government "gains evidence by physically intruding on constitutionally protected areas." *Florida v. Jardines*, 569 U.S. 1, 16 (2013).

Appellant and the majority opinion cite cases suggesting that use of a cell-site simulator could constitute trespass to chattels, *ante* at 24–25 n.27, but my colleagues do not rely on that case law for their conclusion. Moreover, as Justice Alito noted in his concurrence in the judgment in *Jones*, "today there must be some actual damage to the chattel before [an] action [for trespass to chattels] can be maintained." 565 U.S. at 419 n.2 (Alito, J., concurring in judgment) (internal quotation marks omitted); *see also* Restatement (Second) of Torts § 218 cmt. (e) (1965) (stating that, generally, "one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time"). If *arguendo* use of the cell-site simulator in this case (which, according to the evidence, may have caused calls that appellant tried to initiate to be dropped) did constitute a trespass, I do not believe we could reasonably conclude that the police were culpable in failing to recognize it as such (and thus I believe we would have no occasion to apply the exclusionary rule). *See Herring v. United States*, 555 U.S. 135, 141, 143 (2009) (confirming that "exclusion has always been our last resort, not our first impulse" and that the Court has "never suggested that the exclusionary rule must apply in every circumstance in which it might provide marginal deterrence," and stating that "[t]he extent to which the exclusionary rule
(continued…)

appellant's cell phone that could have exposed his private information,[11] I am unpersuaded that there was a Fourth Amendment violation in this case.

In the pages that follow, I will explain my reasoning in more detail. But first, I must address a preliminary issue.

I.

After oral argument in this matter, this court directed the parties to submit supplemental briefs on the following issue:

What reasonable and legitimate expectation of privacy

(…continued)
is justified . . . varies with the culpability of the law enforcement conduct.") (internal quotation marks omitted). And, as discussed *infra*, even if police interfered with the operation of appellant's "chattel" when the cell-site simulator "grabbed" his cell phone remotely and rendered it temporarily non-operational for making calls, police were justified in effecting that seizure of appellant's cell phone under the automobile exception to the warrant requirement.

[11] "[C]oncerns about a general 'erosion of privacy' with respect to cell phones . . . revolve around protecting the large quantity of information stored on modern cell phones and on remote servers like the 'cloud.' If all that information were indeed at risk of disclosure [through the government's obtaining cell-site location information], we would share this concern." *Graham*, 824 F.3d at 434 n.13 (internal citation omitted). Documents, however, "stored on phones and remote servers are protected, as 'content,' in the same way that the contents of text messages or documents and effects stored in a rented storage unit or office are protected." *Id.*

> does a person have in his or her location information when the person possesses (outside his or her residence) a stolen cell phone capable of being located by a cell-site simulator or through real-time cell site location information available to the cell phone owner or his or her telecommunications provider?

Asserting that the issue the court raised was waived by the government, appellant argues in his supplemental brief that "waiver rules preclude this court from affirming the trial court's ruling on an alternative ground that the government did not raise at trial or on appeal." I disagree in the strongest terms.[12] Fourth Amendment suppression issues are serious issues. In this case, the evidence sought to be suppressed relates to serial sexual assaults and robberies at knifepoint (with use of a knife that the assailant — confirmed by DNA evidence to be appellant — was still carrying on his person at the time he was stopped by police). We have a duty to analyze for ourselves the antecedent question of whether, on the

[12] Appellant is also incorrect in suggesting that the court directed briefing on an issue entirely absent from the government's initial brief in this court and its arguments in the trial court. The government argued in its opening brief to us that in cases cited by appellant, "the cell-site simulator located the defendant's phone inside a home, thus implicating Fourth Amendment privacy concerns not raised here." Our inquiry about the significance of the fact that appellant possessed the stolen cell phone outside his residence reflected in part that argument. Our inquiry also reflected the prosecutor's repeated argument (to which she mistakenly referred as involving application of the "inevitable discovery" doctrine) to the trial court that suppression was not warranted because there was "a separate, lawful way [police] *could have* gotten to the same thing" (emphasis added) — i.e., use of the cell-site simulator to target the stolen cell phone that was traveling with appellant's phone.

particular facts of this case, use of the technology by which appellant was located constituted a search (and, if so, whether it was a lawful search). In this case as always, this court's task is to "consider[] the briefs and the oral argument, and [to] test[] them against the record and the law," *Watson v. United States*, 536 A.2d 1056, 1068 (D.C. 1987) (en banc), not merely to choose the better or best of the arguments presented in support of a claim. Our responsibility as an appellate court is to decide cases in accordance with the law, and that responsibility is not to be diluted by how counsel have framed the issues or by limitation to the specific authorities counsel have cited.

The Supreme Court's decision in *United States National Bank of Oregon v. Independent Insurance Agents of America, Inc.*, 508 U.S. 439 (1993), is instructive. That litigation commenced after the Comptroller of the Currency issued a ruling allowing the United States National Bank of Oregon "to sell insurance through its branch in Banks, Oregon." *Id.* at 443. Trade organizations challenged the Comptroller's decision, arguing, *inter alia*, that it was inconsistent with section 92, a statutory provision enacted in 1916 that "permit[ted] banks located in small communities to sell insurance to customers outside those communities." *Id.* at 441, 444. The District Court granted summary judgment in favor of the Comptroller, finding that "the Comptroller's interpretation was

rational and consistent with section 92." *Id.* at 444 (internal quotation marks and alterations omitted). On appeal, the trade organizations did not ask the Court of Appeals for the District of Columbia to rule that section 92 no longer existed (it had been repealed in 1918), and they did not take a position on the issue during oral argument or in supplemental briefing. Nevertheless, reasoning that it had "a 'duty' to [decide the issue]," the Court of Appeals determined that section 92 had been repealed. *Id.* at 444-45 (quoting *Indep. Ins. Agents of America, Inc. v. Clarke*, 955 F.2d 731, 734 (D.C. Cir. 1992)).

The case went to the Supreme Court, which concluded that "[t]he Court of Appeals . . . had discretion to consider the validity of section 92," and "did not stray beyond its constitutional or prudential boundaries" in doing so. *Id.* at 447. The Court explained that "[t]hough the parties did not lock horns over the status of section 92, they did clash over whether the Comptroller properly relied on section 92 as authority for his ruling," and the Court of Appeals was not obliged "to treat the unasserted argument that section 92 had been repealed as having been waived." *Id.* at 446-47. The Court confirmed that '"when an issue or claim is properly before the court, the court is not limited to the particular legal theories advanced by the parties, but rather retains the independent power to identify and apply the proper construction of governing law."' *Id*. at 446 (internal alterations omitted)

(quoting *Kamen v. Kemper Fin. Servs, Inc*., 500 U.S. 90, 99 (1991)). The Court further instructed that "a court may consider an issue 'antecedent to and ultimately dispositive of' the dispute before it, even an issue the parties fail to identify and brief." *Id.* at 446-47 (internal alterations omitted) (quoting *Arcadia v. Ohio Power Co.*, 498 U.S. 73, 77 (1990)).

Our court has applied the guidance of *National Bank of Oregon* in various circumstances. For example, in *Martin v. United States*, 952 A.2d 181(D.C. 2008), after requesting supplemental briefs from the parties, we reached the question of whether the police had unlawfully entered Martin's home in violation of the Fourth Amendment, even though "appellate counsel [had] failed to argue that the entry itself constituted an unlawful search either in his principal brief or at oral argument." *Id.* at 188–89.[13] Our sister court, the United States Court of Appeals

[13] *See also Anthony v. United States*, 935 A.2d 275, 282 n.10 (D.C. 2007) ("But no matter whose ox is gored when the parties are directed by the court to file supplemental submissions, 'this court has frequently requested post-argument briefing of issues not adequately raised by counsel, to the end that, after both parties have been fully heard, the court is in the best position to render a sound decision.'" (quoting *Randolph v. United States*, 882 A.2d 210, 226 (D.C. 2005)); *Outlaw v. United States*, 632 A.2d 408, 410–11 (D.C. 1993) (declining to reach the question briefed by the parties — "whether one may be convicted of being an accessory after the fact to murder on the basis of actions taken while the decedent was still alive" — and instead, after requesting and receiving supplemental briefing, ruling based on an issue the panel raised for the first time at oral argument — "whether the evidence was sufficient to support [appellant's] conviction of

(continued…)

for the District of Columbia Circuit, has also considered the merits of issues the parties did not raise. *See United States v. Maynard*, 615 F.3d 544, 560–61 (D.C. Cir. 2010) ("The Government does not separately raise, but we would be remiss if we did not address, the possibility that although the whole of Jones's movements during the month for which the police monitored him was not actually exposed to the public, it was constructively exposed because each of his individual movements during that time was itself in public view.").[14]

(…continued)
[accessory after the fact] to any offense whatever"); *cf. Randolph*, 882 A.2d at 217–18 ("'Once a claim is properly presented to the trial court, a party can make any argument in the appellate court in support of that claim[, and] parties are not limited to the precise arguments made below.'" (internal alterations omitted) (quoting *West v. United States*, 710 A.2d 866, 868 n.3 (D.C. 1998)); *see also id.* at 227 (determining that "the judgment should be affirmed on harmlessness grounds, notwithstanding the government's initial failure to argue that the trial court's error was harmless").

[14] *See also Lesesne v. Doe*, 712 F.3d 584, 588 (D.C. Cir. 2013) (noting that the Supreme Court "has recognized that 'there may always be exceptional cases or particular circumstances which will prompt a reviewing or appellate court, where injustice might otherwise result, to consider questions of law which were neither pressed nor passed upon by the court or administrative agency below,'" and determining that "the proper interpretation of [the Prison Litigation Reform Act's] exhaustion requirement is a dispositive legal issue antecedent to its application" (internal alterations omitted) (quoting *Hormel v. Helvering*, 312 U.S. 552, 557 (1941))); *United States v. Pryce*, 938 F.2d 1343, 1348 (D.C. Cir. 1991) ("Only if one adopts an absolutist approach to the adversary system can one contend that courts must *never* address unargued issues, no matter how obvious their proper resolution may be. Certainly the Supreme Court rejects such an approach.").

In short, case law does not bind us to the approach of addressing only the arguments the parties have framed. The Supreme Court has not followed or dictated that approach,[15] our neighbor the United States Court of Appeals for the District of Columbia Circuit has rejected it, and numerous other federal circuit courts of appeals have said that they have discretion on direct appeal to consider arguments a party has failed to make.[16] The bottom line is that appellate courts "regularly and frequently consider *sua sponte* authorities not cited and grounds of decision not raised."[17]

---

[15] Commentators have frequently mentioned that in *Erie Railroad Co. v. Tompkins*, 304 U.S. 64 (1938), the issue the Court resolved — whether "in diversity cases the substantive law of the state of trial must be applied" — "had not been raised by the parties before either the lower courts or the Supreme Court." Albert Tate, Jr., *Sua Sponte Consideration on Appeal*, 9 TRIAL JUDGES J. 68 (1970), *reprinted in* APPELLATE JUDICIAL OPINIONS 128 (Robert A. Leflar ed., 1974); *see also Singleton v. Wulff*, 428 U.S. 106, 121 (1976) ("The matter of what questions may be taken up and resolved for the first time on appeal is one left primarily to the discretion of the courts of appeals, to be exercised on the facts of individual cases. We announce no general rule.").

[16] *See, e.g.*, *United States v. Rose*, 104 F.3d 1408, 1414 (1st Cir. 1997) ("We join several other circuit courts of appeals in holding that appellate courts have the discretion on direct appeal to overlook the government's failure to argue that the admission of the challenged evidence, if error, was harmless, and that appellate courts may therefore consider the issue of harmlessness *sua sponte*.") (collecting cases).

[17] Albert Tate, Jr., *supra* note 15, at 127; *see also Estate of Girard v. Laird*, 621 A.2d 1265, 1268 n.3 (Vt. 1993) (citing the Tate article in explaining why the court may "reach[] results for reasons different than those argued by the parties"); *State v. Weber*, 471 N.W.2d 187, 199 n.7, 200 (Wis. 1991) (citing the Tate article

(continued…)

When we review denials of motions to suppress, "our role is [essentially] to ensure that the trial court had a substantial basis for concluding that no constitutional violation occurred." *Brown v. United States*, 590 A.2d 1008, 1020 (D.C. 1991). "We must determine whether the court's denial of the motion to suppress is sustainable under any reasonable view of the evidence," and "[i]t is well settled that [we] may affirm a decision for reasons other than those given by the trial court." *Alston v. United States*, 518 A.2d 439, 440 n.2 (D.C. 1986). Thus, in this case, we have a duty to study carefully the particular facts of the case to determine for ourselves whether the trial court's denial of appellant's motion to suppress is sustainable. This means that we have not only the discretion to consider, but an obligation to consider whether appellant had a reasonable and legitimate expectation of privacy in his location information when (as the supplemental briefing order described and among other material facts discussed below) he "possesse[d] (outside his . . . residence) a stolen cell phone capable of being located by a cell-site simulator or through real-time cell-site location information available to the cell phone owner or his . . . telecommunications provider."

(…continued)
in justifying its decision upholding the reasonableness of a search under the Fourth Amendment on grounds that, according to the dissenting justice, the State "was aware of . . . but did not argue . . . in this court").

As explained in the discussion below, "the antecedent question of whether there [wa]s a Fourth Amendment 'search' at all"[18] turns on resolution of that issue (which, on the facts presented here, is ultimately dispositive of the case). And even if *arguendo* use of the cell-site simulator constituted a "search" for Fourth Amendment purposes, application of the automobile exception to the Fourth Amendment warrant requirement requires affirmance of the trial court's denial of the motion to suppress.

II.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. Thus, in analyzing a Fourth Amendment claim, the threshold issue is whether there has been a "search" or "seizure." That "antecedent question whether or not a Fourth Amendment 'search' has occurred is not so simple under [Supreme Court] precedent." *Kyllo*, 533 U.S. at 31. The fundamental principle, however, is that "a Fourth Amendment search does *not* occur . . . unless the individual manifested a subjective expectation of privacy in the object of the challenged search, and society is willing to recognize that

[18] *Riverdale Mills Corp. v. Pimpare*, 392 F.3d 55, 63 (1st Cir. 2004).

expectation as reasonable." *Id.* at 33 (internal quotation marks and alterations omitted). "[W]hether an expectation of privacy is reasonable depends in large part upon whether that expectation relates to information that has been 'exposed to the public.'" *Maynard*, 615 F.3d at 558 (internal alterations omitted) (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). "In considering whether something is 'exposed' to the public as that term was used in *Katz*[,] we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do." *Id.* at 559.

A. Appellant had no reasonable expectation of privacy in his location while he was on the public roads with the powered-on, stolen cell phone.

It appears that police used the cell-site simulator to locate appellant's phone rather than the stolen phone. However, appellant's expectation of privacy with respect to the location of his phone need not come into play in our resolution of this case because appellant exposed that location to discovery by being on the public roads with both his phone and the powered-on, stolen cell phone. Even if appellant generally had a subjective expectation that information about *his* cell phone's location would be private, he could not have had a reasonable expectation that the location of his cell phone would remain private while he was traveling on the public roads with a powered-on, stolen cell phone.

The sexual assaults and robberies in this case occurred in 2013. Well before that time, Apple had introduced the Find My iPhone application ("app"). *See In re J.A.*, No. A-1624-14T2, 2016 N.J. Super. Unpub. LEXIS 430, *11 n.3 (Super. Ct. App. Div. Feb. 29, 2016) (noting that "Apple introduced the Find My iPhone feature in 2011" and that, in that case, the Find My iPhone app "allowed police to track J.A. by following the stolen iPhone's signal to the Shelbourne Lane address within minutes of the robbery"). And indeed in this case, one of the detectives working on the case, Detective Rachel Pulliam, testified that she had "one of the complainant's information in [her] phone as well [as] in the Find My iPhone app" (and thus was able to "get a general idea of where" she would be going to meet the TSU officers who had located appellant through use of the cell-site simulator). It appears that the detective was referring to her ability to use the Find My iPhone app in an effort to locate the Apple iPhone 4S cell phone stolen from the woman the police referred to as complainant number one's cousin (who was robbed but not sexually assaulted at the end of the first of the two incidents involved in this case). As it happened, police in this case tracked the stolen Sprint phone and not that iPhone, but case law is replete with references to iPhone owners or law enforcement officers locating stolen iPhones by using the Find My iPhone app in 2013 or earlier years.[19] The facts caution against assuming that the Find My

[19] *See, e.g.*, *People v. Easton*, No. H041704, 2017 Cal. App. Unpub. LEXIS
(continued…)

iPhone app or similar find-my-device apps *always* pinpoint an address or do so

---

(…continued)
644, *5 (Jan. 30, 2017) ("Using the Find My iPhone application [in 2012], police recovered Casey's cell phone from a recycling bin in front of a residence in Santa Clara within a few blocks of defendant's residence."); *State v. Copes*, No. 84, 2017 Md. LEXIS 478, *5 n.4 (July 28, 2017) (citing a November 2011 publication entitled "*How to Use Find My iPhone to Get Your Stolen iPhone Back*"); *People v. Foy*, 199 Cal. Rptr. 3d 208, 212 (Ct. App. 2016) ("Wang had an application on his iPhone called 'Find My iPhone,' which he used [in 2011] at the suggestion of police to track Song's stolen iPhone. Wang's phone displayed a map indicating that Song's phone was located at 603 Grant Street[.]"); *People v. Robinson*, No. 3268/2013, 2016 N.Y. Misc. LEXIS 652, * 3, (App. Div. Feb. 24, 2016) ("As they were driving [in 2013], the 'Find My iPhone' tracker showed the [stolen] phone to be moving. The movement stopped at East 120th Street and First Avenue in Manhattan."); *People v. Snyder*, No. B265391, 2016 Cal. App. Unpub. LEXIS 8230, *2 (Nov. 16, 2016) ("Using another device's 'find my iPhone' feature [in 2013], Jordyn tracked her iPhone's location to the Mentor Court residence."); *People v. Scales*, No. B260902, 2016 Cal. App. Unpub. LEXIS 1942, *7-8 (Mar. 17, 2016) ("[A] Los Angeles Police Department . . . Officer . . . used a 'Find My iPhone App' [in 2012] to locate Schulz's cell phone that had been taken during the robbery events. It was found on the side of the 10 Freeway about two miles away from the Green Path building."); *Adams v. State*, No. 1142, 2016 Md. App. LEXIS 457, *3 n.3 (Ct. Spec. App. Feb. 5, 2016) ("Because Myers' cell phone was inside his [stolen] vehicle, police [in 2013] were able to locate the car by tracking the phone by use of the 'find my iPhone' application."); *Commonwealth v. Gil*, No. 566-EDA-2014, 2015 Pa. Super. Unpub. LEXIS 3695, *2 (Feb. 10, 2015) ("After the victim reported the robbery [in 2012], the police tracked the iPhone, through a 'Find My iPhone' mobile application, to a house on Washington Street."); *State v. Coleman*, No. W2012-00880-CCA-R3-CD, 2013 Tenn. Crim. App. LEXIS 573, *3 (June 10, 2013) ("Mr. Petty recalled that there was an application on his wife's phone called 'Find My iPhone.' Mr. Petty was able to use his computer to track the phone's location to a general vicinity of Division and Waddell Street."); *Pirozzi v. Apple, Inc.*, 966 F. Supp. 2d 909, 915 (N.D. Cal. 2013) (quoting a statement from Apple's website that "In the event your iPhone is lost or stolen, Find My iPhone allows you to locate it on a map[.]"); *United States v. Flores-Lopez*, 670 F.3d 803, 808 (7th Cir. 2012) (referring to the Find My iPhone app).

accurately,[20] or that the only method officers used in the reported cases to locate the stolen phones was such an app (and not, for example, the app supplemented with use of a cell-site simulator). But the relevant point is that, in 2013, the public had reason to know that, because of "the ubiquity of . . . apps,"[21] it was quite possible for a stolen cell phone to be tracked with precision, even if such efforts were not always successful.

Further, even aside from the apps available to cell phone owners, cellular service providers have long been able to supply cell phone locational data in close to real-time,[22] and, as at least one court observed in 2010, the providers' capabilities were increasing.[23] In 2013, it would have been reasonable to expect

---

[20] Detective Pulliam testified that the Find My iPhone app showed her "[not] an exact, pinpointed location" but, at one point, "a general area . . . in southeast" (perhaps the area of the District into which the phones traveled when, according to other evidence, they left Capitol Heights, Maryland, and headed toward Kenilworth Avenue).

[21] *Commonwealth v. Wilson*, No. 15-P-851, 2016 Mass App. Unpub. LEXIS 466, *3 (Apr. 29, 2016).

[22] The evidence in this case showed that the police TSU received updated location information from the cellular service providers at least every fifteen minutes (every five minutes for the stolen Sprint phone), with only a one-to-three-minute lag time.

[23] The following observations made by that court in 2010 are notable: "Neither the user nor the carrier can predict how precise the next location data will be. For a typical user, over time, some of that [location] data will likely have

(continued…)

that the owner of the stolen cell phone might try to locate it by obtaining cell-site location information from her cellular service provider. Surely "[t]he availability and use of [the foregoing] and other new devices . . . shape the average person's expectations about the privacy of" cell phone movements and location. *Jones*, 565 U.S. at 429 (Alito, J., concurring in judgment).[24] Further, it was reasonable to expect that the owner of the stolen cell phone would seek help from the police and put in motion their efforts, with whatever cell-site location information and devices were at their disposal, to locate the stolen phone. As police TSU Sergeant Perkins testified, with the cell phone simulator, "either one [i.e., the stolen phone or appellant's phone] would have got us to the area [where they found appellant in his

---

(…continued)
locational precision similar to that of GPS"; "Emerging versions of the technology are even more precise"; "[T]he tech-savvy user may now understand that there is a risk that the provider can calculate and record his location and movements very precisely." *In re Application for United States for Historical Cell Site Data*, 747 F. Supp. 2d 827, 833-34, 845 (S.D. Tex. 2010), *rev'd on other grounds*, 724 F.3d 600 (5th Cir. 2013).

[24] Such considerations led the Second Circuit to observe that "any expectation of privacy that [the defendant] had in his cell-phone location [tracked over a less-than-two-hour period] was dubious at best." *United States v. Caraballo*, 831 F.3d 95, 105 (2d Cir. 2016). *See generally United States v. Wheeler*, 169 F. Supp. 3d 896, 908 (E.D. Wis. 2016) (noting that "[t]he media is rife with information — and sometimes warnings — about the fact that one's location can be tracked from one's cell phone").

car].”[25]

By traveling with the stolen cell phone that was susceptible to all the foregoing find-the-phone methods and devices, appellant exposed his location, too. I therefore find it impossible to conclude that appellant could reasonably have expected that his movements and location with the stolen phone in his possession would be private (and thus that he had an “expectation of privacy in his phone’s location”). Moreover, if appellant had such an expectation, I suspect that it is not one that society is prepared — and in my view it is not one that we should be prepared[26] — to recognize as reasonable. To be sure, our cell phones play such a central role in our lives and contain so much of our personal data that we must be vigilant about protecting against government intrusions into cell phone privacy. But the other side of that coin is that — I strongly suspect — a great many people who have had a cell phone stolen or who fear such a theft are likely to have a

[25] Appellant suggests that the evidence indicated that the cell-site simulator did not work with the stolen cell phone, but the trial court declined to so find. The court found instead that if the TSU officers “had . . . switched over . . . to use the Sprint number instead, . . . they would have eventually gotten to the exact same place because the phones were together.”

[26] I have in mind the caution that where we may have been “‘conditioned’ by influences alien to the well-recognized Fourth Amendment freedoms, a normative inquiry may be necessary to align” what we are prepared to recognize as legitimate privacy interests “with the protections guaranteed in the Fourth Amendment.” *Tracey v. State*, 152 So. 3d 504, 525–26 (Fla. 2014).

strong desire to recover their stolen phones and to be unwilling to recognize as legitimate the locational-privacy interest of a person who is traveling the streets with a stolen phone.[27] I am not the first to observe that "many people may find the tradeoff [between electronic tracking technology and some diminution of privacy] as worthwhile." *Jones*, 565 U.S. at 427 (Alito, J., concurring in judgment).

To be clear, the analysis above does not rely on the inevitable-discovery

[27] My conclusion that appellant was traveling with a stolen phone as to which he had no locational-privacy interest does not depend on the jury verdict that he was the thief, i.e., the perpetrator of the robberies. *Cf. Godfrey v. United States*, 414 A.2d 214, 214 (D.C. 1980) ("The real question is whether the [proponent of a motion to suppress] can be deemed to have a legitimate expectation of privacy in the thing or area searched and the item seized without reference to" an "unfortunate pretrial connotation that the proponent of the motion to suppress is guilty.") Rather it rests on the evidence presented at the suppression hearing that, when arrested, appellant had with him in his car all four stolen phones as well as the phone used by the perpetrator of the robberies and sexual assaults. (Unlike the defendant in *McFerguson v. United States*, 770 A.2d 66 (D.C. 2001) — a case Judge Farrell suggests is apposite, *ante* at 53 n.2 — appellant was not "a street pedestrian [with] a reasonable expectation of privacy in covered objects associated with his person," *id.* at 71). I believe we can say with confidence that even if appellant had disputed at the suppression hearing that he knew that the victims' (four) phones found in his possession had been stolen and had attempted to show that he had a legitimate possessory interest in and expectation of privacy with respect to the stolen Sprint phone, he would not have been able to carry his burden of so demonstrating. *See Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978) ("The proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure."); *Morton v. United States*, 734 A.2d 178, 182 (D.C. 1999) (referring to defendant's "burden of showing that he had a protectible interest").

doctrine to conclude that use of the cell-site simulator was lawful. As the majority opinion notes, the inevitable-discovery doctrine "shields illegally obtained evidence from the exclusionary rule if the government can show, by a preponderance of the evidence, that the evidence 'ultimately or inevitably *would* have been discovered by lawful means.'" *Gore v. United States*, 145 A.3d 540, 548 (D.C. 2016) (quoting *Hicks v. United States*, 730 A.2d 657, 659 (D.C. 1999)). The inevitable-discovery doctrine thus requires proof that a presumably lawful search process was actually underway; here, at least arguably, that would have entailed at a minimum having entered the pertinent number of the stolen cell phone (which police had obtained) into the cell-site simulator. There was some evidence that the TSU officers did that, but, in the trial court's view, not enough such evidence to enable the government to prove by a preponderance of the evidence that the officers used the cell-site simulator to find the stolen phone rather than appellant's phone. However, for purposes of my analysis focused on what appellant could reasonably have expected others to do, I have properly relied on what the police *could have done* with respect to the stolen cell phone (or, it appears, with respect to the cousin's stolen iPhone) that would have enabled them to locate appellant and his phone.

United States v. Gbemisola, 225 F.3d 753 (D.C. Cir. 2000), illustrates the

point. There, law enforcement agents had installed and subsequently monitored an electronic tracking device in a package addressed to the defendant, which enabled the agents to know if and when the defendant opened the package — which he did while riding in the back of a taxicab. *Id.* at 756. Noting that the agents did not see when the box was opened, the D.C. Circuit concluded that no warrant was required for their use of the electronic device that reported when the box was opened because the "decisive issue . . . [was] not what the officers saw but *what they could have seen*." *Id.* at 759 (emphasis added). "At any time, the surveillance vehicle could have pulled alongside of the taxi and the officers could have watched Gbemisola through its window. Indeed, the taxi driver himself could have seen the event simply by looking in his rear-view mirror or turning around." *Id.*; *see also Maynard*, 615 F.3d at 560 ("[I]t was not at all unlikely Gbemisola would be observed opening a package while seated in the rear of a taxi[.]"). Thus, the fact that the agents learned what they learned through an electronic device (one presumably not generally available to members of the public) was not the important factor; the important factor was that they, or someone else, could have learned that the defendant opened the package through lawful means.[28]

[28] It might be suggested that the analysis in *Gbemisola* is a straightforward application of the Supreme Court's ruling in *United States v. Knotts*, 460 U.S. 276 (continued…)

The same point applies here. Again, police TSU Sergeant Perkins's testimony (and the trial court's finding) was that, with the cell-cite simulator, "either [phone] would have got[ten them] to [where they found appellant in his car]." In other words, officers could have found appellant's location through use of the cell-site simulator targeted at the stolen cell phone that was in his vehicle (the lawfulness of which approach appellant does not challenge, and likely has no

---

(…continued)
(1983), about the lawfulness of use of a monitoring device that reveals no more than could be seen by visual surveillance. *See id.* at 282–84 (holding that the officers' conduct in monitoring signals from a beeper they had installed in a container the defendant subsequently placed in his car did not invade any legitimate expectation of privacy and did not constitute a Fourth Amendment search since the beeper surveillance revealed no more than could have been visible to the naked eye as the car traveled the public highway and raised no constitutional issues that visual surveillance would not also raise); *see also United States v. Karo*, 468 U.S. 705, 714 (1984) ("[T]he monitoring of a beeper *in a private residence*, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.") (emphasis added). However, the Supreme Court's decision in *Bond v. United States*, 529 U.S. 334 (2000), makes clear that what an individual exposes to the public is not limited to what can be learned through visual perception (outside a residence), but also includes what members of the public may be able to discern through predictable tactile actions. *See id.* at 338 ("When a bus passenger places a bag in an overhead bin, he expects that other passengers or bus employees may move it for one reason or another. Thus, a bus passenger clearly expects that his bag may be handled" and "exposed to certain kinds of touching and handling."). I see no reason why the analysis of whether something is exposed to the public based on "what a reasonable person expects another might actually do," *Maynard*, 615 F.3d at 559, should not include as well the find-my-stolen-phone efforts likely to be set in motion by an individual whose cell phone has been stolen.

standing to challenge).[29] The fact that (we presume) police officers actually found appellant's location by using the cell-site simulator on appellant's cell phone should not change the Fourth Amendment calculus.

B. The (assumed) fact that the police actually used the cell-site simulator as to appellant's cell phone while it was on the public roads does not provide a basis for finding a Fourth Amendment violation.

My colleagues focus, however, on the apparent fact that the police entered the identifying number for appellant's cell phone into the cell-site simulator and thus used it to locate appellant's phone rather than the co-located stolen phone. They emphasize that "when it comes to the Fourth Amendment, means . . . matter." *Ante*, at 18 (quoting *Maynard*, 615 F.3d at 566). But, as the D.C. Circuit explained in *Maynard*, what matters with respect to the means employed is whether "one's reasonable expectation of control over one's personal information would . . . be defeated" through that means of information gathering. 615 F.3d at 566. For the reasons already discussed, on the facts of this case, appellant had no reasonable expectation of control over the information about his location while he was on the

[29] *See Lucas v. United States*, 411 A.2d 360, 363 (D.C. 1980) ("[I]t is not so clear that persons can always assume that the right to privacy extends to articles of contraband in their possession."); *United States v. White*, 504 F. App'x 168, 172 (3d Cir. 2012) (citing authority from several federal circuits that one who knowingly possesses a stolen item has no legitimate expectation of privacy with respect to it and no standing to challenge a search of it).

public roads with the powered-on, stolen cell phone in his possession.

Moreover, while the "means . . . matter" principle applies *a fortiori* when it comes to law enforcement efforts to learn about what is contained or is transpiring in a home,[30] the principle applies with much less consistency when what is challenged as a "search" took place on public roads. *See Knotts*, 460 U.S. at 282 (explaining that the defendants had no legitimate expectation of privacy that was violated by use of a beeper, pre-installed inside a container of chemicals that the defendant purchased and put in his car, which sent signals to a police receiver and enabled police to track the movements of the car, because police could have tracked the car's movements by driving behind it); *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (concluding that because the defendant, located with use of a cell-site simulator, was at the time "in a public place, where he had no legitimate expectation of privacy, [he could]not complain about how the police

[30] *See, e.g.*, *Kyllo*, 533 U.S. at 35 n.2 (analyzing whether use of a thermal-imaging device, capable of detecting the amount of heat emanating from a home, constituted an unlawful search when, without a warrant, it was aimed at the home of an individual suspected of growing marijuana in his home using high-intensity lamps; reasoning that the "comparison of the thermal imaging to various circumstances in which outside observers might be able to perceive, without technology, the heat of the home — for example, by observing snowmelt on the roof — is quite irrelevant. The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment" (internal citation omitted)).

learned his location."); *see also Gbemisola*, 225 F.3d at 759.

My colleagues ultimately acknowledge that "certain forms of tracking [in public spaces] . . . do not invade a reasonable expectation of privacy." *Ante* at 18. What they seem to regard as dispositive is that by using the cell-site simulator, the police "actively induce[d] the phone to divulge its identifying information." *Ante* at 17. Judge Farrell sees as the critical fact that with the cell-site simulator, the police TSU officers "commandeer[ed]" appellant's cell phone, turning it into a "self-investigative" tool. I have several responses.

First, for a couple of reasons, I believe the foregoing characterizations somewhat overstate the facts. As one court has noted, "cell phones identify themselves by an automatic process called 'registration,' which occurs continuously while the cell phone is turned on regardless of whether a call is being placed." *Tracey*, 152 So. 3d at 507 n.1.[31] That observation accords with the

[31] *See also Copes*, 2017 Md. LEXIS 478, at *6 ("A cell site simulator . . . takes advantage of the fact that a cell phone — when turned on — constantly seeks out nearby cell towers, even if the user is not making a call . . . When the cell site simulator is close enough, the target phone will connect to it as though it were a cell tower."); *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1014 (N.D. Cal. 2015) ("[C]ell phones, when turned on and not in airplane mode, are always scanning their network's cellular environment. In so doing, cell phones periodically identify themselves to the closest cell tower — i.e., the one with the strongest radio signal (continued…)

testimony by defense telecommunications technology expert Ben Levitan in this case. *See* Levitan Aff. 5 ("When a phone attaches itself to a cell tower, it identifies itself by phone number and various codes."). In other words, identifying themselves constantly is what powered-on cell phones do, regardless of whether a cell-site simulator is in the area. Second, while the majority opinion accurately quotes TSU Sergeant Perkins's testimony that the cell-site simulator "grabs [the target cell phone] and holds on to it for a minute," the opinion does not recount Sergeant Perkins's additional explanation. Sergeant Perkins explained that "by grabs it," he meant that the cell site simulator "just knows it's there," much as one knows when he has arrived at a station he is looking for by scanning the radio dial. Mr. Levitan put it differently, explaining that cell phones "generally connect themselves to the strongest cell tower signal that they detect," and, in that vein, when a cell phone detects the cell-site simulator as having the strongest signal, it will "break its connection with the cell phone network and reattach itself to the newly found . . . simulator." The Department of Justice document entitled "Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3,

---

(…continued)
— as they move throughout their network's coverage area. This process[is] known as 'registration' or 'pinging[.]' . . . Pinging is automatic and occurs whenever the phone is on, without the user's input or control." (record citations omitted)).

2015), http://www.justice.gov/opa/file/767321/download (the "DOJ Policy Guidance"), states similarly that "cellular devices in the proximity of the [cell-site simulator] 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." *Id.* at 2. Thus — if it matters — it appears that it is cell phones that initiate contact with a cell-site simulator and not the other way around.[32]

In any event, my colleagues raise points that must be addressed when they emphasize that by using the cell-site simulator, the TSU officers took "functional control" of and "coopted [appellant's] phone, forcing it to do something [he] surely never intended it to do: reveal its identifying and location information to an entity

---

[32] *But see Andrews*, 134 A.3d at 340 (citing testimony in that case that a cell-site simulator known as the Hailstorm "is an active device that can send an electronic signal . . . and 'draw[] the phone to [the] equipment"' (alteration in original)).

My colleagues also say that the cell-site simulator "exploits a security vulnerability" of cell phones. *Ante* at 17. I would not call what happened here as exploitation of a cell phone security flaw, but as law enforcement's taking advantage of a security-enhancement feature that aids in the recovery of stolen or lost phones. It may place a person who is traveling on the roads with a powered-on, stolen cell phone (that circumstances show he knew to be stolen) in the position either of accepting the risk that at any moment the stolen cell phone or his own cell phone could be converted into a tracking device or, alternatively, turning the phones off, but I do not see why that is an improper choice to foist on the person.

other than a telecommunications provider." *Ante*, at 24 n.27. Judge Farrell finds it "unpersuasive" "to argue that appellant had no reasonable expectation of privacy in the police' use of his phone" for this purpose. *Ante*, at 47. One major problem for my colleagues' analysis, however, is that, as shocking or outrageous as the foregoing characterizations might sound, the officer's use of the cell-site simulator did not constitute a "search" and thus was not a Fourth Amendment violation unless appellant had a reasonable and legitimate expectation of privacy with respect to the object of the challenged search: his location information. For the reasons already discussed, he did not while he was on the public roads with a trackable, stolen cell phone.

It is helpful to recall the facts of *California v. Greenwood*, 486 U.S. 35 (1988). In *Greenwood*, a police detective asked the regular trash collector in Greenwood's neighborhood to pick up the plastic garbage bags that Greenwood had left on the curb in front of his house and to turn the bags over to the detective without mixing their contents with garbage from other houses. *Id.* at 37. The trash collector responded by cleaning his truck bin of other garbage, collecting the garbage bags from the street in front of Greenwood's house, and turning the bags over to the detective. *Id*. The detective searched through the trash and found items indicative of narcotics use. *Id.* at 37–38. The *Greenwood* respondents asserted

"that they had, and exhibited, an expectation of privacy with respect to the trash that was searched by the police," emphasizing that the trash had been placed on the street for collection at a fixed time and was contained in opaque bags, which the garbage collector was expected to pick up, mingle with the garbage of others, and deposit at the garbage dump. *Id.* at 39. The respondents also highlighted that "there was little likelihood that [the trash] would be inspected by anyone." *Id.* The Supreme Court acknowledged that "[i]t may well be that respondents did not expect that the contents of their garbage bags would become known to the police or other members of the public," *id.* at 39, but reasoned nevertheless that the police conduct did not constitute a Fourth Amendment violation (because respondents "could have had no reasonable expectation of privacy in the inculpatory items that they discarded"). *Id.* at 41.

In my view, the intrusive police conduct in *Greenwood*, by which police officers converted the entire contents of respondent's trash into a database of information about his activities, was every bit as objectionable as the temporary "coopt[ing]" of appellant's cell phone. I suspect most of us would be outraged at the effrontery of law enforcement officials in systematically inspecting our trash. But that would not be enough to establish that police officers' systematic

rummaging through our trash is a "search" for Fourth Amendment purposes.[33] And any sense of outrage here is likewise not enough to establish that use of the cell-site simulator in the particular circumstances of this case violated appellant's Fourth Amendment rights.[34]

But even if we assume that the TSU officers' taking "functional control" of and "coopt[ing] [appellant's] phone" was a search and/or seizure for Fourth Amendment purposes, there is yet another consideration that, in my view, should preclude the court from concluding that the search/seizure was unlawful.[35] The

---

[33] *Cf. Historical Cell Site Data*, 724 F.3d at 615 ("We understand that cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, . . . to remain so. But the recourse for these desires is in the market or the political process . . . . The Fourth Amendment, safeguarded by the courts, protects only reasonable *expectations* of privacy." (internal citation omitted)).

[34] Another lesson from *Greenwood* is the principle on which *Gbemisola*, was decided: that if the individual does not have a reasonable expectation of privacy in the object of an activity that we would describe in ordinary parlance as a search, there is no search for Fourth Amendment purposes even if the manner in which law enforcement conducted their garbage inspection was not available to most members of the public. The Supreme Court observed in *Greenwood* that the respondents' trash was readily accessible to "animals, children, scavengers, snoops, and other members of the public." 486 U.S. at 40. But it is likely that few people other than the police would have been granted the accommodation of having the trash collector segregate all of the respondents' garbage from other garbage.

[35] "A 'seizure' of property occurs when 'there is some meaningful interference with an individual's possessory interests in that property.'" *Karo*, 468

(continued…)

police TSU officers could reasonably infer that the stolen cell phone and appellant's phone were traveling together in a car or other vehicle because the real-time location information showed them as having gone from Capitol Heights, Maryland, to Kenilworth Avenue, before moving to the 4000 block of Minnesota Avenue, N.E. The automobile exception to the Fourth Amendment warrant requirement "permits the warrantless search of a car [or other vehicle] that is 'readily mobile' so long as 'probable cause exists to believe it contains contraband.'" *United States v. Eshetu*, 863 F.3d 946, 951 (D.C. Cir. 2017) (quoting *Pennsylvania v. Labron*, 518 U.S. 938, 940 (1996) (per curiam)); *United States v. Shackleford*, 830 F.3d 751, 753 n.2 (8th Cir. 2016) ("The automobile exception requires probable cause to believe contraband or evidence of *any* crime will be found in the vehicle[.]").[36] And, "[i]f probable cause justifies the search of

---

(…continued)
U.S. at 712 (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). There was at least arguably a seizure here, because, according to the testimony, use of the cell-site simulator may have caused calls appellant tried to make from his phone to drop. (I note that to the extent that the presence of the cell-site simulator in the area caused dropped calls or other disruption of the cell phones of other people in the area, appellant has no standing to complain.)

[36] *See also California v. Carney*, 471 U.S. 386, 393 n.2 (1985) ("With few exceptions, the courts have not hesitated to apply the vehicle exception to vehicles other than automobiles."); *id.* at 392-93 (explaining that if a vehicle "is readily capable of such use [on the highways] and is found stationary in a place not regularly used for residential purposes," the "justifications for the vehicle
(continued…)

a lawfully stopped vehicle, it justifies the search of every part of the vehicle and its contents that may conceal the object of the search." *United States v. Ross*, 456 U.S. 798, 825 (1982); *Eshetu*, 863 F.3d at 952.

"Probable cause exists when based on the known facts and circumstances, a reasonably prudent person would believe that contraband or evidence of a crime will be found in the place to be searched." *United States v. Charles*, 801 F.3d 855, 860 (7th Cir. 2015) (internal quotation marks omitted). Here, even before using the cell-site simulator, the police TSU officers had near real-time cell-site location information that gave them probable cause to believe that a vehicle was on the public roads with both the stolen cell phone and the cell phone used by the sexual assault/robbery perpetrator, and thus probable cause to believe that—whatever the subject vehicle's precise location on the roads[37]—it contained contraband and

(…continued)
exception come into play," because "the vehicle is obviously readily mobile by the turn of an ignition key, if not actually moving"); *id.* at 392 ("[I]ndividuals always have been on notice that movable vessels may be stopped and searched on facts giving rise to probable cause that the vehicle contains contraband, without the protection afforded by a magistrate's prior evaluation of those facts." (internal quotation marks and alterations omitted)). And, there is exigency about searching a vehicle where there is probable cause to believe it contains contraband: "[T]he overriding societal interests in effective law enforcement justify an immediate search before the vehicle and its occupants become unavailable." *Id.* at 393.

[37] *Cf. State v. Tate*, 849 N.W.2d 798, 810 (Wis. 2014) (reasoning that even if a warrant had been required to authorize use of a cell-site simulator, the exact (continued…)

evidence of a crime. This means that — under the automobile exception — the vehicle was searchable without a warrant, and that any cell phones in it that might have been contraband or evidence of the crime could be seized.[38] We should therefore hold that when the cell-site simulator simultaneously detected/caught the signal from appellant's cell phone (which was located in a car parked on the street) and "seized" the phone by "hold[ing] on to it for a minute," there was no Fourth Amendment violation. Any locational information obtained from the cell phone was not content that could be searched only pursuant to a warrant.[39]

(…continued)
place to be searched, such as a street address, was not required).

[38] Our request for supplemental briefing signaled, without explicitly suggesting, that the automobile exception might be implicated on the facts of this case (and amici briefly addressed its applicability in their initial brief).

[39] *See Graham*, 824 F.3d at 434 (rejecting the argument that cell-site location information should be treated as "content" for Fourth Amendment purposes).

Again, this case does not involve a warrantless search of any digital content (such as text messages, emails, contact lists, call logs, voicemail messages, photographs, videos, files, internet browsing history, apps that are revelatory of a person's interests, historic location information, etc.) stored on appellant's cell phone, the conduct for which, the Supreme Court determined in *Riley v. California*, 134 S. Ct. 2473, 2485 (2014), a warrant was needed. *See id.* at 2480-81 (involving a search of the cell phone that was found in Riley's pocket after he was stopped for driving with expired tags and subsequently arrested for possession of concealed and loaded firearms); *see also* DOJ Policy Guidance at 2 ("[T]he [cell-site] simulator does not remotely capture emails, texts, contact list, images or any other data from the phone."). The seizure, "interfer[ence] with the functioning" of, or "coopt[ing]" of appellant's phone involved here, including the
(continued…)

***

I end by repeating and underscoring that my dissent rests on the particular facts of this case: Police had near real-time information, from cell phone providers, that the cell phone the robbery/sexual assault assailant had used to lure his victims was traveling on the public streets together with a trackable, powered-on cell phone stolen from one of the assailant's victims (who gave the police permission to obtain her phone records); they could infer that the phones were traveling together in a car or other vehicle; and law enforcement officers' use of a cell-site simulator in the vicinity led them to a "handful of cars" parked at the Minnesota Avenue Metro station and to a car in which appellant sat with the stolen cell phone in his possession. To hold that the officers' use of the cell-site simulator in this case was lawful would come nowhere close to holding, as my colleagues conclude, that police may use cell-site simulators "at will" to locate any individual who is carrying a cell phone, without regard to whether the individual is known to be in a vehicle moving through the public streets and without regard to

---

(…continued)
effect of having his calls dropped, is akin to the interruptions or intrusions that the *Riley* Court found permissible when police officers execute a search incident to arrest that turns up a cell phone: they are "free to examine the physical aspects of [the] phone," may "turn the phone off or remove its battery," or may "leave a phone powered on and place it in an enclosure that isolates the phone from radio waves." 134 S. Ct. at 2485, 2487.

whether the individual is known to have with him in the vehicle both a trackable cell phone stolen during a set of robberies and the cell phone from which an assailant placed calls to lure his sexual assault/robbery victims. Quite the contrary, the holding I believe is the right one would, because of its nuanced analysis, sound a cautionary note about using a cell-site simulator in other circumstances without a warrant.[40]

What we should not do in resolving this appeal is to jump on the bandwagon of decrying what is claimed to be a Fourth Amendment violation from use of cell-site-simulator technology without recognizing how the particular, material facts of this case distinguish it from the cell-site simulator cases courts have decided before this one. The Supreme Court has recognized the need for "consideration of case-

[40] In addition, even if I assume *arguendo* that there was a Fourth Amendment violation, I am doubtful that suppression in this case would "pay its way," *United States v. Leon*, 468 U.S. 897, 907 n.6 (1984), under the "cost-benefit analysis in exclusion cases," *Davis v. United States*, 564 U.S. 229, 238 (2011), particularly in light of the Department of Justice's announced general policy that the government now must seek warrants for cell-site simulator use. DOJ Policy Guidance at 3-4. "[T]he [exclusionary] rule's operation [is limited] to situations in which th[e] purpose [of deterrence] is thought most efficaciously served"; accordingly, "[w]here suppression fails to yield appreciable deterrence, exclusion is clearly unwarranted." *Davis*, 564 U.S. at 237 (internal alterations and quotation marks omitted).

specific exceptions to the warrant requirement";[41] we are remiss if we do not carefully consider the distinguishing facts of this case; and the public deserves no less from us, even as we do what we must to protect precious Fourth Amendment rights.

For all the foregoing reasons, I respectfully dissent from the judgment reversing appellant's convictions of two counts of first-degree sexual abuse while armed, two counts of kidnapping while armed, four counts of robbery while armed, and one count of threats.

[41] *Riley*, 134 S. Ct. at 2486.