Filing # 104053917 E-Filed 02/28/2020 12:14:45 AM

IN THE CIRCUIT COURT OF THE 17th JUDICIAL CIRCUIT
IN AND FOR BROWARD COUNTY, FLORIDA

STATE OF FLORIDA, **CASE NUMBER: 15-1926CF10A**
JUDGE: DUFFY

v.

JONATHAN GORDON,
Defendant.
_____/

GORDON'S REPLY TO STATE'S MEMORANDUM OF LAW REGARDING ELECTRONIC SURVEILLANCE AND CELL SITE INFORMATION

NOW COMES Defendant Gordon, through his undersigned counsel, and states:

1. Defendant Gordon moves this Court to suppress the arrest of Gordon, any items seized in his residence, and the seizure of his car and any items seized from his car, and the DNA sample taken from Gordon, and any items gathered as fruits of the unconstitutional use a cell-site simulator, also known as a "Stingray," a device that impersonates a wireless carrier's cell tower to force wireless devices within range to communicate with it.

2. Because the warrantless use of a Stingray to obtain location information is unconstitutional under the Fourth Amendment, the location information, and all the fruits thereof, must be suppressed.

3. A Stingray functions by forcing phones to repeatedly transmit their unique identifying electronic serial numbers. Using those transmissions, the

technology can quickly and accurately locate one or more target phones. It is both a precise and broad tool—a Stingray can capture location information that pinpoints a cell phone user in a specific room of an apartment, and it can collect the location information of hundreds or thousands of individuals at a time.

4. Using a Stingray without a warrant violates the Fourth Amendment. A warrantless Stingray search is impermissible under the Fourth Amendment because it tracked and located the defendant in a constitutionally protected space. This surveillance technique permitted the police to do the otherwise impossible - locate the defendant out of thin air - with no judicial oversight that could have ensured that the Stingray was used in a particular location, over a minimal time-frame, and to prohibit the collection of communication content and the retention of third-party records.

5. By not seeking a warrant, the government knowingly prohibited the court from exercising its constitutional oversight function and cannot have acted under good faith. The Fourth Amendment therefore requires suppression of the search-produced evidence.

Background

6. This case involves the surreptitious use of a international Mobile Subscriber Identity-catcher ("IMSI-catcher"), Stingray (or other similar cell-site simulator), one of a class of cell phone surveillance devices commonly known as

"Stingrays."[1] These privacy-invasive devices have been employed by law enforcement agencies for years with little to no oversight from legislative bodies or the courts due to an intentional policy of secrecy. See Brad Heath, Police Secretly Track Cellphones to Solve Routine Crimes, USA Today, Aug. 24, 2015, http://usat.ly/1LtSLdI. Cell-site simulators can be carried by hand, installed in vehicles, or mounted on aircraft. See Devlin Barrett, Americans' Cellphones Targeted by Secret U.S. Spy Program, Wall St. J., Nov. 13, 2014, https://perma.cc/F4TW-GKB8 ("The Justice Department is scooping up data from thousands of mobile phones through devices deployed on airplanes that mimic cell towers").

7. The devices masquerade as cellular tower antennas used by companies such as AT&T and Sprint, and in doing so, force mobile phones within the range of the device that subscribe to the impersonated wireless carrier to emit identifying signals, which can locate not only a particular suspect, but bystanders.

[1] "Stingray" is the name for one cell-site simulator model sold by the Harris Corporation. Other models include the "TriggerFish," "KingFish," and "Hailstorm." *See* Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, Ars Technica, Sept. 25, 2013, http://bit.ly/1mkumNf. Stingrays, Hailstorms, and other models of cell-site simulators are also called "IMSI catchers," in reference to the unique identifier—or international mobile subscriber identity—of wireless devices that they track. Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1, 11 (2014). Newer devices, such as Hailstorm or Boeing's DRTBox are "capable of accessing phone content and data." Nicky Woolf, *Stingray Documents Offer Rare Insight into Police and FBI Surveillance*, Guardian (Aug. 26, 2016), https://perma.cc/676R-GHPU.

8. A Stingray is an invasive investigative tool. Depending on the particular features of the Stingray and how the operator configures them, Stingrays can locate "cell phones to within six feet," including in a user's home or apartment, see Adam Bates, Stingray: A New Frontier in Police Surveillance, Cato Institute, at 5, Jan. 25, 2017; capture the content of voice and text messages made to or from the cell phone, see Kim Zetter, Turns Out Police Stingray Spy Tools Can Indeed Record Calls, Wired, Oct. 28, 2015, https://perma.cc/663E-2KH7; and even block or drop calls made on devices near the Stingray, see Kim Zetter, Feds Admit Stingrays Can Disrupt Cell Service of Bystanders, Wired, Mar. 1, 2015, https://perma.cc/K7CX-8UBD.

9. Stingrays are commonly used by law enforcement agencies in two ways: to discover a previously unknown target, or to track a known target. In the first method, law enforcement uses the Stingray to collect the unique electronic serial numbers associated with all phones in a given area, and from that information, attempts to deduce the target's number.

10. In the second method, law enforcement can program the Stingray with, for example, the phone number of the target, and then employ the Stingray to locate and track that device. Jennifer Valentino-DeVries, How 'Stingray' Devices Work, Wall St. J. (Sept. 21, 2011), http://on.wsj.com/1D2IWcw.

11. In both instances, however, the device will prompt all wireless devices within range that use the impersonated wireless carrier to communicate with it, providing law enforcement with the unique identifying information and relative location of these cell phones. See Staff Comm. on Oversight and Government Reform, 114th Cong., Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendation, Dec. 19, 2016, at 12, https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf ["Staff Committee Report"] ("While searching for the target phone, the simulator will also make contact with other, non-target cell phones that happen to be within range of the simulator device, even if those phones' owners are innocent bystanders who are not suspected of any criminal wrongdoing"); Cyrus Farivar, How Florida Cops Went Door to Door With Fake Cell Device to Find One Man, Ars Technica, June 4, 2014, https://perma.cc/HJT6-TL2D ("Such searches are controversial in part because stingrays necessarily capture data about all other compatible phones nearby. . . . [T]he gear evaluates all the handsets in the area as it searches for its target") (internal citations omitted).

12. Stingrays can gather the electronic serial numbers of "up to 10,000 phones at a time." See Jason Murdock, Is the U.S. Government Spying on You? Why 'Stingray Tech Is So Controversial, Newsweek, Apr. 4, 2018, https://perma.cc/88SG-6NZD (internal citation omitted).

13. Here, the Broward County Sheriff's Office ("BSO") and U.S. Marshall's Fugitive Task Force transmitted signals through the walls of homes in a Ft. Lauderdale, FL, neighborhood to force Gordon's mobile phone to transmit its unique serial number, and reveal its location. BSO and the U.S. Marshalls did so without knowing Gordon's particular location at his home at 128 SW 22nd Ave., Ft. Lauderdale, FL, and the officers did so without a warrant.

14. The home is at the "very core" of the interests the Fourth Amendment protects, and enjoys the maximum protection it provides. See Florida v. Jardines, 133 S.Ct. 1409, 1414 (2013).

ARGUMENT

I. Use of a Stingray Is a "Search" Under the Fourth Amendment

The Supreme Court recently held in *Carpenter v. United States* that individuals have a reasonable expectation of privacy in their cell phone location data, and that the government's acquisition of those records from the defendant's cellular service provider was a Fourth Amendment search. 138 S.Ct. 2206, 2217 (2018). This holding must apply with equal force when the government gathers location data through the use of its own device, a Stingray. However, even prior to *Carpenter*, almost every court to address the question has held using a Stingray is a Fourth

Amendment search.[2] Whether this Court analyzes this claim under the reasonable expectation of privacy framework in *Katz v. United States*, or a property-based theory of the Fourth Amendment, it will reach the same conclusion - using a Stingray to gather cell-phone location information is a "search" under the Fourth Amendment.

A. Users Have a Reasonable Expectation of Privacy in Their Cell Phone Location Data

In considering whether individuals reasonably expect information to remain private, the Supreme Court has crafted "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also Carpenter*, 138 S.Ct. at 2213, 2217 (applying the *Katz* analysis in cell-site location information

---

[2] *See, e.g.*, *United States v. Lambis*, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016) ("The use of a cell-site simulator constitutes a Fourth Amendment search within the contemplation of Kyllo"); *Prince Jones v. United States*, 168 A.3d 703, 707 (D.D.C. Sept. 21, 2017) ("[T]he government violated the Fourth Amendment when it deployed the cell-site simulator against him without first obtaining a warrant based on probable cause"); *United States v. Ellis*, 270 F. Supp. 3d 1134, 1146 (N.D. Cal. Aug. 24, 2017) ("[T]he court holds that Ellis had a reasonable expectation of privacy in his real-time cell phone location, and that use of the Stingray devices to locate his cell phone amounted to a search requiring a warrant, absent an exception to the warrant requirement."); *State v. Andrews*, 227 Fd. App. 350, 355 (2016) ("We conclude that people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement and . . . that people have an objectively reasonable expectation in real-time cell-phone location information"); *Cf. United States v. Patrick*, 842 F.3d 540, 544 (7th Cir. 2016), *cert. denied*, 138 S. Ct. 2706 (2018) ("The United States has conceded for the purpose of this litigation that use of a cell-site simulator is a search"); *State v. Tate*, 849 N.W.2d 798, 807 (WI 2014) ("[B]ecause the parties do not dispute that a search occurred, we assume, without deciding that tracking a cell phone using cell-site information and a stingray constitutes a search that has constitutional implications"); *United States v. Temple*, 2017 WL 7798109, at * 30 (E.D. Mo. Oct. 6 2017) ("[F]or purposes of deciding Temple's motion to suppress physical evidence seized on April 24, 2015, the undersigned will assume that the use of a Cell Site Simulator was a Fourth Amendment search"); *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 999 (D. Ariz. Jan. 5, 2012) ("The government has conceded . . . that use of the mobile tracking device constituted a search for purposes of the Fourth Amendment").

and concluding that users have a reasonable expectation of privacy in this information). For reasons discussed below, Gordon has evinced both a subjective and objective expectation of privacy in his personal cell phone, and using a Stingray device to track location information is a Fourth Amendment search.

U.S. Supreme Court precedent shows that using a Stingray device is a Fourth Amendment search. First, *United States v. Karo* and *Kyllo v. United States* unequivocally hold that law enforcement must get a warrant prior to using surveillance technology to learn information about the interior of constitutionally protected spaces. 468 U.S. 706, 719 (1984); 533 U.S. 27, 40 (2001). If a Stingray is deployed while the target is carrying her phone around her home, the Stingray will provide law enforcement with the precise location of the targeted individual within her "dwelling place," *United States v. Knotts*, 460 U.S. 276, 282 (1983), an impermissible search without a warrant.

Second, recent precedent in *United States v. Carpenter* compounds the conclusion that a warrant is required for a Stingray search. In *Carpenter*, the Court held the government's acquisition of the cell-site records was a search because of "the deeply revealing nature of cell-site location information ("CSLI"), its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." 138 S.Ct. at 2223. These factors give rise to a reasonable expectation of

privacy, and are equally relevant when the government collects real-time location information using a Stingray device.

Besides these concerns, using a Stingray raises two unique issues that further strengthen the conclusion that using this device is a search.

First, use of a Stingray grants the government a significant new power. Prior to the cell phone age, to track a suspect the government first had to know that person's precise location to follow them or install a tracking device on their person or effects. *See, e.g.*, *Knotts*, 460 U.S. at 277 (government agents installed a beeper in a can of chloroform that the defendant then purchased to track the defendant's car); *United States v. Jones*, 565 U.S. 400, 402 (2012) (government agents "installed a GPS tracking device on the undercarriage of the [defendant's] Jeep").

With a Stingray device, this investigative step is removed—a Stingray permits law enforcement to locate an individual whose precise location was previously unknown. *Prince Jones*, 168 A.3d at 712. This unprecedented ability to locate someone raises unique constitutional concerns to be protected by informed judicial oversight. *Carpenter*, 138 S.Ct. at 2221.

Second, the third-party doctrine is wholly inapplicable to using a Stingray device because the government gathers the cell-site location information itself, rather than through a third-party such as a cell phone carrier. Users do not voluntarily

share this information with the government; a Stingray *forces* its connection to nearby devices, exploiting the way cell phones function. *Id.* at 2220.

a. *Kyllo* and *Karo* Requires Law Enforcement to Get a Warrant if It Uses Surveillance Technology to Search the Inside of a Home

Stingrays gather information about constitutionally protected spaces, including the home—which is "presumptively unreasonable in the absence of a search warrant." *Katz*, 389 U.S. at 361. No matter how the Stingray is employed, it cannot prevent devices near it from communicating with it if those devices use the wireless carrier the Stingray is impersonating. *See* Cyrus Farivar, *How Florida Cop Went Door to Door With Fake Cell Device to Find One Man*, Ars Technica, June 4, 2014, https://perma.cc/HJT6-TL2D ("Such searches are controversial in part because stingrays necessarily capture data about all other compatible phones nearby. . . . [T]he gear evaluates *all* the handsets in the area as it searches for its target") (internal citations omitted). Every device that connects to the Stingray will reveal its unique identifying information and relative location.

As the Stingray communicates with nearby users, it gathers cell phone location information which can precisely pinpoint suspects' locations, including in specific apartments or areas within large apartment complexes. *See, e.g.*, *State v. Tate*, 849 N.W.2d 798, 804 (Wis. 2014) (tracking phone to southeast corner of apartment building); *United States v. Rigmaiden*, No. CR 08-814-PHX_DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) (locating cellular aircard "precisely

within Defendant's apartment"); Tr. Of Official Proceedings at 56–58, *State v. Andrews*, Nos. 114149007-009 (Balt. City. Cir. Ct., Md., June 4, 2015), *available at* bit.ly/1S125bl (locating phone in single apartment in 30-35 unit apartment building); Tr. Of Suppression Hr'g at 15–18, *State v. Thomas*, No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010), *available at* bit.ly/1jYYUgUT (identifying "the particular area of the apartment that the handset [signal] was emanating from").

This differs from merely observing an automobile pull into an individual's driveway, *see Knotts*, 460 U.S. at 282, because cell-site location information can place an individual "within a dwelling place." *Id.*

Even if the government does not use this information in a criminal investigation, or collects a small amount of information only from a user, the Court has emphasized that due to the "sanctity" of the home, "*all* details are intimate details." *Kyllo*, 533 U.S. at 37 (2001); *see also id.* at 40 ("We have said that the Fourth Amendment draws 'a firm line at the entrance to the house'") (citing *Payton v. New York*, 445 U.S. 573, 590 (1980)); *Knotts*, 460 U.S. at 282 (noting that the respondent "undoubtedly had the traditional expectation of privacy within a dwelling place insofar as the cabin was concerned"); *United States v. Karo*, 468 U.S. 705, 715 (1984) ("We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable

suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time").

When law enforcement uses a Stingray, it not only risks piercing the wall of *one* individual's home, but *hundreds or thousands* of homes, with no one ever learning their privacy was invaded. The sheer volume of users that might be captured by a Stingray search creates a high probability the device will ping a cell phone inside a home as it drives past.

This is far too expansive an invasion of the "sanctity of the home" or any other constitutionally protected area. *Kyllo*, 533 U.S. at 37; *see also United States v. Lambis*, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016) (citing *Kyllo*, 533 U.S. at 35–36) ("The DEA's use of the cell-site simulator revealed 'details of the home that would previously have been unknowable without physical intrusion,' namely, that the target cell phone was located within Lambis' apartment").

b. Searches That Are Deeply Revealing, Comprehensive, and Inescapable Violate Users' Reasonable Expectation of Privacy

The Court in *Carpenter* held the government's acquisition of the cell-site records was a search because of "the deeply revealing nature of CSLI" 138 S.Ct. at 2223. As the Court explained, "its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." 138 S.Ct. at 2223. These factors are equally relevant when the government collects real-time location information

using a Stingray device, and should similarly demand Fourth Amendment protection.

i. A Stingray Collects Information that is "Deeply Revealing" Because It Intrudes on Constitutionally Protected Spaces and Can Gather a Comprehensive Array of Information, Including Voice and Data Communications

The information a Stingray reveals to law enforcement about cell phone users is "deeply revealing" for two important reasons. 138 S.Ct. at 2223. *First*, besides revealing information about the home, Stingrays reveal *private* facts about other protected activities and intimate spaces. A Stingray will locate the cellular device wherever the user carries it. Because "individuals . . . compulsively carry cell phones with them all the time," the Stingray will reveal the location of the device and "its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter* 138 S.Ct. at 2218. An amicus brief in *Carpenter* noted the concern that requests for cell-site location information near an 8:30 pm Alcoholics Anonymous meeting "will reveal all the devices—and therefore individuals—in that meeting. . . . The same conclusions hold for other sensitive and protected associational activities—including religious evangelism, student activism, and union organizing." *Brief of Technology Experts as Amici Curiae in Support of Petitioner, Carpenter v. United States*, 2017 WL 3530967, at *35–36 (Aug. 14, 2017).

Another brief worried that "[d]ue to the ubiquitous nature of cell phones, location information gleaned from cell towers can disclose an individual's expressive and associational activities such as "a journalist's newsgathering process." *Brief of the Reporters Committee for Freedom of the Press and 19 Media Organizations as Amici Curiae in Support of Petitioner, Carpenter v. United States*, 2017 WL 3530966, at *14 (Aug. 14, 2017).

These briefs expressed the fears that cell-site location information ("CSLI") can reveal information not only about intimate and constitutionally protected spaces, but also infringe on First Amendment activities.

These same fear holds true to using a Stingray device—which will gather unique identifying information of all users that use the impersonated wireless carrier whether they are at church or in a political meeting. The need for a warrant is critical to ensure that a Stingray device causes only a minimal invasion of privacy, as "[a]wareness that the Government may be watching chills associational and expressive freedoms." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

Second, Stingrays not only have the capacity to gather real-time location information about an individual, they also "have the capability of intercepting the *content of communications*" including phone calls and text messages. *Ellis*, 270 F. Supp. 3d at 1147 (emphasis added). This matters even if law enforcement does not actually use the device in this fashion.

In *Riley v. California*, the issue was not whether law enforcement actually looked through the comprehensive information stored on the cellular device, but that they *could*. 134 S.Ct. at 2481 (noting that officers only "pressed one button on the phone to access its call log, then another button to determine the phone number associated with the 'my house' label").

The *Riley* Court noted "a cell phone's capacity allows even just one type of information to convey far more than previously possible." *Id.* at 2489. E-mails can contain an individual's "entire business and personal life," *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). Because of the "privacy interests at stake," the Court held that law enforcement would need a warrant to search a cell phone incident to arrest. *Id.* at 2495; *see also Warshak*, 613 F.3d at 286 (holding that before law enforcement could view the "contents of a subscriber's emails, those agents have . . . conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.").

The same rationale should apply when the government uses a Stingray to track a user's location: that the device can gather content such as text messages should require prior judicial oversight in a warrant.[3]

[3] The government may argue that the Department of Justice provides that "cell-site simulators . . . may not be used to collect the contents of any communication." Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology [hereinafter "DOJ Guidance"] (Sept. 3, 2015). However, "the DOJ policy memorandum does not describe any sort of enforcement mechanism that would ensure compliance with the policy, and . . . the present administration or a subsequent one may well revise this policy." *Jones*, 168 A.3d at 721. As a result, there is still a "need to deter future constitutional violations." *Id.*

ii. A Stingray Search is Far More Comprehensive and Broad Than Traditional Tracking Because it is a Dragnet Search

The State's use of a Stingray amounts to a "dragnet-type law enforcement practice" that the Court feared in *Knotts*, 460 U.S. at 284, sweeping up the location data of any mobile device in its path hoping to find one potential lead. The Court has always been "careful to distinguish between rudimentary tracking . . . and more sweeping modes of surveillance," *Carpenter*, 138 S.Ct. at 2215 (citing *Knotts*, 460 U.S. at 284), in deciding whether a search is entitled to heightened protection under the Fourth Amendment. Using a Stingray falls on the "sweeping" end of this spectrum, and is therefore entitled to heightened protection under the Fourth Amendment.

Regardless of how law enforcement uses the Stingray device—with or without a known phone number—the device will collect the information of many of the cellular devices it passes. Stingrays emulate a wireless carrier's base station, prompting many wireless devices within range to communicate with the impersonated wireless carrier. Cell phones automatically communicate with the strongest base station "by dint of its operation." *Carpenter*, 138 S.Ct. at 2220.

If that strongest base station is the Stingray, cell phones that use the impersonated wireless carrier will automatically connect to it because "phones have no way to differentiate between a legitimate base station . . . and a rogue device impersonating a carrier's base station." Staff Committee Report, at 10 (internal

citations omitted). This is an unconstitutional dragnet search, as the government could never amass probable cause, let alone reasonable suspicion, to acquire the location information of these third-parties. *See Ybarra v. Illinois*, 444 U.S. 85, 86 (1979) (noting that "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."); *Knotts*, 460 U.S. at 284 (stating that a dragnet search would be held unconstitutional).

The number of bystanders swept up in this search without probable cause could have numbered in the hundreds or thousands. The Stingray device used at bar likely has an extensive range. BSO and the U.S. Marshalls operated the cell-site simulator in such a manner any functioning cell phone on the impersonated network within range of the Stingray device. As it roamed the streets, cell phones would have been forced to broadcast identifying data to the BSO and the U.S. Marshalls.

This would include passengers of cars on Broward Blvd. and Interstate 95, two of Broward County's most heavily-traveled thoroughfares.. And there were many customers and employees of a shopping plaza on Broward Blvd. that includes a Super Walmart, Wawa and Racetrac gas stations, and many businesses and restaurants.

Also, there were residents of private homes and apartment buildings in this densely populated area near Gordon's home at 128 SW 22nd Ave. , Ft. Lauderdale.

Other adjacent areas include Stranahan High School, an Amtrak station, a Tri-Rail Park and Ride area, Broward County bus stops, and several churches.

While police are tracking (or trying to locate) a particular signal, the Stingray can sweep up and search through the location of *everyone* in its path who uses the impersonated wireless carrier. This is the digital version of the "writs of assistance" that permitted "British officers to rummage through homes in an unrestrained search for evidence of criminal activity;" searches that "helped spark the Revolution itself." *Riley*, 134 S.Ct. at 2494; *see also Carpenter*, 138 S.Ct. at 2213 (citing *Riley*, 134 S.Ct. at 2494).

The U.S. Supreme Court has repeatedly prohibited this "exploratory rummaging" as the provenance of general warrants forbidden by the Fourth Amendment. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *Wilkes v. Wood*, 98 Eng. Rep. 489, 498 (1763); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814).

The difference here is that even the "reviled general warrants and writs of assistance of the colonial era," *Riley*, 134 S.Ct. at 2494 (internal quotations omitted), were subject to the practical constraints posed by "limited police resources and community hostility." *Illinois v. Lidster*, 540 U.S. 419, 426 (2014).

This is not so with a Stingray search. Individuals will not be alerted when law enforcement officials have obtained their cell-site location data, and few will even know that their local police use these devices. *See generally* Dell Cameron & Patrick

Howell O'Neill, *Police Documents Reveal How Law Enforcement Keep Stingray Use Secret*, DailyDot, Oct. 7, 2016, https://perma.cc/W65B-M2H5 ("The FBI has gone to extraordinary lengths to keep local, state, and federal law enforcement quiet about the surveillance device—even if it means dropping a criminal case.").

That the government may "discard that information before alerting officials to the presence of the sought-after person" *Patrick*, 842 F.3d at 542, does not change the dragnet nature of this search. Instead, it highlights the important need for meaningful judicial oversight involving the disclosure of the government's exact plan for the time and location it plans to use the device, and how it plans to minimize the collection and retention of non-targeted individual's CSLI. *See In the Matter of the Application of the United States of America for an Order Relating to Telephones Used by Suppressed*, 2015 WL 6871289, at *3 (N.D. Ill. Nov. 9, 2015) [*Order Relating to Telephones Used by Suppressed*] ("[A] process must be created to reasonably ensure that innocent third parties' information collected by the use of a cell-site simulator is not retained by the United States or any government body.").

This is critical, as the government has at its availability "the most advanced twenty-first century tools, allowing it to 'store such records and efficiently mine them for information years into the future,'" creating a risk of repeated surveillance. *Klayman v. Obama*, 957 F. Supp. 2d 1, 33 (D.D.C. 2013) (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *see also Order Relating to Telephones Used by*

Suppressed, 2015 WL 6871289, at *3 ("The concern over collection of innocent third parties' information [through the use of a Stingray] is not theoretical. It has been reported that the government collects telephone numbers, maintains those numbers in a database and then is very reluctant to disclose this information").

iii. Stingray Surveillance is "Inescapable and Automatic"

The invasive nature of the Stingray device is made even more dangerous because the surveillance is "inescapable and automatic." 138 S.Ct. at 2223. When a Stingray is near a target, the Stingray operates by "grab[bing] the target phone . . . [and] prevent[ing] [it] from communicating with an actual tower." *Prince Jones*, 168 A.3d at 709 (internal citations omitted).

Unless the user "disconnect[s] the phone from the network, there is no way to avoid leaving behind a trail of location data." *Id.* Simply being near the Stingray will automatically turn the user's phone into a "tracking device." *United States v. Lambis*, 197 F. Supp. 3d 606, 611 (S.D.N.Y. July 12, 2016).

This form of tracking is inescapable, even as the individual goes out of the public sphere and into the private realm, such as inside her home. As the Court remarked in *Carpenter*, earlier forms of tracking—whether through "the bugged container in *Knotts* or the car in *Jones*"—could provide the police only with knowledge otherwise publicly observable. *See Carpenter*, 138 S.Ct. at 2218

(citing *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (plurality opinion) ("A car has little capacity of escaping public scrutiny")).

If law enforcement is tracking a person in a car, the GPS surveillance will be compromised by the fact that "individuals regularly leave their vehicles." *Carpenter*, 138 S.Ct. at 2218. With the Stingray device, law enforcement is no longer hampered in this way because people "compulsively carry cell phones with them all the time," *id.*, "with 12% admitting that they even use their phones in the shower." *Riley v. California*, 134 S.Ct. at 2490.

The Court has repeatedly understood and remarked that it is a fact of life that cell phone users will carry their phones around with them at all times. *Carpenter*, 138 S.Ct. at 2218 (citing *Riley*, 134 S.Ct. at 2484) (noting that the cell phone is "almost a 'feature of human anatomy'").

This fact gives rise to "an even stronger privacy interest in real time location information associated with [users'] cell phones, which act as a close proxy to one's actual physical location because most cell phone users keep their phones on their person or within reach, as the Supreme Court recognized in *Riley*." *United States v. Ellis*, 270 F. Supp. 3d 1134, 1145 (N.D. Cal. 2017); *see also Carpenter*, 138 S.Ct. at 2218 ("When the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user").

c. A Stingray Has the Capacity to Locate Someone in Time and Space Prior to Tracking Them

Stingrays are an investigative tool that gives the government the power to not only "track" an individual, but to also "locate" them. Although technology has enhanced law enforcement's ability to determine the whereabouts of an individual—so law enforcement no longer has to "visually track a suspect from some starting location"—no previous technology has permitted the government to locate a person whose whereabouts were not precisely known. *Prince Jones*, 168 A.3d at 712.

When law enforcement seeks to use new technology, courts have the important duty to "take the long view, from the original meaning of the Fourth Amendment forward." *Kyllo*, 533 U.S. at 40. A Stingray is the "tool" that "risks Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent." *Carpenter*, 138 S.Ct. at 2223 (citing *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

The Court has approved of location tracking when it "enable[s] police officers to accomplish the same task that they could have accomplished through 'visual surveillance from public places.'" *Prince Jones*, 168 A.3d at 712 (citing *Knotts*, 460 U.S. at 282). In traditional tracking, police need to either know the exact whereabouts of the individual to follow them "from some starting location," *Jones*, 168 A.3d at 712, or they must first install a tracking device "on some object that the target will later acquire of use." *Id*.

In *United States v. Knotts*, the government first needed to install a beeper in a can of chloroform the defendant purchased and placed in his car to track his location. 460 U.S. at 277. In *United States v. Jones*, the Court first needed to "install[] a GPS tracking device on the undercarriage of the [defendant's] Jeep" to conduct surveillance. 565 U.S. at 403.

No longer. With a Stingray device, the government avoids these traditional investigative steps—"no longer need[ing] to track a person visually from some starting location or [to] physically install a tracking device on an object that is in, or will come into, his or her possession—by "remotely activat[ing] the latent tracking function of a device that the person is almost certainly carrying in his or her pocket or purse: a cell phone." *Id.* at insert. This permits the government "to discover that person's precise location remotely and at will." *Id.*

When the government uses new technology with new capabilities courts should be able to exercise their constitutional oversight function through, at minimum, the requirement of a warrant. *Cf. Kyllo*, 533 U.S. at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—*at least where (as here) the technology in question is not in general public use*.") (internal citations omitted) (emphasis added); *Carpenter*, 138 S.Ct. at 2223 (citing *Olmstead v. United States*,

277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)) ([T]he Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections").

d. The Third Party Doctrine Does Not Apply Because the Government Has Obtained the Data Directly and Users Do Not Voluntarily Share This Information

Even before the Supreme Court clarified the third-party doctrine to digital-age searches in *Carpenter*, the third party doctrine could not apply to using a Stingray device because the government obtains the information *directly* from the tracked individual(s), as opposed to through a third party. Unlike dialed phone numbers transiting the phone company's network, *see Smith v. Maryland*, 442 U.S. 735 (1979), the location information was obtained by law enforcement directly from the Defendant's phone itself.

When the police seek information by directly interacting with a suspect's phone, no third party is involved, "[t]hus[] it cannot be said that [the Defendant] assumed the risk that the information obtained through the use of the [Stingray] device would be shared." *State v. Andrews*, 227 Fd. App. at 398.

Individuals also do not voluntarily share their location information with the Stingray device, further supporting that third-party doctrine is inapposite in this context. The third-party doctrine is justified by the assumption that an individual

cannot reasonably expect "information he voluntarily turns over to third parties" to remain private. *Smith*, 442 U.S. at 44. In *Carpenter*, the Court emphasized that cell phone users' "sharing" of their location data with their service provider is not done voluntarily: "Cell phone location information is not truly 'shared' as one normally understands the term. First, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." 138 S.Ct. at 2220 (quoting *Riley*, 134 S.Ct. at 2484).

Moreover, "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Carpenter*, 138 S.Ct. at 2220.

The use of a Stingray device has "'an additional layer of involuntariness' that renders the third party doctrine inapplicable," *Ellis*, 720 F. Supp. 3d at 1145 (quoting *Lambis*, 179 F. Supp. 3d at 615)—it "*forc[es]* [the cell phone] to repeatedly transmit their unique identifying electronic serial numbers," as opposed to a traditional cell site, which only gathers CSLI "transmitted in the normal course of the phone's operation." *Ellis*, 270 F. Supp. 3d at 1145 (quoting *State v. Andrews*, 227 Fd. App. at 393).

The only way an individual could avoid "sharing" their cell phone location data would be to "disconnect the phone from the network" altogether, rendering it useless as a communication device. *Carpenter*, 138 S. Ct. at 2220.

It cannot be that by choosing to "participat[e] in modern society" by carrying a cell phone turned on, an individual relinquishes any expectation of privacy in their location information. *Id.*

B. Both the Cell Phone Itself and Its Location Information Is Property That is Protected by the Fourth Amendment's Prohibition Against Unreasonable Searches and Seizures

Using a Stingray seizes two "papers" or "effects"—data on the phone, and the cellular device itself—the search of which is unconstitutional without a warrant. Under a property-based theory of the Fourth Amendment, defendant's location data constitutes his or her "papers or effects," and therefore cannot be searched or seized without a warrant. *Carpenter*, 138 S.Ct. at 2272 (Gorsuch, J., dissenting).

In his dissent in *Carpenter*, Justice Gorsuch explained that under a "traditional approach" to the Fourth Amendment, the protection against unreasonable searches and seizures applied if "a house, paper, or effect was yours under law." *Id.* at 2267–68 (Gorsuch, J., dissenting); *see also Florida v. Jardines*, 569 U.S. 1, 5 (2013) (citing *United States v. Jones*, 565 U.S. 400, 406 n.3 (2012)) ("The Amendment establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections: When 'the Government obtains information by physically intruding' on

persons, houses, papers, or effects, 'a search' within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'"). A person's data *should* "qualify as *his* papers or effects under existing law." *Id.* at 2272 (Gorsuch, J., dissenting). In looking to what qualifies as a paper or effect, it is helpful to look to "[s]tate (or sometimes federal) law [that] creates rights in both tangible and intangible things." *Id.* at 2270.

Congress *has* granted cell phone "customers certain rights to control use of and access to" their wireless or electronic communications. *Id.* at 2272. For example, statutes explicitly protect an individual's "wire or electronic communication," such as the Stored Communications Act (SCA), 18. U.S.C. § 2701(a)(2) (prohibiting the "access to a wire or electronic communication" in excess of authorization), or the Wiretap Act, 18 U.S.C. § 2511(1)(a) (holding liable "any person who—intentionally intercepts . . . any wire, oral, or electronic communication"); see also The Federal Telecommunications Act, which requires "express prior authorization" of the customer before a service provider can "use or disclose . . . call location information," which the law categorizes as "customer proprietary information." 47 U.S.C. § 222(f).

Florida law is in accord. *See* §316.305(3)(a), Fla. Stat. (2019) Wireless communications devices; prohibition, and §316.306, Fla. Stat. (2019) School and work zones; prohibition on the use of a wireless communications device in a

handheld manner; §§740.002, 740.04, 740.05 (Fla. Stat. 2019) Fiduciary Access To Digital Assets. This interest should not be diminished when it is the State, as opposed to a third-party carrier, who is accessing the wire or electronic communications, for Congress has espoused the general aim that "customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use." *Carpenter*, 138 S.Ct. at 2272 (Gorsuch, J., dissenting).

Use of a Stingray is also an unreasonable search and seizure of the cellular device itself—clearly an "effect" under the Fourth Amendment. *See Tracey v. Florida*, 152 So.3d 504, 524 (Fla. 2014) ("[W]e conclude that cell phones are 'effects' as that term is used in the Fourth Amendment").

Although the government does not literally *seize* the device, it remotely alters the function of it, "virtually" seizing it. As a direct function of a Stingray's normal use, it "grabs" the device, *Jones*, 168 A.3d at 707, and "begins reporting general location and signal strength that can be used to locate the target phone's exact location." *Id.* In doing so, the government effectively "turn[s] a citizen's cell phone into a tracking device." *Lambis*, 197 F. Supp. 3d at 611.

As a side effect of their normal use, Stingrays disrupt the ability of cell phones in the area to make and receive calls. Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology ["DOJ Guidance"] 5 (Sept. 3, 2015) ("[T]he target

cellular device (*e.g.*, cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider.").

Recently, Senator Ron Wyden "confirmed that the use of a cell-site simulators for conducting real-time surveillance on cell phones may interfere with 911 calls." Zack Whittaker, *Stingray Cell Phone Surveillance Devices May Interfere with 911 Calls, Senator Says*, TechCrunch (Aug. 28, 2018), https://perma.cc/2EJ5-F6LN. Although Stingray devices designed by Harris Corporation are supposed to prevent this from occurring, "officials at Harris . . . told [Sen. Ron Wyden] that a feature designed to prevent interference with 911 calls was neither tested nor confirmed to work." *Id.*

Even if this feature works, urgent calls to doctors, psychologists, workplaces, and family members may be blocked while the cell-site simulator is in use nearby. Both the direct and tangential effects of using a Stingray involves changing the function of the individual's cellular device, constituting a sort of "taking" of the device.

II. Use of a Stingray Requires a Warrant Based on Probable Cause Which Meets the Fourth Amendment's Particularity and Minimization Requirements

When a search violates a user's reasonable expectation of privacy, it requires, at minimum, a warrant based on probable cause. *Carpenter*, 138 S.Ct. at 2222 (holding that "a warrant is required . . . where the suspect has a legitimate privacy

interest in the records"); *Riley*, 134 S.Ct. at 2493 (citing *Coolidge v. New Hampshire*, 403 U.S. at 481) ("Our cases have historically recognized that the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow 'weighed' against the claims of policy efficiency'"). The government's failure to get a warrant requires suppression of the fruits of the unconstitutional search.

A. The Good Faith Exception Should Not Apply if the State Did Not Get a Warrant Prior to using a Stingray

The State knew that a Stingray raises unique privacy concerns that at minimum require a warrant. By failing to seek judicial authorization to use the device, the State prevented the court from exercising its constitutional oversight function, and the good-faith exception should not apply.

The State knew only a warrant could protect against the unreasonable invasion of privacy that occurs when it uses a Stingray device. The Department of Justice and Homeland Security have issued guidance that absent exigent or exceptional circumstances, a warrant is required when agencies seek to use a cell-site simulator. DOJ Guidance at 3; U.S. Dep't of Homeland Sec., Policy Directive 047-02, at 6 (Oct. 19, 2015), http://1.usa.gov/1mqvY88; *see also* DOJ Guidance at 5 (requiring that "applications for use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.").

And every court to address the question of Stingray searches has held a warrant is required. *See supra* note 2.

BSO was therefore on sufficient notice a warrant was required, yet it still failed to obtain one. This conclusion is bolstered by the Supreme Court's recent holdings in *Riley* and *Carpenter*.

Both cases espoused the general principle that precise electronic location tracking requires a warrant because it intrudes on reasonable expectations of privacy. *Carpenter*, 138 S.Ct. at 2217 ("Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI"); *Riley*, 134 S. Ct. at 2490 (noting Fourth Amendment implications of cell phone location data that can "reconstruct someone's specific movements down to the minute, not only about town but also within a particular building"); *see also United States v. Jones*, 565 U.S. at 964 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

In hoping these cases were not applicable to using a Stingray device, the State sought to thread the thin needle between the narrow difference of real-time and historical-location tracking. Instead, these cases should have alerted the State to the privacy interests at stake when it employs modern technology that permits it to track

an individual extensively, precisely, and within the confines of constitutionally-protected spaces.

When the State has sought to do this, courts have repeatedly responded with the same conclusion: "get a warrant." *Carpenter*, 138 S.Ct. at 2221; *Riley*, 134 S.Ct. at 2495.

B. Suppression Is the Appropriate Remedy When Officers Act in Bad Faith

BSO declined to apprise the Broward Circuit Court in its applications for Gordon search warrants it intended to use a Stingray, and how it works. So the State prevented the Court from exercising its constitutional function of ensuring searches are not overly intrusive, the rights of non-suspects are protected, and all aspects of the search are supported by probable cause and described with particularity. *See Johnson v. United States*, 333 U.S. 10, 14 (1948) ("Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of policy officers.").

Had the issuing Broward judge had access to full and accurate information regarding the use of a Stingray when deciding Gordon search warrants, he likely would have withheld or modified the orders, as other fully informed judges have done. *See United States v. Williams*, No. 13 Cr. 548, Mag. No. 12-3092 (D.N.J. July

13, 2012), ECF No. 63-8 (modifying the government's proposed order to prohibit the FBI from using the cell-site simulator "in any private place or where [FBI agents] have reason to believe the target [phone] is in a private place.").

Or the Broward judge may have denied the application for the Gordon search warrants altogether because use of a Stingray is too intrusive, for example, because of the impact on third parties. *See In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197, 201 (C.D. Cal. 1995) (denying statutory application to use a Stingray because "depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted").

To avoid this outcome, BSO omitted critical information from the issuing Broward judge. This should result in the suppression of the results of the searches (i.e. contents of Gordon's home, car, cell phone, DNA, and his arrest).

The State's omission of its use of the Stingray to the issuing Broward judge when applying for the 4 Gordon search warrants, violates *Franks v. Delaware*. 438 U.S. 154, 155-56 (1978). In *Franks,* the Supreme Court held a defendant can challenge the truthfulness (or omissions) of factual statements made in an Affidavit supporting a warrant.

Where a defendant makes a substantial preliminary showing an affiant knowingly and intentionally made a material omission, and the omission may have affected a finding of probable cause, a hearing is required per *Franks*. See *Johnson v. State,* 660 So. 2d 648, 655 (Fla. 1995) (holding any discussion of omissions of material facts in Affidavits must begin with *Franks*).

At bar, BSO and the U.S. Marshalls used the Stingray to locate Gordon before they applied for the 4 Gordon search warrants. When a search warrant application contains information derived from a prior illegal search (i.e. unauthorized use of Stingray), the *Franks* inquiry includes whether the officer would have sought a warrant had he not known the prior illegal search. *Untied States v. Albury,* 782 F. 3d 1285 (11th Cir. 2015). BSO illegally used Stingray to locate Gordon, his phone, car, and his home. BSO *then* applied for the 4 search warrants for those items. This violates *Albury, supra.*

In *United States v. Leon,* 468 U.S. 897 (1984), the Court set forth its "good faith" exception to the exclusionary rule. Specifically, it held the exclusionary rule does not bar the use of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a neutral magistrate but ultimately found to be unsupported by probable cause.

However, one of the four situations outlined in *Leon* where the "good faith" exception does *not* apply is where the magistrate was misled by the information in an affidavit the officer knew or should have known was false except for the officer's reckless disregard of the truth (i.e. a *Franks v. Delaware* violation).

In such a case, the affidavit does not support issuing the warrant. *United States v. Martin*, 297 F.3d 1308 (11th Cir. 2002). So by not detailing their prior illegal use of Stingray, the BSO officers misled the Broward judge by that omission.

Did BSO and the U.S. Marshalls *purposely* not divulge their use of Stingray as a matter of agency policy, or a non-disclosure agreement with the Stingray manufacturer? This is a common practice to keep the technology secret from the courts and the public.

In *Thomas v. State*, 127 So.3d 658, 659-60 (Fla. 1st DCA 2013) a young woman reported that she had been raped and her purse, containing a cellular telephone, had been stolen. About 24 hours later, police tracked her cell phone to the apartment defendant Thomas shared with his girlfriend. For the next few hours, six or seven police officers milled around outside the apartment, but did not try to obtain a search warrant.

The *Thomas* police did not want to obtain a search warrant, because they did not want to reveal information about the technology they used to track the cell phone signal. "[T]he Tallahassee Police Department is not the owner of the equipment."

The prosecutor told the court that a law enforcement officer "would tell you that there is a nondisclosure agreement that they've agreed with the company." *Id.*

An investigator in *Thomas* with the technical operations unit of the Tallahassee Police Department testified: "[W]e prefer that alternate legal methods be used, so that we do not have to rely upon the equipment to establish probable cause, just for not wanting to reveal the nature and methods." He also testified: "We have not obtained a search warrant [in any case], based solely on the equipment." *Id.*

The State at bar should be queried by this Court whether (1) there was an agency policy by either BSO or the U.S. Marshalls not to divulge to courts their use of CSLI technology, (2) there was a non-disclosure agreement between BSO or the U.S. Marshalls and the manufacturer of the CSLI not to divulge the technology, and its ownership and use, and (3) the 4 Gordon search warrants were obtained *after* the Stingray per *Thomas, supra*. The answers would go a long way in determining whether BSO and the U.S. Marshals acted in good faith.

In *United States v. McGough,* 412 F.3d 1232 (11th Cir. 2005), the court held the good faith exception to the exclusionary rule does not apply where a search warrant is obtained based on information observed by the police during an unlawful warrantless search. BSO's use of Stingray to locate Gordon was an unlawful warrantless search. So the evidence resulting from the subsequent 4 Gordon search

warrants (using facts based on the Stingray search) should be suppressed per *McGough.*

Florida cases show warrantless use of Stingray devices requires Gordon's evidence to be suppressed

Recent Florida case law follows the *Carpenter* rationale that use of a Stingray device is a "search" under the 4th Amendment, which must be closely scrutinized by the courts. In *State v. Martin,* Case no. 4D18-3417 (Fla. 4th DCA, Nov. 27, 2019) in 2012, the State charged the defendant with first-degree murder after his mother was found dead in their shared apartment. BSO Detectives tracked the defendant using cell-site location information and a cell-site simulator.

Martin was found sitting in the victim's parked car along with several pieces of evidence. He moved to suppress the evidence obtained by the cell-site simulator, arguing its use violated his Fourth Amendment rights. The trial court granted the motion to suppress, and the State appealed. The *Martin* court affirmed the suppression order. This Court should similarly suppress Gordon's evidence.

In *State v. Sylvestre,* 254 So. 3d 986, 990 (Fla. 4th DCA 2018), the State applied for a search warrant based on information obtained from historical CSLI and a cell-site simulator. After Sylvestre moved to suppress evidence found during the search, the circuit court found probable cause existed to support the CSLI order. But the court suppressed evidence discovered through the State's warrantless use of the cell-site simulator.

The State appealed the court's order suppressing the search, and Sylvestre cross-appealed the court's finding that the CSLI order was supported by probable cause. The *Sylvestre* court affirmed the suppression of the evidence derived from the warrantless search by the cell site simulator. This Court should do the same.

Gordon was not a "fugitive", so there were no exigent circumstances to locate him

Because Gordon was arrested at his home residence in Ft. Lauderdale, in Broward County near where the homicide occurred, he was not a "fugitive from justice" as the State alleges. He was the non-shooter in an incident where he only went to the deceased's house to pick up possessions of a 3rd party. Gordon was not even aware the victim had died, until shortly before his arrest nearly 3 days after the incident. So he was *not* "fleeing". Gordon wasn't even sure charges had been filed against him.

In *State ex rel. Myers v. Allen*, 83 Fla. 655, 662–63 (1922), the court posited a fugitive from justice is one who, having committed a crime within a state, either conceals himself within the state or departs therefrom so he cannot be reached by ordinary process. Therefore, in determining whether he be delivered on the demand of the state in which he is charged with crime, it must appear not only that he was properly indicted; it must also appear that he was within the state when the crime charged was committed, and also that he had *concealed himself*, or had *absconded*,

so he *could not be reached* by ordinary process (emphasis added).

To make one a fugitive from justice, it must appear, first, that he was within the state when the crime charged is alleged to have been committed; second, that, being amenable to criminal process, he either *concealed* himself, or *avoided* it so he could not be served, or that he *departed* the state, and so *avoided* service. If, therefore, it could be shown that *he did not conceal himself* within the state during the period which he was amenable to criminal process, this would be evidence establishing the fact that he was *not* a fugitive from justice (emphasis added). This testimony would not go to the sufficiency of the indictment, or to any manner of defense; it would be directed solely to whether he was a fugitive from justice -- a question of fact. *Id*. at 663.

One charged by indictment or affidavit before magistrate with offense and *leaving state* becomes "fugitive from justice," regardless of motive and belief (emphasis added). *Chase v. State*, 93 Fla. 963 (1927).

The Florida supreme court held a person charged by indictment, … with the commission within a state for a crime covered by its laws, and who after commission of such crime *leaves the state*, becomes, from the time of such leaving, a fugitive from justice … (emphasis added). *Chase v. State,* 93 Fla. 963, 976 (1927).

When a warrant is based upon a facially valid probable cause hearing *in the foreign state*, the accused may only defeat extradition on this issue by producing clear and convincing proof he is not a fugitive from justice (emphasis added). *Galloway v. Josey*, 507 So. 2d 590, 591 (Fla. 1987).

Whether an accused is a fugitive from justice asks nothing more than whether he was bodily present *in the demanding state* at the time of the offense and thereafter *departed from that state* (emphasis added). *Id.* at 594.

Since Gordon was in Florida only a few miles away from where the incident happened, and took no effort to conceal himself, he was *not* a fugitive. So the State can't rely on the exception to the general requirement that a search warrant was needed to use a Stingray device to locate him.

Gordon adopts and incorporates by reference as if fully stated herein, co-defendant Andres' *Reply to the State's Memorandum* filed on or about February 26, 2020.

CONCLUSION

By not seeking a warrant for the Stingray device, the State prohibited the Broward court from exercising its constitutional oversight function. There are complicated legal questions when the government seeks to employ a Stingray device.

When modern technology is invasive, the Court needs to be "careful to distinguish between rudimentary tracking . . . and more sweeping modes of surveillance," *Carpenter* 138 S.Ct. at 2215, and to ensure that "'[s]ubtler and more far-reaching means of invading privacy' . . . does not erode Fourth Amendment protections." *Id.* at 2223 (citing *Olmstead v. United States*, 277 U.S. 438, 473–74 (1928)). When a device has the inherent capacity to infringe on the reasonable expectations of privacy of large numbers of innocent suspects, Fourth Amendment concerns are amplified.

The State knew that use of this technology should at least be restrained by a probable cause warrant that mandates the minimization of innocent parties' data. Because law enforcement failed to obtain a warrant based on probable cause, no exception to the general warrant requirement or special consideration can justify this search.

Gordon respectfully requests an evidentiary hearing on the specific uses of the Stingray device, and that this Court grant *Gordon's Motion to Suppress Real-Time*

Cell Phone Tracking Using Cell-Site Simulator (filing# 99574110), and suppress any evidence and records obtained directly or indirectly by the Stingray device.

Respectfully submitted,

s/Michael Hursey
MICHAEL HURSEY, P.A.
Florida Bar No. 457698
Co-counsel for Defendant Gordon
5220 S. University Dr., Suite C-110
Ft. Lauderdale, FL 33328
Phone: (954) 252-7458
Fax: (954) 252-3353
Email: mhpalaw@bellsouth.net

s/ Paul Molle
Molle Law Firm
Florida Bar No. 116671
Co-counsel for Defendant Gordon
110 SE Sixth St., Suite 1703
Ft. Lauderdale, Florida 33301
Office: (954) 522-7575
Email: pmolle@bellsouth.net

CERTIFICATE OF SERVICE

I HEREBY CERTIFY the foregoing has been furnished via efiling at www.myflcourtaccess.com this 27th day of February, 2020.

s/Michael Hursey
MICHAEL HURSEY, P.A.