IN THE THIRD DISTRICT COURT OF APPEAL,
STATE OF FLORIDA

CASE NO. 3D21-1983
L.T. NO. 18-33927

RAUL MAS CANOSA,

Appellant,

vs.

CITY OF CORAL GABLES, *et al.*,

Appellees.

On Appeal from the Final Judgment
of the Circuit Court for the Eleventh Judicial Circuit
of Florida in and for Miami-Dade County

APPELLANT'S INITIAL BRIEF

Rene E. Lamar
Fla. Bar No. 294421
750 Saldano Avenue
Coral Gables, FL 33143
(305) 669-9081

Jared McClain (*Pro Hac* pending)
Richard A. Samp (*Pro Hac* pending)
NEW CIVIL LIBERTIES ALLIANCE
1225 19th Street NW, Suite 450
Washington, DC 20036
(202) 869-5210

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes & Other Authorities

INTRODUCTION

Mr. Raul Mas Canosa appeals the circuit court's grant of summary judgment against him and in favor of the City of Coral Gables ("City") and the Florida Department of Law Enforcement ("FDLE"). The City's use of its automated license plate readers ("ALPR") system, in reliance on a statewide policy that FDLE established in an unpromulgated rule, violates the Fourth Amendment to the United States Constitution and Article I, Section 23 of the Florida Constitution. Mr. Mas presents four issues on appeal:

(1) Whether Mr. Mas has standing to challenge the constitutionality of the City's warrantless recording and cataloguing his public movements, in searchable form, over the course of three years;
(2) Whether the City's ALPR program violates Mr. Mas's Fourth Amendment right to privacy from unreasonable searches and seizures;
(3) Whether the City's ALPR program violates Ms. Mas's right to privacy as protected by Article I, Section 23 of the Florida Constitution;
(4) Whether FDLE's guidance implementing a statewide policy for agencies' use of ALPRs is an unpromulgated rule in violation of the Florida Administrative Procedure Act.

STATEMENT OF THE CASE AND FACTS

A. FDLE's ALPR Guidelines

The Florida State Legislature passed two laws governing ALPR systems back in 2014. *See* §§ 316.0777, 316.0778, Fla. Stat. These provisions defined ALPRs as

a "system of one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of license plates into computer-readable data." *Id.* § 316.0777(c). Neither section addressed use of ALPRs to enforce laws. *See id.* §§ 316.0777-78.

Section 316.0778 tasked the Florida Department of State, "[i]n consultation with" FDLE, to "establish a retention schedule for records containing images and data generated through the use of an [ALPR] system." The legislature commanded that the agencies' "retention schedule must establish a maximum period that the records may be retained." *Id.* Pursuant to this statutory instruction, the Department of State promulgated Rule 1B-24.003(1)(b), General Records Schedule 2, Law Enforcement, Correctional Facilities and District Medical Examiners, Item # 217. R.1536. This rule provided for retention "until obsolete, superseded, or administrative value is lost, but no longer than 3 anniversary years unless required to be retained under another record series." R.1537.

FDLE set out to establish a more complete, uniform statewide policy. Prior to § 316.0778's passage, the Criminal and Juvenile Justice Information Systems Council ("CJJISC"), a council located within FDLE, held a meeting to recommend an ALPR use-and-retention policy. R.875-76. CJJIS held another meeting on August 21, 2014, at which it discussed "privacy concerns" with ALPRs and considered a 2008 assessment that the International Association of Chiefs of Police

("IACP") published. R.827, 833. The IACP report warned about the aggregation of ALPR data:

> Aggregation can cause dignitary harms because of its ability to unsettle an individual's expectations regarding how much information they actually reveal to others. In other words, personally identifiable information brought together from various source systems has the potential to reveal an individual's beliefs or ideas concerning public or social policy, as well as political, educational, cultural, economic, philosophical, or religious matters.
>
> Aggregation can also create interpretation problems where the data compilations used to judge the individual is incomplete or results in a distorted portrait of the person because the information is disconnected from the original context in which it was gathered.

R.903.

Additionally, IACP's report warned against the potential for misuse of stored data and that indefinite retention "can be a form of undesirable social control that can prevent people from engaging in activities that further their own self-development, and inhibit individuals from associating with others, which is sometimes critical for the promotion of free expression." R.923. CJJIS, however, dismissed these concerns because ALPR images identify "a specific vehicle, not a specific person," and the government has to take a second step to link the vehicle to a person. R.872.

Importantly, CJJIS recognized the "possibility that the guidelines may need to go through the rule promulgation process[,]" stating that "FDLE will verify with the Department of State." R.873. When CJJIS forward its proposed guideline to

FDLE, the director noted that personnel from the Department of State had agreed that "rules may need to be promulgated" to implement the ALPR retention schedule. R.1967. And again, in December 2014, CJJIS's director stated that the guidelines proposal was "scheduled to begin making its way to the rule making process in the next week." R.1968.

But FDLE skipped the rulemaking process. Instead, CJJIS simply published its final "Guidelines for the Use of Automated License Plate Readers" (the "Guidelines"). R.483. CJJIS relied on its authority under Florida Statute § 943.08, which allows the Council to "facilitate," "guide," and "support" data collection and retention by criminal-justice agencies and empowers the Council to set "standards," "best practices," and "recommendations." The statute does not, however, grant the Council rulemaking power.

Under the guise of guidance, FDLE issued its formal Guidelines to create a "uniform policy … pursuant to Section 943.08" and to "ensure that ALPRs are used in accordance with the substantive procedural safeguards" that FDLE set out in its Guidelines. R.483. The six-page document uses the mandatory word "shall" 13 times. R.483. The Guidelines explicitly instruct that "all law enforcement agencies must comply with Florida Statutes governing the use of ALPR data[,]" and set out FDLE's interpretation of that Florida law with which local agencies must comply. R.483.

Relevant to this case, Section 6 of the Guidelines leaves no doubt that local law-enforcement agencies must comply with FDLE's interpretation of Florida law:

> ALRP data **shall** he retained in accordance with Florida Statute 316.0778. **ALRP data** that are part of an ongoing or continuing investigation and information that is gathered and retained without specific suspicion **may be retained for no longer than 3 anniversary years**. Access to ALPR data for criminal investigations or intelligence purposes **is limited** to authorized Criminal personnel for no longer than 3 anniversary years and **requires** an agency case number or case. Data captured, stored, generated, or otherwise produced **shall be accessible in the ALPR system** for 30 days for tactical use.

R.487 (emphasis added).

The next subsection, entitled "Oversight, Evaluation, Auditing, and Enforcement," once against uses the compulsory word "shall" repeatedly:

> a. Oversight: Agencies **shall** maintain records documenting ALPR use, or ALPR data access and use, whether kept manually or by means of an automated record-keeping system. Agencies **shall** document in policy a reporting mechanism and a protocol to regularly monitor the use and deployment of ALPR systems to ensure strategic alignment and assessment of policy compliance.
> b. Evaluation: Agencies **shall** annually assess the overall performance of the ALPR system so that it can:
> - identify whether a technology is performing effectively;
> - identify operational factors that may impact performance effectiveness and/or efficiency;
> - identify data quality issues;
> - assess the business value and calculate return on investment of a technology; and
> - ensure proper technology refresh planning.
> c. Auditing: Agencies **shall** document in policy the manner in which audits will be conducted to include all access to data captured, stored, generated, or otherwise produced by the ALPR to ensure that

only authorized users are accessing the ALPR data and establish an annual audit schedule.

d. Enforcement: Agencies **shall** establish procedures for enforcement if users are suspected of being or have been found to be in noncompliance with the Agency's ALPR policy.

R.487-88 (emphasis added).

B. The City Adopted an ALPR Program Consistent with the Guidelines

Following FDLE's issuance of its Guidelines, in September 2015, Assistant Chief of the City's Police Department Michael C. Miller sent the City's then-Director of Public Safety a memorandum entitled, "CCTV/ALPR Project Scope," which proposed that the City adopt an ALPR program as a "public safety enhancement tool" "to assist police" in the "prevent[ion] of crime." R.552, 593. The City's corporate representative recognized that "the main purpose" "of this system [wa]s to either deter crime or help solve crimes." R.593, 599.

After considering third-party proposals, the City adopted Resolution No. 2015-307, which authorized the City to contract with a company named Safeway for 18 ALPR cameras at 11 locations that would form a "geofence" perimeter around the city, encompass the most traffic at the City's "main point[s]" of entry and "critical borders," and provide maximum surveillance potential 24 hours a day. R.595. The ALPRs would "surround[]" the City and capture "whatever comes through," recording the license place of every vehicle, and would "immediately" alert police of any vehicle "wanted for any type of crime." The City would then let

law enforcement to search and review all the collected data. R.1287-88. The City currently has ALPRs at 14 fixed locations and three more on portable trailers. R.1124.

The City created internal guidelines and a retention schedule for its ALPR data pursuant to FDLE's Guidelines. R.1321. Consistent with FDLE's Guidelines, the City allows access "for conducting ongoing or continuing criminal investigations." R.1477.

Resolution 2015-307 also authorized a contract with Vigilant Solutions to share the City's data with law-enforcement agencies in other jurisdictions. R.697. Vigilant's software interface, the Law Enforcement Archival and Reporting Network ("LEARN"), allows users to conduct historical and real-time inquiries into the collected data. R.697. Using LEARN, police can filter through the source of ALPR data, license-plate numbers, time periods, or even "geo-zoning," which "allows the user to actively search using an area of interest with or without a license plate number." R.1300-01. LEARN search results "include a color overview image of the vehicle, a picture of the license plate, [the] system's interpretation of the license plate, date and time of the scan, latitude and longitude[,] as well as the user and system that created the scan." R.750, 1303. The interface will also provide officers with "the geographic coordinates to the nearest physical address and nearest intersection." R.1303.

The City's contract with Vigilant allows unlimited system access to registered users. R.697, 1309-12. FDLE's guidelines require "general limits" on access "for the tactical enforcement of state statutes." R.483, 1475-76, 1560. The City, for its part, allows access "for conducting ongoing or continuing criminal investigations." R.1477. Neither policy requires a warrant, probable cause, or even a showing of reasonable suspicion. R.1477-78. Police need only a "legitimate law enforcement purpose" to search LEARN. R.1486. And even then, the City does not make users articulate a specific purpose; rather, they can simply write that their search is "for law enforcement purposes." R.1486. Worse, LEARN populates results regardless of whether the user fills in the "purpose" field. R.1486.

Vigilant stores the data on the City's servers subject to the City's data-retention schedule. R.697, 1309-12. Under the City's current schedule, based on the Guidelines, Vigilant retains ALPR data for three anniversary years. R.1310-11, 1321.

As of December 2019, LEARN had collected over 106 million images, 101 million of which it still retained pursuant to the City's data retention plan. R.1350-55. City personnel at that time had conducted 12,665 queries, with one user conducting more than 21% of the total searches, a tally of more than a search per day. R.1375-77. LEARN also runs automatic searches every three hours to search

for any plate numbers that appear on a "hotlist" of tags associated with an expired tag file, expired license file, and sanctioned driver file. R.836.

Once a user retrieves ALPR data, he or she can use it to obtain personal information associated with a license plate (*e.g.*, the name of the vehicle's registered owner, driver's license number and photograph, insurance information, and even their phone number) through the State's Driver and Vehicle Information Database ("DAVID"). R.1497-1501. It is "relatively common" for Coral Gables police officers to have access to both LEARN and DAVID, R.1497-98, negating the check on privacy rights on which CJJIS relied while ignoring the concerns outlined in IACP's 2008 report. R.872, 903, 923.

As with LEARN, there is no warrant or quantum-of-suspicion requirement to access personal information through DAVID. R.1501-02. DAVID users do not "necessarily have to suspect [] that the motorist is involved in some kind of criminal activity." R.1501, 1505-06.

The City also shares its database of over 100 million images with other jurisdictions. As of December 2019, the City elected to share its citizens' ALPR data with 68 other jurisdictions. R.832. Through such sharing agreements, the City also receives ALPR data of persons traveling through any one of 76 other jurisdictions. R.833.

C. The City's Surveillance of Mr. Mas

Mr. Mas, a self-employed marketing consultant, has been a Coral Gables resident since 1987. R.1158-59. He has no criminal record. R.1168. Until December 2020, Mr. Mas drove a red Ford Explorer. R.1161. It was "exceptionally rare" that anyone other than Mr. Mas drove the Explorer. R.1161-62.

In September 2018, the City generated a report of the images it collected of Mr. Mas's vehicle; it spanned 80 pages. R.750. Each page has an alert with a photograph of Mr. Mas's license plate, his vehicle, and additional "detection data," including the precise date and time, latitude and longitude of the vehicle, and an estimate of the nearest address and intersection. R.750, 1368-69. Mr. Mas is visible in these images, and some even show his dog's head hanging out the window. R.521-51, 1369. Inexplicably, the report also contains an image of Mr. Mas's car at 400 W. 42nd Street, Miami Beach, FL 33140, well beyond the City's jurisdiction. R.801.

A second query for Mr. Mas's license plate, in January 2020, returned 393 images. R.719. On several days, the results follow Mr. Mas's movement throughout the City, capturing his image, for example, five times on June 6, 2019, and six times on June 20, 2019. R.723-25.

Mr. Mas considers the City's ALPR program to be an invasion of his privacy:

> When I saw those approximately 80 pages of documents that the city sent me of my vehicle movements over a five-month period of time

> it became very obvious to me that the city had an exceptionally good idea of what my daily routine was[.] Because those images captured me going to the supermarket, to the drycleaner, to doctors[’] appointments, to .. the veterinarian with my dog, to a meeting with a client, to … a city commission meeting, to lunch with friends at a restaurant[.] … [Y]ou can put the pieces together and it really pretty much tells you what the daily routine of Raul Mas is on a day-to-day basis from some of these images.

R.1193-94.

D. Mr. Mas’s Lawsuit

Mr. Mas sued Appellees in October 2018, challenging the City’s adoption of its ALPR program and its use of those cameras to constantly record and store activity on the City’s major thoroughfares.[1] Specifically, Mr. Mas alleges that the City’s use of its ALPR system violates (1) the Fourth Amendment to the United States Constitution and (2) Article I, Section 23 of the Florida Constitution; that FDLE’s Guidelines also violate (3) the Fourth Amendment and (4) Section 23; and that FDLE’S Guidelines are (5) an invalid, unpromulgated rule. [2]

Following discovery, Mr. Mas moved separately for summary judgment against both the City and FDLE. He asserted that the ALPR program’s collection,

---

[1] Mr. Mas also sued the Florida Department of State and the Florida Secretary of State, but those parties successfully had the case against them transferred under the home-venue privilege. R.340. The Second Judicial Circuit dismissed these claims with prejudice on March 11, 2021. *Mas Canosa v. Dep’t of State*, No. 2019-CA-2813 (Fla. 2d Jud. Cir. Ct., Mar. 11, 2021).

[2] The complaint so alleged that the City’s use of ALPRs and data-retention program is improper legislative action, but the trial court dismissed those claims on October 16, 2019. R.322.

retention, and aggregation of his physical-location data over a three-year period invaded his privacy interests, protected by the Fourth Amendment and Section 23, by monitoring his public movements over time without a warrant or some exception to the warrant requirement. R.500. Mr. Mas explained that Florida courts have consistently protected against the government's indiscriminate collection and aggregation of a person's location information, and that the U.S. Supreme Court's recent decisions in *United States v. Jones*, 565 U.S. 400, 402 (2012), and *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018), expressly recognized that persons have a legitimate expectation of privacy in the record of their physical movements over time. R.502. Mr. Mas also argued that FDLE's Guidelines are unpromulgated rules that set out mandatory and generally applicable statements of law. R.853.

Appellees both filed cross-motions for summary judgment, and the trial court heard arguments on all four dispositive motions on August 31, 2021. After oral argument on the motions, the court directed Appellees to provide a written order ruling against Mr. Mas, which the court entered, as amended, on October 4, 2021. R.2156. In its order, the court refused to recognize the right to privacy in one's public movement over time. The crux of the court's decision was that, in 1983, the Supreme Court held that a person on a public thoroughfare has no reasonable expectation of privacy in their movement from one place to another, and that Florida's "pervasive regulation" of automobiles further reduces that expectation of

privacy. R.2162. The government's retention and aggregation of that location data over a three-year period made no difference to the court because the Florida Supreme Court, in a pre-*Carpenter* decision, criticized the "mosaic" theory of privacy rights. R.2164. Further, Mr. Mas was wrong to rely on *Carpenter* because cell-phone-location data reveals "the whole of [one's] physical movements in private and public spaces" and vehicle-location data "reveals only a vehicle's movements on public thoroughfares." R.2165. But the government's use of ALPR scanners here does not implicate Justice Alito's concerns in *Jones* because, unlike the device in *Jones*, ALPRs do "not 'secretly monitor and catalogue every single movement of an individual's car'—for any period of time." R.2167. In other words, the trial court ruled that there is no constitutional right of privacy in one's movement over time if the government stops short of monitoring and cataloguing the individual's every single public movement.

The privacy claims against FDLE also failed, the court concluded, because the City had adopted its own ALPR procedures before the Guidelines were *publicly* available (even though the City admitted that it developed its guidelines based on FDLE's) and because "a party that issued such guidelines is not responsible for an alleged constitutional violation, even if one had been found – and here there is none." R.2171.

Moving on to the administrative-law claim, the court held that the Guidelines' repeated use of "shall" did not make them mandatory because the Guidelines are not self-executing and do not actually require compliance. R.2172-73.

Finally, and remarkably, the court concluded that "an independent basis" for ruling against Mr. Mas was that he lacked standing. R.2176. Even though Mr. Mas alleged a constitutional injury based on the government's collection, retention, and aggregation of his location information, and the undisputed facts established that the government had compiled hundreds of photographs and corresponding data of Mr. Mas's movements throughout the City over three years, the court held that Mr. Mas failed to establish an actionable injury because the government has never "utilized" that data against Mr. Mas. R.2176.

Mr. Mas noted his timely appeal on October 13, 2021. R.2151.

SUMMARY OF ARGUMENT

Pursuant to FDLE's Guidelines, the City has been systematically violating Mr. Mas's privacy rights through its geofence of ALPRs that surrounds the City, surveilling its "major" streets on a constant basis. The City then retains that data in aggregated, searchable form for three years of unfettered, suspicion-less police use. Because this data retroactively reveals Mr. Mas's movements over time, the City's collection and retention of that information violates Mr. Mas's right to privacy, as

protected by the Fourth Amendment to the U.S. Constitution and Article I, Section 23 of the Florida Constitution.

Such allegations of constitutional harm, supported by proof that the City compiled over 400 images depicting his whereabouts, is more than enough to confer standing to sue upon Mr. Mas.

Finally, FDLE's Guidelines are an improper, unpromulgated rule. The Guidelines repeatedly use compulsory language as they implement a statewide ALPR use-and-retention policy based on FDLE's interpretation of the law. Because FDLE failed to issue its Guidelines through notice-and-comment rulemaking—despite recognizing at least three times that rulemaking was necessary—this Court should invalidate the Guidelines and require FDLE to engage in rulemaking.

This Court "review[s] the trial court's summary judgment order de novo." *Geico Gen. Ins. Co. v. Hialeah Diagnostics, Inc.*, 326 So. 3d 800, 802 (Fla. 3d DCA 2021).

ARGUMENT

I. MR. MAS HAS STANDING TO CHALLENGE THE GOVERNMENT'S SURVEILLANCE OF HIS MOVEMENTS OVER TIME

It's unusual for a standing analysis to come last in a court's analysis. That sequencing was necessary in this case, however, because the trial court's standing determination depended entirely on its merits conclusion that Mr. Mas has no privacy interest in the City's collection, retention, and aggregation of his location

data. But standing does not require success on the merits. The court's conclusion that Mr. Mas's subjective expectation of privacy was not one that society is prepared to recognize as objectively reasonable does not mean he lacked standing to assert that claim in the first place.

Mr. Mas has alleged that the City violated his constitutional rights by repeatedly collecting his location data as he travels throughout the City, seizing that data for three years, aggregating that information in a database accessible by law enforcement, and sharing that information with other jurisdictions. R.138-39. There is no dispute that the City has collected and maintained nearly 400 of images documenting Mr. Mas's whereabouts for three years at a time. It is a well-settled principle of Florida law that a person can sue any time his or her "constitutional rights have been abrogated or threatened by the provisions of the challenged act." *Hillsborough Inv. Co. v. Wilcox*, 13 S.2d 448, 453 (Fla. 1943).

But the trial court effectively limited relief to instances in which the government already (mis)used that unlawfully seized information. Such a rule diminishes the privacy rights of law-abiding citizens. The City, however, has *already* infringed Mr. Mas's privacy rights—even if none of its officers have further misused his improperly seized location data. As the IACP report explained, aggregation of location data "cause[s] dignitary harms because of its ability to unsettle individual's expectations regarding how much information they reveal to

others." R.903. The hundreds of images the City maintains of Mr. Mas exposes "personally identifiable information" that "reveal[s] an individual's beliefs or ideas concerning public or social policy, as well as political, educational, cultural, economic, philosophical, or religious matters." R.903. This system of "undesirable social control" has a chilling effect. R.903. Mr. Mas has a right to sue to stop the City's unlawful practice before it uses that information against him.[3] *Cf. Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 330 (4th Cir. 2021) (*en banc*) (allowing civil suit by community advocates to go forward to enjoin Baltimore's use of "a first-of-its-kind aerial surveillance program").

The collection itself has caused him a constitutional injury sufficient to confer standing. *See Carpenter*, 138 S. Ct. at 2212, 2221 ("[T]he *acquisition* of Carpenter's location data was a search. … Altogether the Government obtained 12,898 location points *cataloguing* Carpenter's movements[.]") (emphasis added); *Beautiful Struggle*, 2 F.4th at 344 ("*Carpenter* was clear on that issue[.]"); *Ferrari v. State*, 260 So.3d 296, 305 (Fla. 4th DCA 2018) ("[T]he *acquisition* of the cell tower records without a warrant based upon probable cause violated Ferrari's Fourth Amendment rights.") (emphasis added).

[3] *See* Zach Norris, *Opinion: At gunpoint, police handcuffed me after license-plate reader error*, The Mercury New (June 24, 2021).

And as the *en banc* Fourth Circuit just recognized, the government conducts a search not only by collecting raw data but also by integrating that data into "police information systems." *Beautiful Struggle*, 2 F.4th at 344. It is "relatively common" for Coral Gables police officers to have access to both LEARN and DAVID, R.1497-98; "these abilities enable police to glean insights from the whole of individuals' movements." *Id.*

Moreover, the trial court was simply wrong that the City has not searched Mr. Mas's location data. The LEARN system *automatically* searches the City's database every three hours. That the system did not flag Mr. Mas for appearing on the "hotlist," does not negate the City's eight daily searches of his data. The throwaway standing analysis the trial court tacked on to the end of its opinion was dangerously erroneous and would seriously curtail the protection of civil rights if affirmed.

II. THE CITY'S ALPR REGIME VIOLATES MR. MAS'S RIGHT TO PRIVACY

A. The Fourth Amendment Protects Mr. Mas's Legitimate Expectation of Privacy in His Public Movements over Time

The Fourth Amendment protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," absent a warrant supported by probable cause. The "basic purpose" of this Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" *Carpenter*, 138 S. Ct. at 2213 (citation

omitted). Thus, when an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," the official intrusion into the individual's privacy is presumptively unreasonable absent a warrant. *United States v. Karo*, 468 U.S. 705, 714-15 (1984); *Smith v. Maryland*, 442 U.S. 734, 740 (1979).

"Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings 'of what was deemed an unreasonable search and seizure[.]" *Carpenter*, 138 S. Ct. at 2213-14 (citation omitted). Even "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* After all, "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Id.* (citation omitted).

Fourth Amendment protections apply in public spaces. *See, e.g.*, *Katz v. United States*, 389 U.S. 347, 351 (1967) (finding a reasonable expectation of privacy in a public phone booth because "the Fourth Amendment protects people, not places"). "[W]hat [one] seeks to preserve as private, *even in an area accessible to the public*, may be constitutionally protected." *Id.* at 351 (emphasis added). Although public exposure may diminish one's privacy expectation, "[a] person does

not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter*, 138 S. Ct. at 2217. The Fourth Amendment protects this publicly visible information because "the sum of one's public movements" "reflects a wealth of detail about her familiar, political, professional, religious, and sexual associates." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

Carpenter adopted the concurrences of Justices Alito and Sotomayor for the constitutional principle that long-term surveillance can be a search—even in public. *Id.* at 2215 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring), and *id.* at 430 (Alito, J., concurring in judgment); *see also People v. Tafoya*, 494 P.3d 613, 619 (Colo. 2021) (recognizing that *Carpenter* "adopted the *Jones* concurrences").

1. ALPRs Are a Permeating Surveillance System

ALPRs are a technological innovation that enhance the government's surveillance abilities to an extent that "erode[s] the privacy guaranteed by the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (concluding that technology "not in general public use" implicates a reasonable expectation of privacy).

Traditionally, the Fourth Amendment does not protect a single viewing of a person or effect that is publicly visible, including a license-plate number. *See, e.g.*, *United States v. Ellison*, 462 F.3d 557, 561 (6th Cir. 2006). But the government's use of technology to monitor public movements more pervasively can trigger the

warrant requirement even if an officer could have, conceivably, conducted the same search in a single instance. Thus, whether the government may "conduct a search using the license-plate number to access information about the vehicle and its operator that may not otherwise be public or accessible by the police without heightened suspicion" presents a distinct question—particularly when the scope of the search far exceeds a single view. *Id.* at 567 (Moore, J., dissenting).

This "aggregation problem" is exactly what IACP recognized in its 2008 report. *Cf. also* Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 Minn. L. Rev. 577, 590 (2017). "When seen in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about us." *Id.* (quoting Daniel J. Solove, *Access & Aggregation: Public Records, Privacy & the Constitution*, 86 Minn. L. Rev. 1137, 1185 (2002)). Location data aggregated over time tells the government "a great deal more about the subject of the query than … any individual piece of data alone." *Id.* at 591.

The Supreme Court confronted the aggregation of surveillance in *Jones*, 565 U.S. at 402. Police used a GPS tracking device to monitor the movement of Jones's car to within 50 to 100 feet over a 28-day period. *Id.* at 403. The Court held that the search was constitutionally unreasonable because placing the device on the vehicle was a physical trespass, which obviated the need for the Court to rule on the "vexing problems" associated with the aggregation of data. *Id.* at 412-13.

A majority of the Justices wrote separately, though, and concluded that Jones had a reasonable expectation of privacy in his vehicle's movements over time. Justice Sotomayor explained that the government's compiling of a "comprehensive record of a person's public movements" violates a reasonable expectation of privacy and is, therefore, a search. *Id.* at 415 (Sotomayor, J., concurring). "And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" *Id*. (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004)).

Justice Alito, joined by Justices Ginsburg, Breyer and Kagan, wrote separately to highlight the constitutional problems with using technology to prolong the duration of a search: "[T]he use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id*. at 430.

As mentioned above, the concerns expressed by five justices in the *Jones* concurrences became the holding of the Court six years later in *Carpenter*, 138 S. Ct. at 2217. *Carpenter* held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through" digital

surveillance—regardless of whether those movements were disclosed to the public. *Id*. at 2215-17 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).

Carpenter "confront[ed] … how to apply the Fourth Amendment to … the ability to chronicle a person's past movements through the record of his cell phone signals." *Id.* at 2216. "Much like GPS tracking of a vehicle," the Court concluded, tracking a person's movement based on cell-site data reveals information about the person's movement that "is detailed, encyclopedic, and effortlessly compiled." *Id.* The Court was concerned both with the duration of the search and how its retrospective nature allowed the government to compile location data over time:

> [T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, **the Government can now travel back in time to retrace a person's whereabouts**, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years. **Critically, because location information is continually logged … this newfound tracking capacity runs against everyone. Unlike with the GPS device in Jones, police need not even know in advance whether they want to follow a particular individual, or when.**

Id. at 2218 (emphasis added). "Whoever the suspect turns out to be," when a crime occurs, the City's surveillance system has already "tailed" the suspect "every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment." *Id.*

Even if an individual voluntarily discloses this location information to third parties, and even if the government can only pinpoint a person's "location within 50 meters," the Court ruled, the government's monitoring of a suspect's cell-site location through his telephone records for a period of four months, "was a search within the meaning of the Fourth Amendment." *Id.* at 2212, 2219. Because it is a search, "the Government must generally obtain a warrant supported by probable cause before *acquiring* such records." *Id*. at 2220-21 (emphasis added).

The *Carpenter* decision was largely consistent with how Florida courts had already addressed long-term surveillance for some years. In *Tracey v. State*, the Florida Supreme Court had already held that law enforcement must obtain a warrant before collecting cell-site location information from the defendant's cell phone—even for just a *single day*'s worth of data. 152 So.3d 504, 507-08 (Fla. 2014). Quoting Justice Sotomayor's *Jones* concurrence, the Court recognized that technological advances impact the intrusion on privacy: "electronic monitoring of a citizen's location can generate a comprehensive record of a person's public movements," and that "[i]n the past, [] extensive tracking and monitoring required substantial government time and resources, which acted as a check on abusive law enforcement practices; but with the ease of electronic tracking and monitoring, those checks no longer exist." *Id.* at 519. "[S]uch monitoring" can now "be accomplished at a relatively low cost," enabling the government to "compile a substantial quantum

of information about any person whom the government chooses to track." *Id.* This capability alters "the relationship between citizen and government in a way that is inimical to democratic society." *Id.* (citation omitted). Accordingly, the Court "conclude[d] that such a subjective expectation of privacy of location as signaled by one's cell phone—*even on public roads*—is an expectation of privacy that society is now prepared to recognize as objectively reasonable[.]" *Id.* at 526 (emphasis added).

Although *Tracey* declined to adopt the "mosaic" theory of searches (and applied a "normative" theory instead), the Court did so without the benefit of *Carpenter*'s pronouncement that the Fourth Amendment protects against the use of "surveillance technology" to compile data on an individual's physical movements over time. 138 S. Ct. at 2217-20.

Decisions by the District Courts of Appeal since *Carpenter* have expanded on *Tracey*. The Fourth District Court of Appeal, for instance, relied on *Carpenter* in holding that the government's obtaining of historical cell-site location data from a single night was a search that requires a warrant supported by probable cause." *Ferrari*, 260 So.3d at 306. Even though the information revealed only that the target "did not move location," that was enough to constitute a search and require a warrant. *Id.* at 304.

And the Court in *State v. Sylvestre* established the firm constitutional limits imposed on the aggregation of public data. 254 So.3d 986, 990 (Fla. 4th Dist. Ct.

App. 2018). *Sylvestre* explained that "without a warrant, the government cannot: use technology to view information not visible to the naked eye, attach a device to property to monitor your location, search a cell phone in your possession without a warrant, or obtain real-time location information from the cell carrier." *Id.* at 991. Thus, the Fourth Amendment prevents the State from using "stingray" technology that could pinpoint the location of a single cell phone owned by defendant, in real time, "for several concurrent nights" without a warrant. *Id.* at 988.

Finally, in *State v. Martin*, the Court emphasized that cell-site simulator searches were anathema to the Fourth Amendment to such a degree that the traditional good-faith exception to the exclusionary rule would not apply to their use even before the *Sylvestre* decision. 287 So.3d 645, 648 (Fla. 4th Dist. Ct. App. 2019). The Court reasoned that the tracking of a person's movements, particularly when "law enforcement [can] track an individual's location in real time without going through the third-party service provider" raises such "significant privacy concerns" that it justifies the "heavy toll exclusion exacts on the judicial system." *Id*. (citation omitted).

Other courts have reached similar conclusions about the government's prolonged use of cameras in public spaces. The cameras that Baltimore Police used in *Beautiful Struggle* could not see inside the home, it was enough that aerial cameras tracked "shorter snippets" of people's public movements over "12-hour increments,"

enabling "photographic, retrospective location tracking," which was "enough to yield 'a wealth of detail,' greater than the sum of the individual trips." 2 F.4th at 342 (quoting *Jones*, 565 U.S. at 415-17 (Sotomayor, J., concurring)). "*Carpenter* held those deductions go to the privacies of life, the epitome of information expected to be beyond the warrantless reach of the government." *Id.* As in *Carpenter*, Baltimore police could "deduce such information only because it recorded *everyone's* movements." *Id.* Therefore, the surveillance of public movements "opens 'an intimate window' into a person's associations and activities, [so] it violates the reasonable expectation of privacy individuals have in the whole of their movements." *Id.*

The Colorado Supreme Court read *Carpenter* and *Jones* the same way in holding that the government's use of a pole camera was a search: "Together, *Jones* and *Carpenter* suggest that when government conduct involves continuous, long-term surveillance, it implicates a reasonable expectation of privacy. *Put simply, the duration, continuity, and nature of surveillance matter* when considering all the facts and circumstances in a particular case." *Tafoya*, 494 P.3d at 620 (emphasis added). "To reach an answer, we consider the public exposure of an area as well as the duration, continuity, and nature of the surveillance." *Id.* at 622. The court held that the pole camera was a search because police surveilled "the curtilage of Tafoya's property all day, every day for over three months" and "indefinitely stored the

footage gathered by the camera and could review it at any later date." *Id.* "This record, while not of Tafoya's movements as he traveled, still 'reflects a wealth of detail' about him and his associations. … As a result, police would know who Tafoya's friends and associates were, how often they came and went, and how long they stayed at his home." *Id.* at 622-23; *cf. Beautiful Struggle*, 2 F.4th at 345 (reasoning that cameras monitoring public roadways are *more* intrusive than pole cameras, which "are fixed in place, meaning they generally only capture individual trips").

Finally, the Massachusetts Supreme Judicial Court has addressed the circumstances presented here and held that unfettered law enforcement access to years of ALPR data violates the Fourth Amendment. *See Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1103 (Mass. 2020). An ALPR system photographed McCarthy's vehicle on two bridges over a three-month period. *Id*. at 1097. Relying on *Carpenter*, the court recognized the Fourth Amendment's original intent to "place obstacles in the way of a too permeating police surveillance." *Id*. at 1099 (quoting *Carpenter*, 138 S. Ct. at 2214). The Court warned that "advancing technology undercuts traditional checks on an overly pervasive police presence because it (1) is not limited by the same practical constraints that heretofore effectively have limited long-running surveillance, (2) proceeds surreptitiously, and (3) gives police access to categories of information previously unknowable." *Id*. This police presence can

invade a "recognized privacy interest in the whole of one's public movements" "[w]hen collected for a long enough period[.]" *Id*. at 1102 (citation omitted).

Applying these principles to ALPRs, the court ruled: "With enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes." *Id*. at 1104. Importantly, the Court emphasized that "[i]n determining whether a reasonable expectation of privacy has been invaded, it is not the amount of data that the Commonwealth seeks to admit in evidence that counts, but, rather, the amount of data that the government *collects* or to which it gains access." *Id*. (emphasis added).

The Massachusetts court identified three features that would bring ALPRs in tension with privacy rights. *First*, the reach of the ALPR system: "A network of ALPRs that surveils every residential side street paints a much more nuanced and invasive picture of a driver's life and public movements than one limited to major highways that open into innumerable possible destinations." *Id.* *Second*, the extent of data retention: "The one-year retention period indicated in the [Massachusetts] retention policy certainly is long enough to warrant constitutional protection." *Id*. *Third*, whether real-time alerts occur: "[W]ith cameras in enough locations, the hot

list feature could implicate constitutional search protections by invading a reasonable expectation of privacy in one's real-time location."[4] *Id*. at 1105.

2. Mr. Mas Has a Reasonable Expectation of Privacy in His Movements over Time

Mr. Mas testified that the City's ALPR program "[a]bsolutely" invades his right to privacy. R.1193. This expectation is one that society is prepared to recognize as reasonable.

The City uses a "geofence" of cameras at 14 fixed locations and three more on portable trailers to "surround[]" the City and capture "whatever comes through." R.465, 1287-88**.** Using these cameras, the City has photographed Mr. Mas *hundreds* of time, cataloguing a color image of him in his vehicle, the date, time, and location of the scan, and "the geographic coordinates to the nearest physical address and nearest intersection." R.1303. The City then aggregates and stores this data in searchable form in its LEARN system, which conducts automatic searches of Mr. Mas's location data every three hours to make sure he isn't on the "hotlist." If the

[4] Applying these factors in *McCarthy*, the Court concluded that suppression was not necessary because the government used only "four cameras placed at two fixed locations on the ends of the Bourne and Sagamore bridges" monitored for only three months. 142 N.E.3d at 1097, 1105. *Cf. also United States v. Rubin*, 2021 WL 3773609, at *5 (N.D. Cal. Aug. 25, 2021) (finding ALPR use was not a search when record revealed a handful of images in a month) (relying on *United States v. Yang*, 958 F.3d 851, 863 (9th Cir. 2020) (Bea, J., concurring) ("Despite its 5 billion total records, the LEARN database contained a *single* entry for the Yukon that Yang had rented.") (emphasis added)).

system were to flag Mr. Mas's license plate, it would send an automatic alert to police. Even without an alert, many LEARN users can use Mr. Mas's data to cross-search other government databases.

The City's compilation of Mr. Mas's whereabouts over a three-year interval "implicates privacy concerns far beyond" those that would arise if the City just took a single photo of Mr. Mas's vehicle or had an officer follow him through the City for a single day. *See Carpenter*, 138 S. Ct. at 2220. Looking back on its dataset, the City can determine Mr. Mas's movements in detail on specific days. For instance, on June 20, 2019, the system noted Mr. Mas's location six times between 8:18 a.m. and 7:34 p.m. R.723-25. The police also know where he has gone during his days, such as tracking his drive to the gym on July 4, 2019, after he was logged at 527 S. Dixie Hwy at 5:34 a.m. and then at the University of Miami at 5:57 a.m. R.723-35. Police even know that Mr. Mas travels with his dog in the passenger seat. R.1196, 1369.

As IACP warned, and the courts recognized in *Jones*, *Carpenter*, *Beautiful Struggle*, and *Tafoya*, the compilation of location data reveals a lot about a person's life and their associations. Mr. Mas recognized this as well. He testified that "the city ha[s] an exceptionally good idea of what my daily routine was[.] Because those images captured me going to the supermarket, to the drycleaner, to doctors' appointments, to … the veterinarian with my dog, to a meeting with a client, to … a

city commission meeting, to lunch with friends at a restaurant[.] … [Y]ou can put the pieces together and it really pretty much tells you what the daily routine of Raul Mas is on a day-to-day basis from some of these images." R.1193.

The supreme courts in Massachusetts and Colorado crafted tests for video surveillance that account for the duration and extent of the surveillance. *See Tafoya*, 494 P.3d at 620; *McCarthy*, 142 N.E.3d at 1104-05. Any variation of those tests confirms the search here because the City's ALPR program here exceeds the scope and duration of any of those previously considered. The City has violated Mr. Mas's reasonable expectation of privacy in his movements over time.

B. The Trial Court Failed to Account for Technological Advances

The trial court erred in holding that Mr. Mas lacks a legitimate expectation of privacy. Presented with novel facts concerning advanced technology unavailable to the general public, *see Kyllo*, 533 U.S. at 34, the court wrongly compared ALPRs to the outdated analog of a radio-beeper device simply because both devices tracked movements on public roads. R.2162 (applying *United States v. Knotts*, 460 U.S. 276, 281-82 (1983)); *but see Bailey v. State*, 311 So.3d 303, 311 (Fla. 1st DCA 2020) (instructing that courts must examine government surveillance "on a case-by-case basis to determine whether a search occurred"). The decision below is out of step with modern surveillance techniques and modern jurisprudence.

Indeed, even *Knotts* recognized the limitations on its holding that the court below ignored. *Knotts* cautioned that a different rule might apply to surveillance of every citizen as opposed to the discrete search of a suspect's movements from Point A to Point B. *See* 460 U.S. at 283-85. The decision was not a blank check for police whenever "electronic-type tracking occurs in public areas." *Tracey*, 152 So.3d at 513, 525 ("In the *Knotts* era, high tech tracking such as now occurs was not within the purview of public awareness or general availability. Thus, we conclude that we are not bound to apply the holding in *Knotts* to the current, and different, factual scenario."). The trial court's reliance on cases permitting surveillance of a single trip, or an officer's single viewing of a license plate, ignore the aggregation problem the Supreme Court addressed in *Jones* and *Carpenter* that led the Court to hold that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through" digital surveillance—regardless of whether those movements were disclosed to the public at large. *Id*. at 2215-17 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).

As the *en banc* Fourth Circuit recognized in *Beautiful Struggle*, the government's use of cameras to photograph and catalogue movements along public roads is "[m]ore like the CSLI in *Carpenter* and GPS-data in *Jones* than the radio-beeper in *Knotts*," because the system creates "a 'detailed, encyclopedic,' record of where everyone came and went[.]" 2 F.4th at 341; *see also Carpenter*, 138 S. Ct. at

2215 (distinguishing the "rudimentary tracking facilitated by the beeper" in *Knotts* from "more sweeping modes of surveillance" in *Carpenter* because the tracking in *Knotts* was for a limited, discrete use during a single journey). A database of photographs allows the government to "'travel back in time' to observe a target's movements, forwards and backwards." *Beautiful Struggle*, 2 F.4th at 341 (citing *Carpenter*, 138 S. Ct. at 2218). The Fourth Circuit also dismissed the notion—adopted by the trial court here—that photographic monitoring is less pervasive:

> [Aerial Investigative Research] data is a photographic record of movements, surpassing the precision even of GPS data and CSLI, which record variable location points from which movements can be reconstructed. And while the coverage is not 24/7, most people do most of their moving during the daytime, not overnight. Likewise, many people start and end most days at home, following a relatively habitual pattern in between. These habits, analyzed with other available information, will often be enough for law enforcement to deduce the people behind the pixels. And if a track is interrupted by sunset, police will at least sometimes be able to re-identify the same target over consecutive days. For example, law enforcement could use AIR data to track a person's movements from a crime scene to, eventually, a residential location where the person remains. They could then look through time and track movements from that residence. They could use any number of context clues to distinguish individuals and deduce identity. After all, the AIR program's express goal is to identify suspects and witnesses to help BPD solve crimes.

Id. at 343. Then, just like the City here, Baltimore police could "cross-reference" that data "against publicly available information and, even more valuably, their own data systems." *Id.* at 344.

None of this technology was invented—much less at issue—in *Knotts*. The trial court's decision completely failed to account for the retrospective nature of the City's ongoing search that the *Carpenter* Court held to "implicate privacy concerns far beyond those considered" in prior cases. 138 S. Ct. at 2220. "There is a world of difference" between a single search "and the exhaustive chronicle of location information casually collected" using today's technology. *Id.* at 2219. "Thus, *Carpenter* solidified the line between short-term tracking of public movements—akin to what law enforcement could do 'prior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns. The latter form of surveillance invades the reasonable expectation of privacy that individuals have in the whole of their movements over time." *Beautiful Struggle*, 2 F.4th at 341.

The trial court's disregard of these distinctions helps explain its mistaken reliance on *Bailey*, 311 So.3d at 303. Although *Bailey* applied *Knotts* rather than *Carpenter*, the First District Court of Appeal did not adopt some general rule that there is no legitimate expectation of privacy on public roads. Instead, the Court grappled with whether *Carpenter* altered the way the third-party doctrine applies to a person's expectation of privacy while driving *for one night* in *someone else's car* when that vehicle was *already equipped* with a GPS tracking device that the owner had *consented* to attaching on the car. *Id.* at 314-15. Dealing with the particular facts before it, the Court reasoned that Bailey "chose to operate a car on public

roads—a car owned by another who *consented to GPS tracking*. The police played *no role* in the recording of the information and simply availed themselves of the advantages." *Id.* at 315 (emphasis added). The Court concluded that the third-party doctrine applied to defeat Bailey's expectation of privacy, despite *Carpenter*'s refusal to apply the third-party doctrine to cell-phone data, because "[n]othing forced [Bailey] to use the Honda owned by his girlfriend, and any number of other means of travel were available which were not being tracked. *Use of a car owned by another* to traverse public streets renders Appellant's purported expectation of privacy unreasonable." *Id.* (emphasis added); *see also id.* at 314 ("[T]he consent to tracking on the part of the car owner further dilutes the argument that the precedent of *Carpenter* controls.").

As if all those unique facts supporting the court's application of the third-party doctrine were not enough to distinguish *Bailey* from Mr. Mas's case, the First District Court of Appeal also based its holding on the finite period of time that police tracked Bailey's girlfriend's car: "Although the Court in *Carpenter* forbid the government from warrantlessly accessing seven days of historical CSLI from a target's wireless carriers, it refused to address whether one's 'reasonable expectation of privacy in the whole of his physical movements' extends to *shorter* periods of time or to other location tracking devices." *Id.* (quoting *Carpenter*, 138 S. Ct. at 2217 n.3, 2219) (emphasis added). The court held that tracking Bailey's location

over *one night* while he drove *someone else's car* that was already equipped with a tracking device did not violate the Fourth Amendment. *Id.*

Moreover, *Bailey* "acknowledge[d]" that *Knotts* applied to "the '*limited* use which the government made of the signals from this particular beeper' during a *discrete* 'automotive journey,'" and the Court reserved on the question of whether a different rule would apply if technology allowing for twenty-four hour surveillance existed. *See* 311 So.3d at 314 (quoting *Knotts*, 460 U.S. at 283-85) (emphasis added); *Tracey*, 152 So.3d at 513 ("The Court [in *Knotts*] noted that the officers simply augmented their sensory faculties of observation of the vehicle by use of the beeper. … The Court specifically left open the question of the application of the Fourth Amendment to longer term surveillance, stating 'if such dragnet-type law enforcement practices … should eventually occur, there will be time enough then to determine whether different constitutional principles apply.").

Finally, the trial court also relied on an unduly narrow reading of *Jones*. Ignoring entirely the portions of Justice Sotomayor's concurrence that *Carpenter* later adopted, the trial court distinguished *Jones* because the City's ALPRs are not secret and don't catalogue *every single* movement that Mr. Mas makes on public roads. R.2167. But one's advance knowledge of unreasonable governmental action does not negate an ongoing expectation that the government will abide by the law and conduct only reasonable searches supported by probable cause. *Tracey*, 152

So.3d at 522 ("Simply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes … does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes."). Whether the target of a search is aware that the search might occur is in no way dispositive. *See California v. Ciraolo*, 476 U.S. 207, 211 (1986). After all, a person illegally frisked has suffered a constitutional injury despite being well aware of an officer's roving hands. *See, e.g.*, *Arizona v. Johnson*, 555 U.S. 323, 334 (2009). The trial court's contrary rationale would permit pervasive surveillance so long as the government makes the public aware that it's watching.

III. THE CITY'S ALPR SYSTEM VIOLATES THE FLORIDA CONSTITUTION

The City's ALPR system also violates Florida's strengthened right of privacy. Article I, Section 23, of the Florida Constitution recognizes that the "concept of privacy or right to be let alone is deeply rooted in our heritage and is founded upon historical notions and federal constitutional expressions of ordered liberty." *Winfield v. Div. of Pari-Mutuel Wagering, Dep't of Bus. Regulation*, 477 So. 2d 544, 546 (Fla. 1985). This constitutional protection was also a response to the Fourth Amendment's limitations, and Florida's recognition that "the Supreme Court has given much of the responsibility to the individual state" "[i]n formulating privacy interests." *Id.* at 547. Thus, "[t]he right to privacy provided for in the Florida

Constitution is broader in scope than the protection provided in the United States Constitution." *Thomas v. Smith*, 882 So. 2d 1037, 1043 (Fla. 2d DCA 2004). "One of the principal concerns of the drafters of the amendment that became article I, section 23 was the right to informational privacy." *Id.* "Although the general concept of privacy encompasses an enormously broad and diverse field of personal action and belief, there can be no doubt that the Florida amendment was intended to protect the right to determine whether or not sensitive information about oneself will be disclosed to others." *Rasmussen v. S. Fla. Blood Serv., Inc.*, 500 So. 2d 533, 536 (Fla. 1987). Indeed, "a principal aim of the constitutional provision is to afford individuals some protection against the increasing collection, retention, and use of information relating to all facets of an individual's life" "by computer operated information systems." *Id*.

The "right to privacy" attaches whenever a person has a "reasonable expectation of privacy" in the object of the search. *Id*. If such an expectation exists, the right of privacy "is a fundamental right which … demands [a] compelling state interest" *before* it can be invaded. *Id*. The state bears the burden of proof "to justify an intrusion on privacy," which it can meet only by "demonstrating that the challenged regulation serves a compelling state interest and accomplishes its goal through the use of the least intrusive means." *Id*.

Florida courts have routinely found Section 23 to protect interests that were plainly *not* protected by the Fourth Amendment. For example, the "names and contact information" of "Hotel guests" "are constitutionally protected, private details." *Josifov v. Kamal-Hasmat*, 217 So.3d 1085, 1087 (Fla. 3d DCA 2017). Similarly, financial records have been deemed protected by Section 23, *Inglis v. Casselberry*, 200 So.3d 206, 212 (Fla. 2d DCA 2016), as have an individual's Social Security Number, *Thomas*, 882 So.2d at 1043, and even the names and addresses of blood donors have been protected from intrusion. *Rasmussen*, 500 So.2d at 536. The Florida Supreme Court meant its pronouncement that Section 23 "embraces more privacy interests, and extends more protection to the individual in those interests, than does the federal Constitution." *State v. J.P.*, 907 So.2d 1101, 1112 (Fla. 2004).

The City's ALPR system violates Section 23 because the collection and dissemination of three years' worth of location data in a searchable database intrudes into precisely the types of private areas Section 23 is meant to protect. Perhaps most obviously, Florida law already considers this information private and only allows dissemination to an individual if s/he *waives* her or his privacy protections. ALPR data is *exempt* from Florida's public records law, meaning that it is protected from disclosure by state actors. *See* § 316.0777, Fla. Stat. That is why Mr. Mas had to waive his privacy interests to access his *own* records. Yet, the City not only collects

this private information systematically, but *shares it* indiscriminately with 68 other jurisdictions, including the FBI. R.832, 1389.

Moreover, as discussed above, the aggregated data in the City's ALPR system seriously intrudes into the privacy of its residents. The system has aggregated more than 106 *million* images that police can use indiscriminately to track the movements of innocent people like Mr. Mas as they travel throughout the City over a three-year period. *See* R.1266-67, 1389-91. If Section 23 protects the names and contact information of hotel guests, as in *Josifov*, 217 So.3d at 1087, and the names and addresses of blood donors, as in *Rasmussen*, 500 So. 2d at 536, the much greater intrusion at issue here unquestionably violates the Florida Constitution.

The City cannot meet its burden to "demonstrate[e] that the challenged regulation serves a compelling state interest and accomplishes its goal through the use of the least intrusive means." *Id.* at 536. According to the City, "the main purpose" "of this system [wa]s to either deter crime or help solve crimes." R.1463-64. To accomplish this goal, the City constantly surveils its public roads and catalogues images of vehicles—without any suspicion—for three years. Despite this massive amount of surveillance data, the City can only identify a handful of arrests based on ALPR data. *See* R.425. This per-image success rate is so infinitesimally small that show the lack of "clear connection" between any illegal activity and invading the privacy of the millions of affected motorists whose privacy the City is

invading. *See Shaktman v. State*, 553 So.2d 148, 152 (Fla. 1989) (requiring "a clear connection between [] *illegal activity* and *the person whose privacy would be invading*"). And the system falls well short of the least intrusive means available.

The City could tailor the system far more narrowly and thereby abide by the state constitution's privacy provision. It could, for instance, institute a warrant requirement and significantly limit the data-retention period. These measures would have no appreciable impact on the system's minuscule success rate, yet they would respect constitutional limits. Or the City could, in real time, check information contained in databases on stole plates, Amber alerts, and the like against license-plate images without keeping data on every image in a three-year span, unless the real-time check of the "hotlist" gives rise to further suspicion. Instead, the City is eroding the privacy rights of all to help solve a handful of crimes. Its failure to tailor the system in any meaningful way it violates Section 23. *See id*.

IV. FDLE'S GUIDELINES ARE AN UNPROMULGATED RULE

The purpose of Florida's APA is to "press the executive inexorably toward rulemaking[.]" *Dep't of Heath & Rehab. Servs. v. Framat Realty, Inc.*, 407 So.2d 238, 241 (Fla. 1st DCA 1981). Agencies use rulemaking to "interpret statutes in their regulatory care[.]" *Id.* The legislature confers rulemaking authority on agencies to interpret and implement the statutory provisions they administer. *See Ortiz v. Dep't of Health, Bd. of Medicine*, 882 So.2d 402, 403 (Fla. 4th DCA 2004).

When the legislature passed laws on ALPRs, it instructed FDLE, along with the State Department, to implement those laws by establishing a use-and-retention schedule that sets a maximum period that "records containing images and data generated through the use of an [ALPR] system" can be retained. § 316.0778, Fla. Stat.

The State Department and CJJIS recognized at least three times during the drafting process that such guidelines would have to go through the rulemaking process. R. 873, 1967-68. Despite this recognition—and despite the Guidelines' setting a statewide policy that repeatedly uses mandatory terms when interpreting and implementing the statute—FDLE chose to eschew the rulemaking process.

FDLE attempts to avoid the obvious conclusion that its Guidelines apply "uniform[ly] statewide … pursuant to Section 943.08," R.483, by highlighting that not every single clause of every single sentence is explicitly compulsory. But the Guidelines are a direct response to a legislative directive to set a uniform policy that mandates how localities operate their ALPR systems. Recognizing this, the City (and surely other agencies) understood that the Guidelines are binding and "set" "the limit" on their use of ALPR data. R.1321. The trial court also seemed to recognize the Guidelines' binding nature earlier in proceedings when it dismissed Counts VIII and IX of Mr. Mas's amended complaint because the City lacked any authority to destroy ALPR data after 30 days because doing so would violate the State's retention policy. R.340.

The APA required FDLE to promulgate its Guidelines through the rulemaking process, and the trial court erred in holding that the Guidelines are simply "best practices." R.2173.

A. The APA Forbids Unadopted Rules

The APA defines a "rule" as an "agency statement of general applicability that implements, interprets, or prescribes law or policy or describes the procedure or practice requirements of an agency and includes any form which imposes *any* requirement or solicits any information not specifically required by statute or by an existing rule." § 120.52(16), Fla. Stat. (emphasis added). In other words, a rule is any "agency statement that either requires compliance, creates certain rights while adversely affecting others, or otherwise has the direct and consistent effect of law[.]" *Dep't of Revenue v. Vanjaria Enter., Inc.*, 675 So.2d 252, 255 (Fla. 5th DCA 1996). If an agency policy "adversely affect[s] the rights of others, it is a rule." *Coventry First, LLC v. Office of Ins. Reg.*, 38 So.3d 200, 203 (Fla. 1st DCA 2020) (emphasis added).

Consistent with the legislative purpose of the APA, Florida courts interpret "the term to cover a great variety of agency statements regardless of how the agency designates them." *Dep't of Admin., Div. of Pers. v. Harvey*, 356 So.2d 323, 325 (Fla. 1st DCA 1977). Consequently, the rulemaking requirement applies to mere "agency[] polic[ies]" of "general applicability." *Dep't of Highway Safety & Motor*

Vehicles v. Schluter, 705 So. 2d 81, 83 (Fla. 1st DCA 1997). So long as an agency policy applies certain criteria to a given circumstance, it is a "rule" that must go through notice-and-comment procedures. *Id.* at 85. Such policies include any "principle, plan, or course of action, as pursued by a government, organization, individual, etc.," and need not even be written down. *Id.* at 83-84. Even an agency policy of *issuing licenses* can be a rule if the agency applies a uniform interpretation of a statute in a way that affects rights. *See Fla. Quarter Horse Track Ass'n, Inc. v. Dep't of Bus. & Prof'l Reg., Div. of Pari-Mutuel Wagering*, 133 So.3d 1118, 1119, 1225 & n.2 (Fla. 1st DCA 2014). The courts' application of these principles reflects the legislature's preference for rulemaking when an agency interprets or implements the law. *See Framat Realty*, 407 So.2d at 241.

B. The Guidelines Interpret Law and Implement a General Policy

The Guidelines are a rule within the meaning of § 120.52(16). Pursuant to an explicit statutory delegation of authority, the Guidelines purport to impose a set of limitations on the retention of ALPR data. *See* § 316.0778(2), Fla. Stat. (instructing that FDLE, in consultation with the State Department, "*must* establish a maximum period that the records may be retained"). This mandatory directive establishes that localities cannot exceed the Guidelines that the agency sets.

Contrary to the trial court's rationale, R.2174, the Guidelines do more than simply restate a statutory requirement; they interpret and implement the ALPR

statutes. The Guidelines expand on a statutory command and set precise limitations on agencies' use and retention of ALPR data, and they do so in mandatory terms.

Subsection 6.e., for instance, begins by mandating that agencies "shall" comply with § 316.0778, which, again, tasked FDLE to establish a statewide data-retention policy. R.1978. The Guidelines' invocation of this statutory directive signals that the policy that follows is FDLE's interpretation of the law pursuant to its statutory mandate.

The next sentence tells agencies that they can keep ALPR data for "no longer than 3 anniversary years," which leaves little doubt that local agencies lack authority to adopt policies that contravene FDLE's Guidelines. Then, FDLE expressly "limit[s] who may access ALPR data and "requires" agencies to use a case number. R.1978. These instructions do not read like mere suggestions to localities. The final sentence of the subsection again uses the word "shall" to require that agencies make their ALPR data "accessible in the ALPR system for 30 days for tactical use." R.1978. Read together, Subsection 6.e. articulates a statewide policy for how all agencies must use and retain their ALPR data.

Section 7, entitled "Oversight, Evaluation, Auditing, and Enforcement," is no different. Set out more fully above, this section also stakes out a generally applicable policy and requires the compliance of covered agencies through FDLE's repeated use of compulsory language: agencies "*shall* maintain records … to ensure strategic

alignment and assessment of policy compliance," "*shall* document in policy a reporting mechanism," "*shall* annually assess the overall performance of the ALPR system," "*shall* document in policy the manner in which audits will be conducted," and "*shall* establish procedures for enforcement" if its users violate the agency's policy. R.1978.

These provisions of the Guidelines are straightforward "agency statement[]s that either require compliance, create[] certain rights while adversely affecting others, or otherwise ha[ve] the direct and consistent effect of law" because they clearly demarcate what the statute permits, according to FDLE's interpretation. *See Vanjaria Enter.*, 675 So.2d at 255. The Court does not need to infer this premise—the Guidelines say it outright. The Guidelines state explicitly that FDLE's purpose in issuing its policy was to "ensure that ALPRs and ALPR-generated data are used only in a manner that is lawful" and that the Guidelines establish "uniform statewide guidelines" for the use and retention of ALPR data. R.483.

It's no wonder that CJJIS staff believed the Guidelines had to go through the rulemaking process. Such policies of general applicability and requirements of compliance fall squarely within § 120.52(16)'s definition of a rule. Tellingly, FDLE has not suggested that localities that use ALPRs are free to ignore its Guidelines. The very purpose of the Guidelines was to implement a uniform statewide use-and-retention policy consistent with FDLE's interpretation of the law. *See Grabba-Leaf,*

LLC v. Dep't of Bus. And Prof'l Reg., 257 So.3d 1205, 1211 (Fla. 1st DCA 2018) ("The Department's memo constituted a 'rule' because it is a statement of general applicability that implements and interprets the law."). The City recognized this purpose and understood that the Guidelines "set" "the limit" on its use and retention of ALPR data. R.1321.

The trial court erred by ignoring all the traditional hallmarks of a rule on the ground that the Guidelines don't include an inter-governmental enforcement mechanism. But a statewide policy of sanctioning local governments for their failure to comply with state preferences is not what qualifies a policy as a "rule." *Cf. Fal. League of Cities, Inc. v. Admin. Comm'n*, 586 So.2d 397, 406 (Fla. 1st DCA 1991) ("The sanctions policy fits the definition of incipient or evolving policy, and not the section 120.52(16) definition of a rule."). Moreover, the lack of an enforcement mechanism is no surprise since the statute authorizes none and the FDLE lacks rulemaking power to punish municipalities absent legislative authorization. *See* § 120.54(1)(e) – (f), Fla. Stat. And even without an enforcement mechanism, FDLE's repeated use of the word "shall" throughout the Guidelines "has a mandatory connotation." *S.R. v. State*, 346 So.2d 1018, 1019 (Fla. 1977). These features make the Guidelines a rule.

C. The Guidelines Also Affect Rights by Permitting Unconstitutional Data Gathering and Dissemination to Law Enforcement

The Guidelines also qualify as a rule because they are an agency statement of general policy that adversely affects the rights of others. *See Vanjaria Enter.*, 675 So.2d at 255. As set out more fully in Argument Section II, the Guidelines facilitate—and purport to permit, under color of State law—the unconstitutional collection, retention, and aggregation of Mr. Mas's location data, as well as the dissemination of that data to other law-enforcement agencies. The Guidelines create a permission system for localities to systematically violate the privacy rights of Floridians by sanctioning the indiscriminate and continual collection of ALPR data from every vehicle in "public view." R.484. The City used the Guidelines as a framework to infringe Mr. Mas's privacy rights. His injury is traceable to FDLE's generally applicable policy. FDLE violated the APA by failing to promulgate that policy through the required rulemaking procedures.

CONCLUSION

This Court should reverse the trial court's grant of summary judgment in favor of the City and FDLE, and against Mr. Mas.

Respectfully,

Rene E. Lamar
Fla. Bar No. 294421
750 Saldano Avenue
Coral Gables, FL 33143
(305) 669-9081

Jared McClain (*Pro Hac* pending)
Richard A. Samp (*Pro Hac* pending)
NEW CIVIL LIBERTIES ALLIANCE
1225 19th Street NW, Suite 450
Washington, DC 20036

(202) 869-5210

Dated: December 13, 2021

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of this Initial Brief on Appeal has been filed and served electronically on this 13th day of December 2021 upon:

Abigail G. Corbett, Esq.
Veronica L. De Zayas, Esq.
Stearns Weaver Miller Weissler
Alhadeff & Sitterson, P.A.
150 W. Flagler St.
Suite 2200
Miami, FL 33130
acorbett@stearnsweaver.com
vdezayas@stearnsweaver.com

Counsel for Appellee City of Coral Gables

Barbara Junge, Eq.
Office of the Attorney General
110 SE 6th St., 10th floor
Fr. Lauderdale, FL 33301
Barbara.Junge@myfloridalegal.com

Frank A. Shepherd, Esq.
Jack R. Reiter, Esq.
333 SE Second Ave., Suite 3200
Miami, FL 33131
Frank.Shepherd@gray-robinson.com
Jack.Reiter@gray-robinson.com

Co-counsel for Appellees FDLE and Swearingen

/s/ Rene E. Lamar

CERTIFICATE OF COMPLIANCE

I HEREBY certify that this computer-generated brief complies with the Florida Rules of Appellate Procedure, because this brief was prepared in Times New Roman font, size 14, and contains fewer than 50 pages, pursuant to Rule 9.210.

/s/ Rene E. Lamar