IN THE CIRCUIT COURT OF THE 11TH
JUDICIAL CIRCUIT IN AND FOR
MIAMI-DADE COUNTY, FLORIDA

RAUL MAS CANOSA CASE NO.: 2018-33927-CA-01

Plaintiff,
vs.

CITY OF CORAL GABLES, FLORIDA, et al.

Defendants.
_____/

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AGAINST DEFENDANT CITY OF CORAL GABLES

Plaintiff, Raul Mas Canosa, moves for summary judgment against Defendant City of Coral Gables, Florida. For the reasons set out below, this Court should grant summary judgment for Mr. Mas and against the City on Counts III and VI of his amended complaint and issue a judgment declaring that the City's system of automated license plate reading cameras is unconstitutional pursuant to the Fourth Amendment of the United States Constitution and Article I, Section 23 of the Florida State Constitution.

I. INTRODUCTION

"[T]he sum of one's public movements," "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Comprehensive monitoring of a vehicle's public movements in traffic reveals information of such an "indisputably private" nature it "takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *People v. Weaver*, 12 N.Y.3d 433, 441-442 (N.Y. 2009).

As Florida's Supreme Court has recognized, "[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." *Tracey v. States*, 152 So.3d 504, 519 (Fla. 2014). Indeed, "such monitoring" can now "be accomplished at a relatively low cost" so that the government is able to "compile a substantial quantum of information about any person whom the government chooses to track." *Id*. This fact fundamentally alters "the relationship between citizen and government in a way that is inimical to democratic society." *Id*. (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

The unlawful and invasive policies employed by the City of Coral Gables, under the auspices of the Florida Department of Law Enforcement, are likewise inimical to the rights of its citizens to be free from abusive governmental intrusion. Using 18 automatic license plate recognition cameras (and associated software) strategically located across the City, Coral Gables tracks, records, collects, and aggregates the personal and private activities of its citizens and visitors, without any prior suspicion of wrongdoing. It also stockpiles and analyzes this data for at least three *years*. This complete surveillance cannot be countenanced by a free society, and it violates the fundamental rights of every motorist who passes through the "City Beautiful."

II. UNDISPUTED MATERIAL FACTS

On September 28, 2015 Assistant Chief of the Coral Gables Police Department Michael C. Miller sent then-Director of Public Safety, Frank G. Fernandez, a Memorandum entitled "CCTV/ALPR Project Scope." Nelson Gonzalez Dep. 19:16-17, 20:6-12, July 31, 2020; Gonzalez Exhibit 2. The memo proposed the City adopt an automated license plate reader (ALPR) system as a "public safety enhancement tool," "intended to assist police to [] prevent crime." Gonzalez 22:13-14. This proposal was subsequently submitted to the Coral Gables City Council. Gonzalez 25:7-10. According to the City's corporate representative, "the main purpose" "of this system [wa]s to either deter crime or help solve crimes." Maj. Raul Pedroso Dep. 14:25-15:4, Aug. 13, 2020.

The City considered proposals from various ALPR vendors, one from a company called Safeware. Gonzalez 26:7-10; Gonzalez Exhibit 3. In a written proposal to the City on October 21,

2015, Safeware advanced a $1.16 million project involving 18 ALPR cameras in 11 locations. Gonzalez 29:9, 29:17-21, 30:4-6, 33:2; Gonzalez Exhibit 3. The proposed locations formed a perimeter around the City and were selected to encompass the most traffic possible so that the system would provide maximum surveillance potential. Gonzalez 31:22, 32:4, 32:14; Gonzalez Exhibit 3. The proposal also mapped out the cameras' locations. Gonzalez Exhibit 3 at 3.

The City next evaluated proposals for software vendors, and eventually settled on Vigilant Solutions. Gonzalez, 36:9-12; Gonzalez Exhibit 4. The City approved Vigilant Solutions because it was "the only ALPR provider that offers a proven data sharing solution." Gonzalez 36:9-12; Gonzalez Exhibit 4. Vigilant allowed users to share data with other law enforcement agencies and receive images from cooperating jurisdictions. Gonzalez 37:8-10, 38:6-9.

On December 8, 2015, the Coral Gables City Commission adopted Resolution No. 2015-307, authorizing the City to enter into contracts with Safeware and Vigilant Solutions for the purchase, installation and operation of the proposed ALPR system. Gonzalez 39:1; Gonzalez Exhibit 5. The City approved an initial expenditure of $1,314,187.22. Gonzalez Exhibit 5.

At the City Commission hearing prior to adoption of the Resolution, Assistant Police Chief Michael Miller was asked if the ALPR system would be able to constantly monitor the hundreds of thousands of cars that entered and exited the City limits every day, and "sift through these millions of cars that w[ould] be coming through all week." Assistant Chief Miller testified that it would be capable of operating in that fashion. *City of Coral Gables City Commission Meeting: Agenda Item H-1*, at 5 (Dec. 8, 2015). Or, as Assistant City Manager Frank Fernandez put it, the ALPR system would be "surrounding" the entire City. *Id*. at 6. If any vehicle in the system was "wanted for any type of crime" this information would "immediately" be given to police officers. *Id*. at 4. The ALPR system would also allow law enforcement to "go back on this video, go back on the tags," and search collected data, by vehicle tag number or even by reviewing all traffic in an area of the City. *Id*. at 5.

On February 8, 2016, Safeware provided the City with a more detailed proposal for the ALPR system. Gonzalez 45:13, Gonzalez Exhibit 7. As it had before, Safeware proposed that 18

cameras be installed at 11 locations around the city, which would operate 24 hours a day. Gonzalez 46:17, 49:7-9, 53:8-17; Gonzalez Exhibit 7. Safeware referred to the system as a "geo-fence" and explained that each location was strategically chosen because it was a "high traffic" location at a "main point[s] of entry to the City" and at "critical borders of the City." Gonzalez 47:21-48:2, 48:11-15, 50:13-18, 52:8-17; Gonzalez Exhibit 7. The system was designed to capture "whatever comes through" the City and record the license plate of every vehicle that came into camera range. Gonzalez 49:7-13, 50:1-5; Gonzalez Exhibit 7.

The City adopted Safeware's proposal and installed 18 cameras in 11 locations around the City. Gonzalez 53:1-5, 53:14-19, 54:9-11; Gonzalez Exhibit 8. The City also entered into an enterprise services agreement with Safeware that remains in effect. Gonzalez 66:16-19, 71:5-8; Gonzalez Exhibit 9.

Vigilant provided a software interface so that the City could access the ALPR data it gathered from its cameras. Gonzalez 56:1-3, 56:11-15; Gonzalez Exhibit 7 at 91. The interface, called the Law Enforcement Archival and Reporting Network (LEARN), allowed users to conduct both historical and real-time inquiries into the data collected. Gonzalez 56:11-15, 56:20-57:1, 57:10-13; Gonzalez Exhibit 7 at 91-92. The interface allowed a user to search, through a filter, the source of the LPR data, license plate number, time-period, or even "geo-zoning," which "allows the user to actively search using an area of interest with or without a license plate number." Gonzalez 62:15-19, 63:1-3, Gonzalez Exhibit 7 at 91-92.

The results of a LEARN search "include a color overview image of the vehicle, a picture of the license plate, 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." Gonzalez 65:2-11; Gonzalez Exhibit 7 at 93. "The system also provided a feature that resolves the geographic coordinates to a nearest physical address and nearest intersection." Gonzalez 65:12-16; Gonzalez Exhibit 7 at 93.

Coral Gables's license with Vigilant allowed unlimited user access to the system. Gonzalez 74:17-75:4; Gonzalez Exhibit 9. Under the terms of the agreement, Vigilant stored all ALPR data collected by the City on its own servers. Gonzalez 71:13-15; Gonzalez Exhibit 9. The City in turn

set the data retention schedule, which Vigilant agreed to honor. Gonzalez 72:18-73:4; Exhibit 9. At the City's direction, Vigilant currently overwrites ALPR data on a rolling basis 3 years after its collection. Gonzalez 72:18-73:4, 73:5-7. In the City's view, this 3-year period stemmed from guidelines issued by Defendant Florida Department of Law Enforcement (FDLE), which set "the limit" for data retention. Gonzalez 83:14-20. The system has the capacity to set a shorter data retention policy, however. Gonzalez 82:7-11.

As part of its agreement with the City, Vigilant provided a document entitled *Guidelines for Media Responses on Privacy, Data Retention and Policy*. Gonzalez 84:10-12; Gonzalez Exhibit 11. According to this document, "Special interest groups and the media are always looking to sensationalize a story and play on the emotions of the public to help 'sell' their story," and the City should respond to concerns about "privacy issues" by trying to "redirect [the] question." Gonzalez Exhibit 11 at 1. When asked about data retention periods, and "Why keep data that isn't related to a crime," the document recommends responding, "I would hate to tell a father, 'Sorry, we had historical data on your daughter's kidnapper that could have helped us determine some possible locations, but it was deleted last month per agency policy.'" Gonzalez Exhibit 11 at 1-2.

The City allows only registered users to access LEARN. Gonzalez 87:11-14. This includes both information technology staff and police officers, and to date, has included more than 100 individuals. Gonzalez 87:11-14, 93:17, 105:14-17; Gonzalez Exhibit 14. LEARN creates a record of every search conducted and identifies the user. Gonzalez 107:1-7. LEARN also allows the City to audit any query conducted within its data retention period. Gonzalez 111:19-22.

FDLE's Guidelines provide "general limits" for access to ALPR data and allows access by law enforcement "for the tactical enforcement of state statutes." Pedroso 27:25-28:7; Pedroso Exhibit 26. The City in turn, permits access "for conducting ongoing or continuing criminal investigations." Pedroso 28:16-20. Neither requires a warrant, or that police have probable cause, reasonable suspicion or any specific quantum of suspicion. Pedroso 28:21-29:5. The police need only have a "legitimate law enforcement purpose" for LEARN searches. Pedroso 37:7-10.

Typically, searches are conducted in order to "assist[] forensically with an investigation for a detective." Gonzalez 91:15-3, 92:8-15.

The City requires users to identify a reason for every search and requires all searches to be "for law enforcement" or a related, valid purpose. Gonzalez 94:21-22, 95:13-14; Pedroso 37:11-13. However, a user can simply write the search is "for law enforcement purposes," without providing additional information. Gonzalez 97:22-98:6; Pedroso 37:20-25. The system will still display results if a user enters no information in the "purpose" field. Pedroso 37:11-13.

LEARN tallies all queries in a constantly updated list. Gonzalez 137:21-138:2. In December of 2019, the City produced a then-accurate tally of queries, broken down by registered user. Gonzalez 137:15-138:2, 138:6-10; Gonzalez Exhibit 18. At the time of its creation, 12,665 queries had been conducted by City personnel, with one user having queried the system 2,728 times, averaging more than one per day for the life of the system. Gonzalez 139:7-9, 139:10-16, 140:5-8; Gonzalez Exhibit 18. This single user had averaged more than one query per day. Gonzalez 140:5-8.

The LEARN system does not provide personal information related to license plate numbers. Pedroso 26:1-8. However, a separate system, the Driver and Vehicle Information Database (DAVID), which is maintained by the Florida Department of Highway Safety and Motor Vehicles (DHSMV), gives access to motor vehicle records. Pedroso 48:15-49:2. These records include personal information associated with a license plate number, including the name of the registered owner of a vehicle, insurance information, driver's license number and photograph, and, if the DHSMV has such info, the home phone number of the registered motorist. Pedroso 48:21-23, 48:24-49:2, 51:2-12. At one point the system also provided officers with access to a driver's social security number. Pedroso 50:24-51:1.

Thus, Coral Gables police officers can access DAVID to obtain personally identifying information related to LEARN searches. Pedroso 49:3-9. Many Coral Gables police officers have done just that; such joint access is "relatively common" on the police force. Pedroso 49:23-50:4. To access DAVID a police officer need only have a "legitimate law enforcement purpose," and

not probable cause or a warrant. Pedroso 52:12-17. A police officer does not need to articulate a reason for accessing DAVID, and "they don't necessarily have to suspect say, that the motorist is involved in some kind of criminal activity." Pedroso 53:17-19, 53:21-54:1, 56:25-57:3, 57:15-17.

Coral Gables audits use of DAVID by its officers to check for unauthorized uses. Pedroso 58:13-15. In the past five years it has disciplined two employees for misusing the system. Pedroso 60:9-11. Coral Gables does not monitor each use of DAVID, however. Pedroso 60:2-5.

The City also has an agreement with FDLE governing "hotlists." Gonzalez 98:13-17, 99:7-10; Gonzalez Exhibit 13. LEARN automatically searches the City's ALPR images every three hours and runs license plate numbers against a "hot list" of tags that are associated with an "expired tag file, expired license file, and sanctioned driver file." Gonzalez 100:15-22, 101:6-15. The hot list relies on extracts provided by the Florida Crime Information Center and alerts the City when it finds a match with the hot list. Gonzalez 100:15-22, 101:6-15.

LEARN automatically tallies the number of ALPR images the City's system has collected. Gonzalez 112:15-19, 113:8-15; Gonzalez Exhibit 15. As of December 2019, the system had collected 106,053,551 images and had retained 101,074,029 images in its three-year data retention window. Gonzalez 115:20-116:1, 117:2-4, Gonzalez Exhibit 15.

The City has elected to share its ALPR data with other jurisdictions through Vigilant Solutions. Gonzalez 148:4-12, 149:8-14; Gonzalez Exhibit 20. When the City does so it enters a memorandum of understanding (MOU) with the corresponding jurisdiction. Gonzalez 151:15-21. When the City shares its data with other jurisdictions it notes the number of images it is sharing, and as of that date, the other jurisdiction may access the City's files at will. Gonzalez 158:20-159:1, 159:2-5, 161:12-16; Gonzalez Exhibit 23. As of December 2019, Coral Gables had elected to share its ALPR data with 68 other jurisdictions, including the Federal Bureau of Investigation. Gonzalez 151:13-16; Gonzalez Exhibit 20.

The City also elected to receive ALPR data from other jurisdictions. Gonzalez 150: 2-5; Gonzalez Exhibit 20. These, too, required an MOU with the other jurisdiction. Gonzalez 151:17-22, 165:20-166:2. However, the other jurisdictions determine data retention for these images, and

the City may access at will any images shared by the other jurisdictions. Gonzalez 167:2-12, 169:8-12, 170:9-11; Gonzalez Exhibit 25. As of December 2019, the City had access to images from 76 other jurisdictions, including U.S. Customs and Border Protection. Gonzalez 152:15-21, 166:3-6; Gonzalez Exhibit 20.

The City can audit LEARN queries to discover the purpose of searches. Pedroso 40:13-16. It also keeps records in police reports, and other sources, identifying when the ALPR system has been useful for solving crimes. Pedroso 44:16-25, 45:6-10. The City's police representative would "expect" any officer who had used LEARN in making an arrest to note it in his or her reports. Pedroso 42:19-22, 45:17-19, 48:2-9.

The City agreed it was possible to calculate the number of arrests made as a result of its use of the LEARN system. Pedroso 62:17-20. It presented a corporate representative who agreed he was qualified to testify about "[t]he use of any ALPR data collected, received and/or shared by the City using ALPR cameras in any criminal investigation or prosecution by any entity from 2015 to present." Pedroso 10:21-11:6; Pedroso Exhibit 1. Nevertheless, the City was unable to say how many LEARN queries conducted by the City resulted in arrests. Pedroso 62:4-6.

Ultimately, the City produced two undated "progress briefing" reports presenting "select success stories." CG903-942. Specifically, the first briefing discussed a "stolen vehicle" that was detected by a commercial LPR and resulted in "successful recovery." CG908-09. Next, the briefing discussed a vandalism arrest after an LPR camera "put[] the suspect at the crime scene." CG910. The City's ALPR system also automatically alerted after a license plate from a hot list was detected in the City. CG911. Police stopped the vehicle and arrested the driver with contraband. CG912-13. Finally, this briefing discussed the "theft of used cooking oil," where police obtained a license plate number for a suspect's van. CG914. Using the ALPR system, the police "detected [the van] many times" and plotted the van's location within the City. CG914. LEARN provided police with six alerts, each with a time and place, in Coral Gables over a six-day period, and police were able to use this information to place the suspects near the scene of the crime. CG 914-16. Those were the only instances in which the system was "successfully" used to detect criminal activity.

The second briefing discussed a single case related to credit card fraud. CG924. After police found a card "skimmer" at a gas station, surveillance footage showed a suspect's SUV, but the license plate number was illegible. CG925-26. Using the ALPR system, Coral Gables's police searched "several hundred" images from a nearby ALPR camera and found a "possible match." CG929. Then, running the license plate from that possible match, police monitored each instance in which that SUV entered the system. CG935. After obtaining personally identifying information concerning the license plate from DAVID, police went to the registered owner's home and arrested him. CG930, 932, 942.

The City also presented a memorandum commending an officer for stopping a suspected burglar after the ALPR system alerted to a wanted tag number. CG943-44. It appears that this commendation relates to one of the case studies presented in the first progress briefing. CG912-13, 943-44.

On September 12, 2018, the City generated an 80-page report of every image it had collected for a vehicle with Florida license plate BLI0M. Gonzalez 127:2-6; Gonzalez Exhibit 17. Each page depicts an alert with a photograph of the license plate, the vehicle (a Red Ford Explorer), and "detection data" that lists the precise date, time and latitude and longitude of the vehicle. Gonzalez 130:6-9, 131:11-14; Gonzalez Exhibit 17. The report also provides an estimate of the nearest address and intersection. Gonzalez 130:17-21, 131:1-1; Gonzalez Exhibit 17. In some of the photos, a dog's head hanging out the window of the Ford Explorer can be seen. Gonzalez 131:18-22; Gonzalez Exhibit 17.

This report contains a "system error," as it produced an image from Miami Beach, Florida. Gonzalez 136:4-7. The result of the query should only have displayed images from cameras inside Coral Gables's city limits. Gonzalez 133:14-20. However, the report included a vehicle detection from April 7, 2018, which lists the "nearest address" as 400 W. 42nd St. Miami Beach, FL, 33140. Gonzalez 134:18-135:3; Gonzalez Exhibit 17 at 54. It also lists latitude and longitude for Miami Beach; rather than an estimate, latitude and longitude coordinates are "accurate." Gonzalez 131:6-

10; Gonzalez Exhibit 17 at 54. The image, inexplicably, came from a source "not in Coral Gables's system." Gonzalez 135:5-11; Gonzalez Exhibit 17 at 54.

On January 10, 2020, the City generated another report for Florida license plate BLI0M. Gonzalez 119:4-8; 120:14-29, 121:2-5; Gonzalez Exhibit 16. This report contained the earlier images, as well as those recorded after the first report's creation. Gonzalez 129:7-13. The 2020 report listed 393 records of images taken of the Explorer, including date, time and the camera that captured the image. Gonzalez 121:13-18; Gonzalez Exhibit 16. While the report did not list address information, as with the 2018 report, that information was available to a user. Gonzalez 123:3-9.

The 2020 report established that on a number of days, multiple images of the Explorer were taken. For instance, on March 5, 2019, the system captured the vehicle at 800 Ferdinand St. at 7:29 a.m., 1501 Coral Way at 9:16 a.m. and then 928 Bird Rd. at 12:49 p.m. Gonzalez Exhibit 16 at 12. On June 6, 2019, the system recorded five images of the Explorer, between 6:42 a.m. and 2:40 p.m. Gonzalez Exhibit 16 at 8. On June 8, 2019, the system recorded four images of the Explorer between 12:47 p.m. and 10:06 p.m. Gonzalez Exhibit 16 at 7. And on June 20, 2019, the system noted the Explorer's location six times between 8:18 a.m. and 7:34 p.m. Gonzalez Exhibit 16 at 5-6. The system also recorded the Explorer's movements across the City; for instance, on July 4, 2019 the Explorer was logged at 527 S. Dixie Hwy at 5:34 a.m. and then at the University of Miami at 5:57 a.m. Gonzalez Exhibit 16 at 5.

Mr. Mas is a self-employed marketing consultant with degrees from Georgetown University and Harvard Business School. Raul Mas Canosa Dep. 7:16-21, Mar. 4, 2021. He has lived in Coral Gables continuously since 1987 and resides there with his wife, Ana Maria Permuy Mas. Mas 8-19-22, 9:6. He is a law-abiding person and has no criminal record. Mas 17:8-15.

Mr. Mas drives a vehicle with Florida license plate number BLI0M. Before December 2020, he drove a Red Ford Explorer, which was registered in his wife's name, with that license number. Mas 9:23-10:4, 10:17-20, 11:10-12. Mr. Mas was listed as a driver on the Explorer's insurance, and, in his estimation, was the driver of the Explorer 99.9% of the time. Mas 10:21-23,

13:8-12, 20:13-14, 44:16-18. It was "exceptionally rare," that anyone other than Mr. Mas drove the Explorer. Mas 20:13-14.

Mr. Mas was the driver in the images of the Red Ford Explorer in the LEARN report generated for BLI0M. Mas 44:16-18; Mas Exhibit 2. Mr. Mas also identified his dog in some of the images of his car. Mas 45:16.

Mr. Mas considers the City's ALPR system an invasion of his privacy. Mas 42:14-17. In describing his concerns, he said:

> 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.

Mas 42:20-43:8.

III. DISCUSSION

Pursuant to Florida Rule of Civil Procedure 1.510, a court may grant summary judgment for a movant "if the pleadings and summary judgment evidence on file show that there is no genuine dispute as to any material fact and that the moving party is entitled to a judgment as a matter of law." This standard adopts the "summary judgment standard … of the federal courts[.]" *In re Amends. to Fla. Rule of Civ. Proc. 1.510*, 309 So. 3d 192 (Fla. 2020).

Under this standard, "[e]vidence is viewed in a light most favorable to the nonmoving party[.]" *Beal v. Paramount Pictures Corp.*, 20 F.3d 454, 458–59 (11th Cir. 1994). "[T]his, however, does not mean that [a court is] constrained to accept all the nonmovant's factual characterizations and legal arguments. If no reasonable jury could return a verdict in favor of the nonmoving party, there is no genuine issue of material fact and summary judgment will be granted." *Id*. (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)).

A. The City Has Violated Mr. Mas's Fourth Amendment Rights Because It Has Invaded His Protected Privacy Interests

1. The Fourth Amendment Forbids Monitoring a Person's Public Movements over Time Without a Warrant

The Fourth Amendment to the United States Constitution prohibits "unreasonable searches and seizures," and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The "basic purpose of this Amendment," which is applicable to the states, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528 (1967). 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 that private sphere generally qualifies as a search and requires a warrant supported by probable cause. *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 when the Fourth Amendment was adopted.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2213-14 (2018) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)). And the Court has stressed the need to keep "Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* (internal citations and quotation marks omitted). After all, "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Id.* (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

ALPR technology presents one such innovation in surveillance technology that could not have been anticipated when the Fourth Amendment was adopted. However, a comprehensive data-collection program using ALPR technology such as the one at issue here intrudes into privacy

interests that the Fourth Amendment was designed to protect. Moreover, because the City's system does not incorporate the Amendment's warrant requirement, it fails the constitutional test of reasonableness.

Traditionally, the Fourth Amendment has permitted a single, but suspicionless, view of a license plate number in public by a member of law enforcement, because it is not considered an invasion into any private space. *See, e.g.*, *United States v. Ellison*, 462 F.3d 557, 561 (6th Cir. 2006). Following *New York v. Class*, 475 U.S. 106 (1986), a case which held that a vehicle owner has no "reasonable expectation of privacy" in a VIN number "in plain view from the exterior of the automobile," courts have concluded that "this reasoning extends to a legally-required identifier located *outside* the vehicle." *Ellison*, 462 F.3d at 561.

But courts have rightly distinguished that scenario from one in which law enforcement collects such data over a period of time. As Sixth Circuit Judge Karen Nelson Moore has noted, whether law enforcement 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 separate question. *Id.* at 567 (Moore, J., dissenting). Relatedly, the *scope* of license-plate data retention and searches is usually much broader than the single inspection at issue in *Class*. *Id.*

Judge Moore's concerns have since been termed the "aggregation problem." 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 and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1185 (2002)). At some point, "when government officials search—or query—aggregated information, they can learn a great deal more about the subject of the query than they could have done using any individual piece of data alone." *Id.* at 591. This creates a much different constitutional question than the one decided by *Class*. *Id.*

In *United States v. Jones*, 565 U.S. 400, 402 (2012), the Court took up the aggregation problem by asking if a motorist had a reasonable expectation of privacy in his vehicle's movements over a 28-day period. Police had attached a global-positioning system (GPS) tracking device to the underside of Jones's car without first obtaining a warrant, and had monitored his car's movements to within 50 to 100 feet for 28 days. *Id.* at 403. Ultimately, the Court invalidated the use of the tracking device because it constituted a physical trespass and declined to rule on the "vexing problems" associated with the aggregation problem. *Id.* at 412-13.

Yet *five members* of the Court wrote concurring opinions concluding that Jones had a reasonable expectation of privacy in his vehicle's movements over time. Justice Sotomayor wrote that because such a "precise, comprehensive record of a person's public movements" exposes "a wealth of detail about [that person's] familial, political, professional, religious, and sexual associations," it violates a reasonable expectation of privacy and should therefore be considered a search. *Id*. at 415. "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, "[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.

In *Carpenter v. United States*, 138 S.Ct. 2206, 2217 (2018), the Court expressly held what had been recognized implicitly by the various *Jones* concurrences—"an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through" digital surveillance. *Carpenter* explicitly adopted the view that because "monitoring of a vehicle tracks "every movement" a person makes in that vehicle, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"—regardless of whether those

movements were disclosed to the public at large. *Id*. at 2215 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)). Indeed, even if such information is voluntarily disclosed to third parties, and even if it is only able to pinpoint a person's "location within 50 meters," the Court held that 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).

Florida courts correctly anticipated the *Carpenter* decision and have consistently protected individuals from the indiscriminate collection and aggregation of public information. In *Tracey v. State*, 152 So.3d 504, 507-08 (Fla. 2014), the Florida Supreme Court held that law enforcement was required to obtain a search warrant before collecting cell-site location information from the defendant's cell phone over the course of a *single day*. Relying on Justice Sotomayor's concurrence in *Jones*, the Court recognized that "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 (citing *Jones*, 132 S.Ct. at 956 (Sotomayor, J., concurring)). The Court further recognized that "such monitoring" can now "be accomplished at a relatively low cost" so that the government is able 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.* (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)). Thus, the Court specifically adopted what it called the "mosaic" theory of the Fourth Amendment, which held "that discrete acts of surveillance by law enforcement may be lawful in isolation, but may otherwise infringe on reasonable expectations of privacy in the aggregate." *Id.* at 520.

Recent decisions of the Fourth District Court of Appeal, which are binding on this Court,[1] illustrate the significant protections established by this "mosaic" theory. In *Ferrari v. State*, 260 So.3d 295, 304, 306 (Fla. 4th Dist. Ct. App. 2018), law enforcement obtained historical cell-site location information related to two cell phones associated with a defendant for a *single night*. This information revealed only that, when "imported onto a mapping program to show the location of the towers that received the phone's data at certain times," "the phones … did not move location" from one near the victim "from 6:40 p.m. to 9:19 p.m." *Id.* at 304. Despite only recovering this small amount of raw information, the Court held, pursuant to *Carpenter*, that "the government's acquisition of such data constitutes a search which requires a warrant supported by probable cause." *Id.* at 305.

Similarly, in *State v. Sylvestre*, 254 So.3d 986, 990 (Fla. 4th Dist. Ct. App. 2018), the Court established the firm constitutional limits imposed on the aggregation of public data. The Court 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 state was forbidden from using technology that could pinpoint the location of a single cell phone owned by defendant "for several concurrent nights" without a warrant. *Id.* at 988. Importantly, the Court extended the analysis to technology that was not implicated in *Carpenter*—real-time cell-site monitoring and "stingray" devices, which mimic cell towers for the purpose of locating a cell phone. *Id.*

Finally, in *State v. Martin*, 287 So.3d 645, 648 (Fla. 4th Dist. Ct. App. 2019), 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. Thisruling was because mobile tracking of a person's movements, particularly when "law enforcement [can] track an individual's location in real time

[1] *See Pardo v. State*, 596 So.2d 665, 666 (Fla. 1992) ("in the absence of interdistrict conflict, district court decisions bind all Florida trial courts").

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).

The Massachusetts Supreme Judicial Court has combined these principles and held that, in circumstances such as those presented here, 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). McCarthy's vehicle had been captured by an ALPR system on two bridges that connected to Cape Cod over a three-month period. *Id*. at 1097. The data showed only that McCarthy had crossed onto the Cape on those dates, but law enforcement used this information to connect him to alleged drug offenses, and McCarthy sought to suppress the ALPR evidence. *Id*.

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*. 1102 (citation omitted).

Applying these principles to ALPRs, the court held: "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. The court also explained, "In 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*.

The court further explicated three features of ALPRs that are relevant to assessing whether a constitutional violation occurred. First, a court should consider the extent of the ALPR system's reach—"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, a court should consider 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, a court should consider 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." *Id*. at 1105.

Ultimately, the court denied suppression, but only because of the limited number of cameras and data collection in the record before it. *McCarthy*, 142 N.E.3d at 1105. At issue were "four cameras placed at two fixed locations on the ends of the Bourne and Sagamore bridges," which were monitored only for three months. *Id*. at 1097, 1105. Thus, the court said, "On this record … we need not, and indeed cannot, determine how pervasive a system of ALPRs would have to be to invade a reasonable expectation of privacy." *Id*. at 1105.

2. The City's ALPR System Intrudes into Protected Areas of Privacy by Collecting 3 Years of Location Data at Major Intersections in Coral Gables

The City's ALPR system violates the Fourth Amendment because it invades Mr. Mas's reasonable expectation of privacy in his movements over time. The City's ALPR system allows "an overly pervasive police presence" in Coral Gables that gives police full access to Mr. Mas's private movements. *See id*. at 1102. It would have been unthinkable to the Founders, not merely as a matter of technology, but as a matter of *intrusion*.

First, the sheer number of cameras, as well as the "historic location data from [the] ALPR system" invades Mr. Mas's "reasonable expectation of privacy and [] constitute[s] a search for constitutional purposes." *See id*. at 1104. The City has 18 cameras in 11 locations that operate continuously. Gonzalez 53:105, 14-19, 54:9-11; Gonzalez Exhibit 8. And they are spread out over a City with a population of just under 50,000 and a land area of less than 13 square miles. *See* U.S. Census Bureau, Coral Gables City, Florida (last visited May 21, 2021) https://www.census.gov/quickfacts/fact/table/coralgablescityflorida/PST040219#PST040219.

The cameras are designed to capture an image of every vehicle that passes into view, no matter how heavy the traffic. Gonzalez 49:7-13, 50:1-5; Gonzalez Exhibit 7. And each image logs the time, date, specific location and license number and *image* of the vehicle. Gonzalez 65:2-11; Gonzalez Exhibit 7 at 93. The cameras are so pervasive in their data collection that as of December 2019, the system had collected 106,053,551 images. Gonzalez 115:20-116:1, 117:2-4, Gonzalez Exhibit 15.

More concerning than the raw number of cameras and images gathered, the City's ALPR system is designed to intrude into protected areas. Each of the camera locations was selected to maximize the odds of collecting data, as well as to create a barrier around Coral Gables, as the cameras are spread out to have nearly-total coverage of Coral Gables's minuscule footprint. *See* Gonzalez Exhibit 8. Safeware referred to the system as a "geo-fence" and explained that each location was strategically chosen because they were "high traffic" locations that were "main point[s] of entry to the City" as well as "critical borders of the City." Gonzalez 47:21-48:2, 48:11-15, 50:13-18, 52:8-17; Gonzalez Exhibit 7. During his testimony before the City Council, Assistant City Manager Fernandez put this in explicit terms, explaining that the system was meant to track ingress and egress into the City's borders because it would "surround[]" the City. *City of Coral Gables City Commission Meeting: Agenda Item H-1*, at 4 (Dec. 8, 2015).

The invasiveness of the system is not merely hypothetical. The reports capturing Mr. Mas's movements demonstrate the amount and type of information that the City's system can collect. The police collected 393 unique images of Mr. Mas in the City between October 13, 2017 and January 5, 2020. Gonzalez Exhibit 16. Each of these detections captured an image of his SUV, and recorded the precise date, time and location. Gonzalez 123:3-9; Gonzalez Exhibit 16. This system allows the police to create a broad picture of Mr. Mas's whereabouts, within the city limits, for *years*.

The police can even track 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. Gonzalez Exhibit 16 at 5-6. 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. Gonzalez Exhibit 16 at 5. Police even know that Mr. Mas tends to travel with his dog in the passenger seat. Gonzalez 131:18-22; Gonzalez Exhibit 17; Mas 45:16. As Mr. Mas said, "[T]he 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." Mas 42:20-43:8.

How the police have used the system also proves the pervasiveness of the coverage. For instance, after touting its success in making an arrest for the "theft of used cooking oil," the police department explained that they were able to "detect [a van] many times" and plot the van's location within the City over a six-day period using the ALPR system. CG914-16. The police were even able to indiscriminately search all traffic near the scene of a crime to narrow down a suspect, which they then tied to the location of an offense. CG929, 935. The police can and do use the system to track innocent motorists as they move about the City.

Even the International Association of Chiefs of Police (IACP) has recognized the danger presented here. "Aggregation," of ALPR data "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." FDLE 21.

Compared with the intrusions discussed in *Carpenter*, *Tracey*, *Ferrari*, *Sylvestre* and *McCarthy*, there is little doubt that the City's ALPR system constitutes an invasion of Mr. Mas's protected privacy rights. In *Tracey*, the state using "real time cell site location data to track [the defendant] on public streets" over the course of a single night constituted a Fourth Amendment

Violation. 152 So. 3d at 508. And in *Ferrari*, 260 So.3d at 304, the state's intrusion involved nothing more than showing the defendant "did not move location" during a single evening, while in *Sylvestre*, 254 So.3d at 988, the intrusion was limited to pinpointing a defendant's location in a house over several nights. And, in *Carpenter*, the intrusion consisted of the government's mere approximation of the defendant's public location "within 50 meters" over the course of a week. *See* 138 S.Ct. at 2219. If a state invades a protected privacy interest by tracking a person's public movements on a public road for an evening, as in *Tracey*, pinpointing a person's *single* location, as in *Ferrari* or *Sylvestre*, or merely approximating his public location for a short period of time, as in *Carpenter*, then unquestionably the City's conduct here—which involved pinpointing Mr. Mas's location nearly 400 times—did so as well.

The comparison with *McCarthy* is equally stark. In that case "four cameras placed at two fixed locations on the ends of the Bourne and Sagamore bridges" did not create a sufficient picture of McCarthy's movements to constitute a search for Fourth Amendment purposes. *McCarthy*, 142 N.E.3d at 1097, 1105. But, as discussed, the Court was concerned enough to set out markers of impermissible data-gathering. Coral Gables's comprehensive network of cameras gathers much more information than present in *McCarthy*.

The City's three-year retention period compounds the constitutional intrusion. If the "one-year retention period indicated in the [Massachusetts] retention policy certainly is long enough to warrant constitutional protection," then this Court should be deeply concerned about the system at issue here. *See id.* at 1104. In *Carpenter*, the Court declined to "decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be," but had no trouble saying that monitoring a person's location for "seven days" "constitutes a Fourth Amendment search." 138 S.Ct. at 2217, n. 3. *Ferrari*, *Sylvestre* and *Tracey* went further, though, with *Sylvestre* determining that monitoring a person's location for "several concurrent nights" was a search, 254 So.3d at 988, while *Ferrari*, 260 So.3d at 304, and *Tracey*, 152 So.3d at 508, held that *a single night* of monitoring constituted a search. Yet again, this is a concern that was raised by IACP, which noted

that "retaining certain types of information indefinitely 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." FDLE 41. Although courts have not definitely established a temporal limit, there is no question that the City's *three years* of location monitoring constitutes a search for constitutional purposes.

Together, these features of the City's ALPR system establish that the police are conducting searches of Mr. Mas for Fourth Amendment purposes.

3. The City Unconstitutionally Provides Suspicionless Access to Its ALPR Data

Not only does the data gathering itself present constitutional concerns, but the method of sharing that information with police violates the Fourth Amendment's warrant requirement. *See Carpenter*, 138 S.Ct. at 2220-21; *Tracey*, 152 So.3d at 520. The police need only have a "legitimate law enforcement purpose" to conduct LEARN searches. Pedroso 37:7-10. They do not need a warrant, or even a specific quantum of suspicion such as probable cause or reasonable suspicion. Pedroso 28:21-29:5. Relatedly, the police can access personally identifying information related to LEARN searches using the DAVID system. Pedroso 49:3-9. And police officers do not need to articulate a reason why they are accessing DAVID, and "they don't necessarily have to suspect say, that the motorist is involved in some kind of criminal activity." Pedroso 53:17-19, 53:21-54:1, 56:25-57:3, 57:15-17. Police can, therefore, conduct suspicionless searches through the ALPR system, and then gather personal information about a motorist without any judicial oversight. Thus, law enforcement has unlimited access to Mr. Mas's protected information, even though it has never suspected him of wrongdoing. Certainly, this violates the Constitution's warrant requirement.

4. The ALPR System Is Not Anonymized

Defendants were alerted long ago that ALPR systems such as the one used here implicate serious "privacy concerns," particularly those concerning the "[a]ggregation of LPR DATA." *See* FDLE 21. Yet Defendants have continuously dismissed those issues because "a license plate number identifies a specific vehicle, not a specific person. Although a license plate number may

be linked or otherwise associated with an identifiable person, this potential can only be realized through a distinct, separate step (*e.g.*, an inquiry to a Secretary of State or Department of Motor Vehicles data system)." FDLE 233. Defendants' justification makes no constitutional difference.

The separation between ALPR data and personally identifiable information solves *none* of the constitutional problems presented here. As noted above, while LEARN does not tie a license plate number to an individual, the DAVID system does. Pedroso 48:15-49:2. A user of DAVID can readily access the name of the registered owner of a vehicle, insurance information, a driver's license number and photograph, and, if the DHSMV has such info, the home phone number of the registered motorist. Pedroso 48:21-23, 48:24-49:2, 51:2-12. At one point the system also provided officers with access to a driver's social security number. Pedroso 50:24-51:1. Many Coral Gables police officers have access to both DAVID and LEARN, and, using both systems can easily discover personally identifying information related to LEARN searches. Pedroso 49:3-9, 49:23-50:4. And, as discussed, neither search requires a particularized showing of suspicion. Pedroso 28:21-29:5, 53:17-19, 53:21-54:1, 56:25-57:3, 57:15-17.

Mr. Mas's experiences demonstrate the speciousness of Defendants' justification. In order to obtain a copy of his own ALPR detection report, Mr. Mas had to waive privacy protections under Florida law and present the City with a copy of his vehicle registration. *See* Mas Exhibit 1. If the City did not consider this information private, it seems bizarre that it would insist on such a waiver. And even though Mr. Mas's Ford Explorer was registered in his wife's name, anyone running his tag through DAVID would be able to see that he was a registered driver for insurance purposes. *See* Pedroso 51:6-12 (DAVID provides access to insurance information); Mas 13:8-12 (Mr. Mas is a listed driver on the Explorer's insurance). They would then be able to find his home address, phone number, and potentially even his social security number. *See* Pedroso 48:21-23, 48:24-49:2, 51:2-12.

B. The City Has Violated Mr. Mas's Right of Privacy Under Article I, Section 23 of the Florida Constitution

Article I, Section 23 of the Florida State Constitution protects the "right of privacy" and provides, "Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein."

This provision was passed in recognition 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). But it was also a response to the Fourth Amendment's limitations, and the notion that "the Supreme Court has given much of the responsibility to the individual state" "[i]n formulating privacy interests." *Id.* at 547.

"The 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. 2nd Dist. Ct. App. 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*.

In applying this test to law enforcement data collection, the Florida Supreme Court has cautioned that, to justify the use of surveillance, law enforcement must demonstrate "a clear connection between [] illegal activity and the person whose privacy would be invaded." *Shaktman v. State*, 553 So.2d 148, 152 (Fla. 1989). Furthermore, law enforcement must show that the surveillance "was the least intrusive means available to accomplish its goal," which generally requires demonstrating that the state has employed significant "procedural safeguards" before resorting to surveillance. *Id*.

Florida Courts have not hesitated to apply Section 23 to a host of private subjects. 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. 3rd Dist. Ct. App. 2017). Similarly, financial records have been deemed protected by Section 23, *Inglis v. Casselberry*, 200 So.3d 206, 212 (Fla. 2nd Dist. Ct. App. 2016), as have an individual's social security number, *Thomas*, 882 So. 2d at 1043, and the names and addresses of blood donors. *Rasmussen*, 500 So. 2d at 536. In short, Section 23 prohibits indiscriminate collection and use of "information relating to all facets of an individual's life." *Id.*

The City's ALPR system violates Section 23 because its collection and dissemination of three years' worth of license plate 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* his or her privacy protections. ALPR data is *exempt* from Florida's public records law, meaning that it is protected from disclosure by state actors. *See* Fla. Stat. §§ 316.0777. That is why Mr. Mas had to waive his privacy interests in order to access his *own* records. *See* Mas Exhibit 1. Plainly, this information is considered private, yet the City not only collects it indiscriminately, but *shares it* indiscriminately with 68 other jurisdictions, including the Federal Bureau of Investigation. Gonzalez 151:13-16; Gonzalez Exhibit 20.

Moreover, as discussed above, the aggregated data that the police collect from the City's ALPR system seriously intrudes into the privacy of its residents. The system has collected more

than 106 *million* images, which it has stored and aggregated, so that police can track the movements of innocent people through the City for a period of three years and search these images at will. *See* Gonzalez 115:20-116:1, 117:2-4, Pedroso 28:21-29:5; Gonzalez Exhibit 15. Mr. Mas is one of those innocent people. Gonzalez 44:16-18; Gonzalez Exhibit 2. The City also shares these images indiscriminately with other law enforcement agencies. Gonzalez 151:13-16; Gonzalez Exhibit 20. If Section 23 applies to information such as 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 privacy rights that the Florida Constitution protects.

The City cannot demonstrate a narrowly tailored justification for this system. It is the City's 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." *Rasmussen*, 500 So. 2d at 536. According to the City's corporate representative, "the main purpose" "of this system [wa]s to either deter crime or help solve crimes." Pedroso 14:25-15:4. But the scattered successes the City has promoted pale in comparison to the massive privacy intrusions it has perpetrated. The City conceded that it keeps records of occasions on which the police have used the ALPR system, and it has the ability to generate the number of arrests made as a result of its use of the LEARN system. Pedroso 62:17-20. Yet the City produced only two undated "progress briefing" reports presenting "select success stories" from the ALPR system, as evidence of its efficacy. CG903-942. These briefings discuss *five* cases that resulted in charges, although it is unclear whether they resulted in convictions. And the cases involved a "stolen vehicle," vandalism, "theft of used cooking oil," burglary and credit card fraud—hardly crimes like kidnapping or murder that Vigilant Solutions has advocated using to stoke fear in the public. *See* CG903-942; Gonzalez Exhibit 11 (media guidelines suggest that when asked "Why keep data that isn't related to a crime," police should respond, "I would hate to tell a father, 'Sorry, we had historical data on your daughter's kidnapper that could have helped us determine some possible locations, but it was deleted last month per agency policy.'"). But even accepting these arrests as successes, they represent *five* instances of

success after collecting more than 106,053,551 images. *See* Gonzalez 115:20-116:1, 117:2-4, Gonzalez Exhibit 15. That per-image success rate is so infinitesimally small that it beggars belief that the City would tout the system as anything other than a total failure. Thus, the system has no "clear connection" between any illegal activity and invading the privacy of the millions of affected motorists. *See Shaktman*, 553 So.2d at 152. And the system falls well short of the least intrusive means available. Indeed, Coral Gables is "boiling the ocean" to solve a handful of crimes.

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. But because the City has not tailored the system in any meaningful way, it violates Section 23. *See id*.

IV. CONCLUSION

The City's ALPR system unlawfully aggregates data about Mr. Mas's movements over time, and impermissibly shares that data with law enforcement without any particularized suspicion. The City has therefore routinely violated limits set out in the Fourth Amendment and Article I, Section 23. This Court must declare the City's actions unlawful and enjoin further violations by the City.

Dated: June 2, 2021

Respectfully,

/s/ Caleb Kruckenberg
Caleb Kruckenberg
Litigation Counsel
New Civil Liberties Alliance
1225 19th St. NW, Suite 450
Washington, DC 20036
caleb.kruckenberg@ncla.legal
(202) 869-5210
Pro Hac Vice No. 1011501
Counsel for Plaintiff

CERTIFICATE OF SERVICE

I CERTIFY that on this day, June 2, 2021, undersigned counsel has electronically filed the foregoing document with the Clerk of the Court using the Florida Courts E-Portal. Pursuant to Fla. R. Jud. Adm. 2.516(b), I also certify that the foregoing document has been furnished to all counsel of record and interested parties identified on the attached Service List via transmission of Notices of Service of Court Document generated by the E-Portal, or in the manner listed on the attached service list.

/s/ Caleb Kruckenberg
Caleb Kruckenberg

SERVICE LIST

Abigail G. Corbett
Veronica L. de Zayas
Laura Farinas
Stearns Weaver Miller Weissler
Alhadeff & Sitterson, P.A.
150 West Flagler Street
Suite 2200
Miami, Florida 33130
acorbett@stearnsweaver.com
vdezayas@stearnsweaver.com
lfarinas@stearnsweaver.com

and

Frank A. Shepherd
Jack R. Reiter
GrayRobinson, P.A.
333 S.E. Second Avenue, Suite 3200
Miami, Florida 33131
frank.shepherd@gray-robinson.com
jack.reiter@gray-robinson.com

Counsel for Defendant City of Coral Gables

Barbara Junge
Office of the Attorney General
110 S.E. 6th Street, 10th Floor
Fort Lauderdale, Florida 33301
barbara.junge@myfloridalegal.com
Counsel for Defendants Florida Department of Law Enforcement and Commissioner Swearingen