UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	22 Cr. 178 (NSR)
– v. –	:	
DAVID ZAYAS	:	

DAVID ZAYAS'S MOTION TO SUPPRESS ALL EVIDENCE STEMMING FROM THE WARRANTLESS SEARCH OF YEARS OF HIS LOCATION DATA

Benjamin Gold
Assistant Federal Defender
Federal Defenders of New York
81 Main Street, Suite 300
White Plains, New York 10601

Sidney Thaxter
Senior Litigator, 4th Amendment Center
NACDL
1660 L. St. NW, 12th Floor
Washington DC 20036

Attorneys for DAVID ZAYAS

To: Honorable Nelson S. Román
United States District Court Judge
Southern District of New York
300 Quarropas Street
White Plains, New York 10601

Damian Williams
United States Attorney
Southern District of New York
300 Quarropas Street
White Plains, New York 10601
Timothy Josiah Pertz
Assistant United States Attorney

NOTICE OF MOTION

David Zayas (herein "Mr. Zayas") moves this Court for an order suppressing all evidence stemming from the warrantless search of years of Mr. Zayas's location information.

INTRODUCTION

This case began years ago with law enforcement's collection of troves of data memorializing the precise travels of virtually anyone who drives the roads of Westchester County. As conceded by the Government, Mr. Zayas's travels, and those of countless others, were tracked, stored, and preserved for law enforcement to peruse as they saw fit. Law enforcement then choose to conduct an unprecedented search of over 1.6 billion of these location and travel records. This law enforcement search was conducted without judicial supervision, without a suspect, and unconnected to any particular crime. It was a digital dragnet, the results of which caused the government to open an investigation into Mr. Zayas, flag his car for interdiction, and delay his traffic stop while police interrogated him and used a canine to perform a warrantless search of Mr. Zayas and his automobile. Mr. Zayas has a privacy interest in his historical location information and the warrantless collection and search of years of his travels violates the Fourth Amendment. As a result, all evidence obtained from law enforcement's utilization of this unprecedent tracking system, including items recovered following the prolonged seizure and subsequent search of Mr. Zayas's vehicle, must be suppressed.

STATEMENT OF FACTS

In this case Sgt. Kyle McCarrick and other officers in the Westchester Real Time Crime Center (hereinafter "RTC") searched the location history of Mr. Zayas and hundreds of millions

of other people in order to identify driving patterns they deemed, "consistent with interstate narcotics trafficking." *See Opposition to Motion to Dismiss*, at 1-2. They conducted these searches without any judicial oversight and without any reason to believe a specific crime had occurred—let alone any reason to suspect Mr. Zayas of a committing a crime.

This search was conducted using a surveillance system built on automatic license plate readers (hereinafter "ALPR"). *Id.* ALPR systems combine high-speed cameras with analytic image software to collect the plate numbers, images, date, time and GPS location of every vehicle as it passes by a camera.[1] The collection of this ALPR data is indiscriminate by design and captures images (and/or video) of every passing vehicle. *See* Roberts & Casanova*, supra note 1.* Typically, each vehicle's plate number is then compared against "hot lists" of people who law-enforcement agencies have flagged for arrest or investigation. *See id.* The plate numbers (and associated data) are also added to large databases regardless of whether they matched any plates from the "hot lists." *See id.* In fact, only a tiny fraction of the location data collected is linked to any criminal activity.[2] What happens to those scans once they are entered into a database—including the amount of time they are retained for and with whom they are shared—depends on the policies of the department maintaining the ALPR surveillance network. *See id.* Thus, surveillance networks based on ALPR technology can track people's movements retroactively with a simple search query. The breadth and detail of that search is limited only by the number of cameras inputting information into the database and the length of time the data is retained.

---

[1] David J. Roberts & Meghann Casanova, AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS: POLICY AND OPERATIONAL GUIDANCE FOR LAW ENFORCEMENT, (Sept. 2012), https://www.ojp.gov/pdffiles1/nij/grants/239604.pdf.

[2] *See* George Joseph, *What Are License-Plate Readers Good For*?, BLOOMBERG: CityLab (Aug. 5, 2016), http://www.citylab.com/crime/2016/08/what-are-license-plate-readersgood-for/492083/; Dave Maass & Beryl Lipton, *What We Learned*, MuckRock (Nov. 15, 2018), https://www.muckrock.com/news/archives/2018/nov/15/alpr-what-we-learned/.

The Westchester RTC started in 2017 and operates one of the largest ALPR databases in the country—currently scanning and archiving, approximately ***16.2 million plates per week***. *See RTC FOIL Response*, § 3(B) (Exhibit A).[3] The expansive surveillance network includes 480 ALPR cameras—434 stationary systems and 46 mobile systems. *Id.* at § 3(C). Its cameras also record video footage, GPS coordinates, and utilize artificial intelligence to track and record the make, model, and color of the vehicles in addition to the plate number.[4] The government has refused to provide the location of the fixed cameras but has disclosed that they "change frequently." *See Government Discovery Response* 12/21/22, P. 2 (Exhibit B). The database of location data collected by these cameras currently contains two years' worth of scans, or over ***1.6 billion images***[5] of license plates from ***hundreds of millions of vehicles*** belonging to Westchester County citizens and anyone else who traveled through the area regardless of any connection to a crime. *RTC FOIL Response*, § 4(A).[6] The scope of this surveillance network is likely even larger than reported as the RTC participates in data-sharing with other local departments and has access to a national database containing an unknown number of records.[7]

ALPR surveillance networks have several common law-enforcement uses. First, the police can input the plate numbers of stolen vehicles, wanted persons, or missing persons into a

[3] *See also, RTC: Westchester County, NY,* MOBOTIX https://www.mobotix.com/en/lpr-westchester-county-ny (last visited March 10, 2023).
[4] *Id.*
[5] The number estimated by RTC was 1,664,000,000. However, that appears to be an error based on rounding down the weekly numbers to 16 million. The actual number of scans in the database using their statistic of 16.2 million weekly scans is 1,684,800,000.
[6] The exact number of unique plate scans is unknown. However, in 2019 (the most recent year available) Westchester had an average daily traffic volume on monitored roads of 20,604,383 vehicles. *See* New York Bureau of Transportation website: https://data.ny.gov/d/6amx-2pbv/visualization (must utilize the visualization tool to get this data) (last visited March 10, 2023). This is a weekly total of 144,230,681. Dividing the 16.2 million plate scans by that weekly total equals 0.11 or 11%. Eleven of 1,684,800,000 is 185,328,000 unique scans.
[7] RTC is also a part of the Rekor Public Safety Network ("RPSN") which shares ALPR data across every law enforcement agency enrolled in the network. *Rekor Systems Launches Public Safety Network*, BLOOMBERG: BUSINESS (Aug. 21, 2019) https://www.bloomberg.com/press-releases/2019-08-21/rekor-systems-launches-public-safety-network.

"hotlist" that will alert police when that vehicle passes an ALPR camera. *See, e.g., United States v. Thomas*, 997 F.3d 603 (5th Cir. 2021), *cert. denied*, 142 S. Ct. 828 (2022) (officers were informed that a vehicle stolen in an aggravated robbery had been identified in the area by an ALPR). Second, an ALPR database may be queried to identify vehicles that passed by a specific location in order to identify possible suspects or witnesses. *See, e.g., United States v. McLeod*, 2022 WL 2763574, at *2 (D.N.J. July 15, 2022). Third, they may be used to track the locations of known suspects retroactively or in real time. None of these uses resemble the way the ALPR surveillance network was leveraged to surveil the public in this case.

In this case Sgt. McCarrick, and other officers at the RTC—without any reason to suspect any individual, and without connection to any particular criminal investigation—searched the RTC's massive location database to identify travel patterns they believed to be "consistent with interstate narcotics trafficking." *See Opposition to Motion to Dismiss*, at 1. The exact terms of this search is unknown to Mr. Zayas at this time.[8] However, it was conducted without any judicial oversight or any guidance from internal rules or directives of the RTC.[9] Furthermore, the

[8] Defense counsel will file a separate motion to compel the Interdiction Analysis report pursuant to F.R.C.P. 16(a)(1)(E). The software platform running the ALPR network for RTC is called Rekor Scout. Based on the government's description of the query this was an "Interdiction Analysis" performed using the "Analytic Report" function of the software. On November 10, 2022, defense counsel filed a demand for "Any and all 'Analytic Reports' or other reports resulting in the identification of or related to the 2020 gray Chevrolet Equinox bearing the Massachusetts license plate 3CD192, or Mr. Zayas." The government in their response asserted that "Nor does WCPD maintain a separate 'Analytic Report' resulting in the identification of or related to the defendant's vehicle." *See* Government Discovery Response 12/21/22. However, this appears to be incorrect as the software provider's website explains, once an "Interdiction Analysis" report is created it is "automatically stored under the 'Reports' module of this menu for further and/or later review." *What is on the Analytic Reports page?*, REKOR, https://help.rekor.ai/what-is-on-the-analytic-reports-page (last visited on February 9, 2023).

[9] The defense asked Westchester County for "All records regarding access to ALPR data, including . . . purposes for which the data may be accessed; purposes for which the data may not be accessed; [and] who may access the data, what procedures they must go through to obtain access, and who must authorize access." Westchester responded, "According to Department Policy; it's a legitimate law enforcement purposes." The County also referenced the Department Manual, and indicated that information could be accessed "thru an Intel Unit supervisor or their designee and he/she must be a sworn Law Enforcement officer or crime analysist working under direct supervision of a L/E officer." *See RTC FOIL Response*, § 5. The County Department Manual, however, contains no specific guidance about proper and improper access and use of the LPR information. Department Manual, § 104.07 (Exhibit C).

searches appear to have been run across the entire dataset of more than 1.6 billion ALPR records over a period of two years. Therefore, the search was not just of Mr. Zayas's location information—it was a search of *every* individual in the database over a two-year period. In other words, the government searched the location data of hundreds of millions of people who they had no reason to suspect of any crimes.

Upon searching everyone's personal location information over a two-year period, police located two trips by Mr. Zayas that they deemed suspicious. One of these, occurring on October 16, 2020, showed Mr. Zayas passing southbound through Scarsdale at 12:44 p.m. and then northbound through Yonkers at 3:31 p.m. On August 21, 2021, the records show that he passed southbound through Rye at 8:17 a.m. and through Yonkers at 9:10 a.m. Law enforcement also saw that Mr. Zayas made other trips, but noted nothing specific about these trips that rendered them suspicious. Despite this, law enforcement continued to investigate Mr. Zayas using other data from the RTC surveillance network, among other sources, and eventually "alerted the vehicle" in the ALPR system. When that alert was triggered by Mr. Zayas's travel through Westchester County, Sgt. McCarrick notified P.O. DiRienzo who began following Mr. Zayas and eventually pulled him over. They then used the ALPR data as part of their justification for the stop of the vehicle and subsequent extension of that stop to question Mr. Zayas and conduct a canine sniff of his vehicle. *See Opposition to Motion to Dismiss*, at 8-13, 14-15.

Thus, the identification of Mr. Zayas and investigation into him began with the suspicionless search of his ALPR location information and culminated with the physical search of his vehicle. Therefore, all evidence obtained in this case flowed from the initial search of his ALPR records.

ARGUMENT

Sgt. McCarrick's search of Mr. Zaya's location information (and that of every person traveling through Westchester County) over a two-year period, without any reason to suspect him (or any individual) of a crime, was a warrantless dragnet search. This court should therefore suppress the "fruits" of that search, *i.e.*, the subsequent seizure of Mr. Zayas and the search of his vehicle.

I. Mr. Zayas Has a Reasonable Expectation of Privacy in His Historical Location Information

A person does not surrender all Fourth Amendment protection by venturing into the public sphere. *Carpenter v. United States*, 138 S.Ct. 2206, 2217 (2018). Individuals maintain a reasonable expectation to privacy in their movement over extended periods of time—even when traveling on open roads and in public view. *See id.* (citing *United States. v. Jones*, 565 U.S. 400, 430, (2012) (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring).

In *Carpenter*, the court explained that "[a]lthough 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.'" *Id.* at 2213-14 (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)). There, in finding an expectation to privacy in seven days of cell site location information (CSLI), the Court examined the "deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach…." *Id.* at 2223. The Court's analysis focused on several factors: 1) the length of the surveillance, *id.* at 2215, 2220; 2) the precision of the technique, *id.* at 2219; 3) the automatic and indiscriminate collection, *id.* at 2218; 4) the inescapable nature of the technique, and 5) the ability to retrospectively obtain otherwise unknowable information. *Id.*

The search in this case was unreasonable and unlike anything conceivable at the founding of our nation and establishment of the Fourth Amendment. It exceeded the level of surveillance possible using other techniques in the length of time it covered, precision of the location information, automatic collection, inescapable nature, and its ability to track everyone retroactively.

A. The ALPR Database Allows Unprecedented Surveillance of the Public That Threatens Traditional Expectations of Privacy

The search of Mr. Zayas's location history over a period of two-years represents a search of previously unimaginable proportion that threatens to shatter the "degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

Drivers may not have an expectation of privacy when it comes to isolated observations of their license plate or vehicle registration while driving on public roads. *See United States v. Miranda-Sotolongo*, 827 F.3d 663, 667 (7th Cir. 2016) (citing cases); *see also United States v. Matthews*, 615 F.2d 1279, 1285 (10th Cir. 1980). But this is a different scenario: the ALPR surveillance network here, and the way it was leveraged in this case, is nothing like the isolated reading or input of a license plate into a database. Comparing a single reading of a plate to a search of hundreds of millions of people's location information over a period of two years is like comparing "a ride on horseback… [to] a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley v. California*, 573 U.S. 373, 393 (2014). The question for this court is not whether there is a right to privacy in the isolated observation of a plainly visible license plate on a public road; it is, "whether people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects, and stores for… years their [license

plate location data] for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval." *Klayman v. Obama*, 957 F.Supp.2d 1, 37 (D.D.C. 2013).

Here, a vast network of cameras and a database of location information "has afforded law enforcement a powerful new tool… [which also] risks Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent." *Carpenter*, 138 S.Ct. at 2223 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). Specifically, it allowed the government—without any reason to think that a specific crime had been committed (let alone to suspect any particular person)—to search over 1.6 billion location records for evidence of what they deemed to be "traffic patterns consistent with narcotics trafficking." This would not have been possible without the "ever alert" network of cameras and the "nearly infallible" memory of the ALPR database created and maintained by RTC. *See id.* at 2219. "[I]t is almost impossible to think of late-18th-century situations that are analogous to what took place in this case." *Jones*, 565 U.S. at 420 (Alito, J., concurring). Therefore, the court should find a reasonable expectation of privacy in the two-years of Mr. Zayas's historic ALPR data gathered and accessed by the government in this case.

B. The Duration of the Surveillance.

The ALPR data searched in this case exceeded the breadth of the CSLI data searched in *Carpenter* and the GPS data in *Jones* because it spans a longer period of time.

The court, in examining the breadth of location information, must first look to the duration of the surveillance. *See Carpenter,* 138 S.Ct. *at 2215; see also Leaders of a Beautiful Struggle v. Balt. Police Dep't,* 2 F.4th 330, 341 (4th Cir. 2021); *United States v. Moalin*, 973 F.3d 977, 991 (9th Cir. 2020); *Klayman,* 957 F.Supp.2d at 32. This is because "[p]rior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so 'for

any extended period of time was difficult and costly and therefore rarely undertaken.'" *Carpenter 138 S. Ct.* at 2217 (quoting *Jones*, at 565 U.S. at 429 (Alito, J. concurring)). Thus, while "relatively short-term" tracking of a "person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable[,]" *Jones*, 565 U.S. at 430 (Alito, J., concurring) (citation omitted), "longer term" tracking "impinges on expectations of privacy." *Carpenter*, 138 S. Ct. at 2231 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)); *see also Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *Leaders*, 2 F.4th at 341.

Sgt. McCarrick searched Mr. Zayas's location data for a period of two years. The search itself was apparently not specific to Mr. Zayas, but it was a search across all 1.6 billion individuals in the database, including Mr. Zayas. This was not an isolated use of surveillance tools to enhance officer's visual observations a during a discrete "automotive journey" like those police used in *Knotts*. *Carpenter*, 138 S.Ct. at 2215; *see also United States v. Knotts*, 460 U.S. 276, 282(1983). To the contrary: the duration of the tracking here (some 730 days) dwarfs both the 28 days of surveillance considered in *Jones* and the 127 days searched in Carpenter. *See Carpenter*, 138 S.Ct. at 2212; *Jones*, 565 U.S. at 403. In fact, the Court in *Carpenter* held that obtaining as little as seven days of CSLI records was a search under the Fourth Amendment. *Carpenter*, 138 S. Ct. at 2217. Here, without any suspicion that Mr. Zayas had committed a crime, police looked at two years of his location information. This weighs heavily in favor of finding a reasonable expectation to privacy in Mr. Zayas's ALPR location data.

The existence of gaps in the data or timeframe is not dispositive of the expectation of privacy. In other words, the program need not achieve "perfect tracking of all individuals it captures across all the time it covers." *Leaders*, 2 F.4th at 342; *see also Carpenter,* 138 S. Ct. at 2211 (noting that companies only record CSLI when the phone makes a connection to the

network, by placing a phone call or receiving a text message). Therefore, while the there are gaps in the two years of surveillance of Mr. Zayas's travel patterns, they do not negate his reasonable expectation of privacy in his location information.

C. The Precision of the Location Information.

In analyzing the constitutionality of warrantless location tracking, it is also necessary to examine the precision of the data being searched. *Carpenter,* 138 S. Ct. at 2212, 2218; *see also Leaders*, 2 F.4th at 343. Here, the multi-year collection of ALPR records and subsequent search allowed law enforcement to identify the precise location of Mr. Zayas with greater accuracy than the GPS tracker that was deemed unlawful in *Jones*. For example, two of the 21 datapoints in this case that the government relied on were 40.913933º latitude by -73.850319º longitude and 40.976852º latitude by -73.758293º longitude. These coordinates are accurate enough to pinpoint the ALPR camera's location to a distance of two-to-four inches and as a result, within feet of the vehicle whose plate was scanned.[10] This provides greater precision than the GPS technology used in *Jones*. *See Jones*, 565 U.S. at 403 (stating GPS device was accurate to within 50 to 100 feet).

By contrast, the precision of CSLI "depends on the size of the geographic area covered by the cell site." *Carpenter*, 138 S. Ct. at 2211. This may be sufficient to place a person "within a wedge-shaped sector ranging from one-eighth to four square miles," for example. *Id.* at 2218. As a result, a single CSLI data point could be used to determine which neighborhood or zip code someone was in; but it would not be accurate enough to identify the block and building. Moreover, even though cell phones "ping" nearby cell sites several times a minute, service

[10] See Decimal degrees, WIKIPEDIA, https://en.wikipedia.org/wiki/Decimal_degrees (noting at six decimal places, coordinates are accurate to within 43-to-111 mm and precise enough to identify individual humans).

providers only log when the phone makes a connection, by placing a phone call or receiving a text message, for example. *Id.* at 2211.

Therefore, here the ALPR surveillance system which can track a surveilled license plate within a few feet, is more precise than the GPS location information in *Jones* and the CSLI location information in *Carpenter*.

D. The Automatic and Indiscriminate Collection and Retention of ALPR Data.

RTC's ALPR data is overly comprehensive in its reach. Like the CSLI in *Carpenter,* it was collected automatically and indiscriminately, without a connection to any particular investigation, suspect or crime. Thus, "this newfound tracking capacity [of searching ALPR data] runs against everyone," which is precisely the type of warrantless Governmental intrusion that was rejected by *Carpenter. Id.* at 2218, 2223.

Like CSLI, the collection of ALPR data is indiscriminate by design and captures images of every passing vehicle. ALPR data is retained and added to large databases regardless of whether the individual driving the vehicle is implicated in a crime or doing anything suspicious. In fact, only a tiny fraction of the location data collected is linked to any criminal activity.

In this case the surveillance network is vast and the volume of data retained within the government's databases is immense. The database created by that network currently contains datapoints from hundreds of millions of people who passed through Westchester County, regardless of whether they engaged in any wrongdoing. Furthermore, the search conducted in this case appears to have been run across the entire dataset of more than 1.6 billion ALPR records over a period of two years. Therefore, the search was not just of Mr. Zayas's location information—it was a search of *every record* from *every individual* in the database over a two-year period. In other words, the government searched the location data of hundreds of millions of

people who they had no reason to suspect of any crimes. They also stored this information, allowing them to continue to search this private information as long as they so desire.

Therefore, the ALPR data in this case, like the CSLI data in *Carpenter*, was collected and searched automatically and indiscriminately such that it "runs against everyone." *Id.*

E. The Inescapability of ALPR Surveillance

The location tracking here is also comprehensive in its reach because of the inescapable nature of this ALPR surveillance network. The reason for this is that ALPR networks like the CSLI tracking in Carpenter attach geolocation information to an essential element of modern society—driving.

Like cellphones, automobiles are, "indispensable to participation in modern society." *Id.* at 2210. Americans take 1.1 billion trips a day—four for every person in the U.S.[11] Eighty-seven percent of these daily trips take place in personal vehicles. Bureau of Transp. Stats., *supra* note 12. Forty-five percent of daily trips are taken for shopping and errands. *Id.* Twenty-seven percent of daily trips are for social and recreational purposes, such as visiting a friend. *Id.* Fifteen percent of them are taken for commuting to work. *Id.* On average 75.61% of Americans commute via motor vehicle- 67.82% drive alone in a personal vehicle.[12]

Vehicular travel is just as essential in Westchester County as in the rest of the nation. In New York State 77.2% of long-distance travel (50 miles or more one way) originating in the state was done in a personal use vehicle.[13] These trips included everything from daily commutes

[11] Based on National Household Travel Survey, 2001-2002, *See Bureau of Transportation Statistics National Household Travel Survey Daily Travel Quick Facts*, (last updated May 31, 2017), https://www.bts.gov/statistical-products/surveys/national-household-travel-survey-daily-travel-quick-facts (last visited March 3, 2023).
[12] Bureau of Trans. and Stats., U.S. Dep't of Transp., *Commute Mode Year 2021*, https://www.bts.gov/browse-statistical-products-and-data/state-transportation-statistics/commute-mode (last visited March 3, 2023).
[13] CTR. FOR TRANSP. ANALYSIS, 2001 LONG DISTANCE TRAVEL IN NEW YORK STATE 3 tbl.1 (2005), https://www.dot.ny.gov/divisions/policy-and-strategy/darb/dai-unit/ttss/repository/Full%20LD%202001%20Results%20Report.pdf (last visited Feb. 16, 2023).

and business trips to vacation and visiting family. Ctr. for Transp. Analysis, *supra* note 14. In 2021, 55.16% of people in New York State commuted to work every day via personal motor vehicle. Bureau of Transp. Stats., *supra* note 13. In Westchester County, only 17.2% of people commute by train.[14]

The surveillance network here includes over 1.6 billion scans with the location data of everyone who passed through Westchester County—hundreds of millions of individuals. The actual reach of the network may be even larger than reported as the RTC participates in data-sharing with other local departments and has access to a national database containing an unknown number of records.[15]

Here, like the CSLI in *Carpenter* and the pole cameras in *Moore-Bush*, avoiding ALPR cameras theoretically possible. *See, e.g., Carpenter*, 138 S. Ct. at 2218; *United States v. Moore-Bush*, 36 F.4th 320, 338 (1st Cir. 2022). For example, one could forgo the use of a car altogether and rely solely on public transit. However, for many people that would virtually eliminate their constitutional right to travel. *See Kent v. Dulles*, 357 U.S. 116, 125 (1958) ("The right to travel is part of the 'liberty' of which the citizen cannot be deprived without the due process of law under the Fifth Amendment"). For instance, those with compromised immune systems who should not travel on crowded trains or buses (especially during a pandemic), have no choice but to travel by car. And given the limited public transit available, even those without health issues often require a car to work, travel or socialize. Of course, if the cameras were visible and recognizable to the public, one could theoretically map out the hundreds of cameras and find a

[14] Westchester Cty. Dep't of Planning, *Commuting by Train*, https://planning.westchestergov.com/images/stories/Census/traincommute1317.pdf (last visited Feb. 16, 2023).
[15] RTC is also a part of the Rekor Public Safety Network ("RPSN") which shares ALPR data across every law enforcement agency enrolled in the network. *Rekor Systems Launches Public Safety Network*, https://www.bloomberg.com/press-releases/2019-08-21/rekor-systems-launches-public-safety-network (last visited Feb. 16, 2023).

path where the fixed cameras are not located. However, given the size of the network such a task would require months if not years of work to accomplish. Additionally, "the location of these cameras change frequently," so avoiding this vast network of LPR cameras is simply not feesible. *See Government Discovery Disclosure* at ¶ 13.

Given the vast nature of the ALPR network and the need to travel public highways to engage in modern life, avoiding ALPR surveillance is both unfeasible if impossible. Indeed, as with cellphones "[o]nly the few without [vehicles] could escape this tireless and absolute surveillance." *Carpenter*, 138 S. Ct. at 2218.

F. The Ability to Retrospectively Obtain Otherwise Unknowable Information

This search of this ALPR data violated Mr. Zayas's reasonable expectation of privacy because, like the CSLI in *Carpenter*, it allowed police to retrospectively track Mr. Zayas (and hundreds of millions of others) to learn information that would have been otherwise unknowable.

The Court in *Carpenter* noted that the "retrospective quality" of CSLI made it even more invasive than the type of location tracking in *Jones*. *Id.* This is because it "gives police access to a category of information otherwise unknowable." *Id.* The Court noted that "[i]n 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 polices of the wireless carriers, which currently maintain records for up to five years…. Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when. Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years." *Id.*

Here, from law enforcement's perspective the primary utility of the ALPR data was its retrospective nature. At the outset of their investigation the government admittedly had no suspects—indeed they had no particular crime to investigate. Instead, they explicitly set out to look at the historic location records of everyone passing through Westchester County (and perhaps other locations) to identify those vehicles they considered to be exhibiting, "traffic patterns consistent with narcotics trafficking." *See Opposition to Motion to Dismiss*, at 2. To do this they looked two years into the past to examine who, if anyone, might fit their unknown parameters of suspicion.

This type of suspicionless collection of location data so that the government can, "call upon the results of that surveillance without regard to the constraints of the Fourth Amendment…" is exactly the type of "tireless and absolute and tireless surveillance" that lead the Court in *Carpenter* to find a reasonable expectation of privacy in a week's worth of CSLI. *Carpenter*, 138 S.Ct. at 2218. In this investigation the government did not suspect Mr. Zayas of a crime and surveil his vehicle to confirm their suspicions. They "called upon" a database of indiscriminately gathered information to retroactively traced his location on the chance it might produce something suspicious. This is far more concerning from a constitutional perspective than tracking the location of a single person for which the government has cause to believe committed a crime. This is a kind of mass surveillance unprecedented outside of the war on terror. *See e.g. Moalin*, 973 F.3d at 992-93 (finding bulk metadata collection likely unconstitutional, but denying suppression on the grounds that the collection did not taint the evidence introduced by the government at trial); *Klayman*, 957 F.Supp.2d 1 (granting a preliminary injunction on NSA's bulk metadata collection).

To examine the facts of this case against the "historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted…'" *Carpenter*, 138 S. Ct. at 2213-2214 (citation omitted), is "almost impossible." *Jones*, 565 U.S. at 420, (Alito, J. concurring). To borrow from the analogy discussed in *Jones*: to achieve this level of surveillance in 1791 the government would have had to set up thousands of extremely focused, eagle-eyed constables, trained as scriveners and working in shifts around Westchester County recording everyone who passed. *See Jones*, 565 U.S. at 420 (Alito, J. concurring); *see also id.* at 407 n. 3. Assuming the recording of everyone's travel through Westchester could be accomplished by this fastidious group of constables, thousands more would be required to pour over the records for months at a time to identify travel habits, they believed were suspicious. *See id.* This as would have been both "difficult and costly" such that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—" *Carpenter,* 138 S.Ct. at 2217, track the travels of every citizen traveling the roads over a two-year period.

II. Prior ALPR Cases Are in Conflict with the Supreme Court's Holding in *Carpenter* and Are Distinguishable from the Dragnet Search Employed Here.

There are a number of cases that have found that there is no reasonable expectation of privacy in data related to ALPR surveillance. *See e.g. United States v. Porter*, No. 21-CR-00087, 2022, 2022 WL 124563 (N.D. Ill. Jan. 13, 2022); *United States v. Brown*, No. 19 CR 949, 2021 WL 4963602 (N.D. Ill. Oct. 26, 2021); *United States v. Bowers,* No. 2:18-CR-00292-DWA, 2021 WL 4775977 (W.D. P.a. Oct. 11, 2021); *Commonwealth v. McCarthy*, 484 Mass. 493, 507 (2020); *United States v. Graham*, No. 21-645 (WJM), 2022 WL 4132488, at *5 (D.N.J. Sept. 12, 2022). However, these decisions are all distinguishable and contain several analytical errors that conflict with *Carpenter's* holding. First, they inappropriately apply antiquated law to cases

involving modern surveillance technology. Second, they treat the number of datapoints collected as dispositive while failing to consider the other factors considered by the Court in *Carpenter*. And they are distinguishable because none involved the type of suspicionless dragnet of extended periods of location information conducted in this case.

The first error in these cases is comparing a persistent and pervasive network of ALPRs to isolated observations of license plates and short-term tracking of vehicles. *See, e.g.*, *Brown*, 2021 WL 4963602, at *3 (first quoting *United States v. Miranda-Sotolongo*, 827 F.3d 663, 667-68 (7th Cir. 2016); and then quoting *Knotts*, 460 U.S. at 281); *Porter*, 2022 WL 124563, at *3 (citing *Knotts*, 460 U.S. at 281); *Bowers*, 2021 WL 4775977, at *3 (first citing *Knotts*, 460 U.S. at 281-82; and then quoting *United States v. Ellison*, 462 F.3d 557, 561-62 (6th Cir. 2006)). Although license plates are involved in the functioning of an ALPR surveillance system, the isolated reading of a license plate cannot be compared to the searching of years of location information belonging to hundreds of millions of people. *See supra* § A.

These comparisons represent the kind of "mechanical" application of old doctrine to new surveillance technologies that the Court has warned will leave society "at the mercy of advancing technology." *Carpenter,* 138 S. Ct. at 2214 (*quoting Kyllo*, 533 U.S. at 35); *see also Riley*, 573 U.S. at 393 (rejecting application of the search incident to arrest doctrine to cell phones found in an arrestee's possession); *Moore-Bush*, 36 F.4th at 338 (rejecting the application of prior pole camera and aerial observation law to eight months of video recordings of the curtilage of a home). Moreover, the Supreme Court has already rejected comparisons between the limited surveillance conducted in *Karo* and *Knotts* and the long-term tracking of vehicles and people. *Jones*, 565 U.S. at 419, 430, (Alito, J. concurring) ("Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that

our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *id.* at 415 (Sotomayor, J. concurring); *see also Knotts*, 460 U.S. at 284 ("[I]f such dragnet type law enforcement practices… should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

The second error in these ALPR cases is their fixation with the number of location datapoints at issue. *See Brown*, 2021 WL 4963602, at *3 ("The record contains about two dozen snapshots of a car on the streets over ten weeks . . . ."); *Bowers*, 2021 WL 4775977, at *4 ("[T]he ALPR cameras in this case captured Defendant's license plate on 106 occasions in thirty-three unique public locations over a four-and-a-half-month period. This limited data collection does not even begin to approach the same degree of information as that gathered in *Carpenter*, nor does it otherwise implicate similar privacy concerns."); *United States v. Yang,* 958 F.3d 851, 863 (9th Cir. 2020) (Bea, J., concurring) (A single entry "[c]ontrasted with the nearly 13,000 unique data points—more than 100 per day—that the search of cell phone records in *Carpenter* revealed, it's not hard to see how that search infringed on Fourth Amendment rights while the search here did not."). While the number of location datapoints was considered by the Court in *Carpenter*, it was merely a single factor out of many. *See supra,* § B-F. In examining the nature of the surveillance technique employed *Carpenter* considered: the length of time covered; the level of detail of the location information; the automatic and indiscriminate collection; the inescapable nature of the technique; and the ability to retrospectively obtain otherwise unknowable information. *See id.* The analysis must focus on whether the surveillance is long-term and transcends ordinary police capabilities, or whether it is merely an "augmentation of

ordinary police capabilities," equivalent to "traditional, short-term surveillance." *Leaders*, 2 F.4th at 343-345. Thus, existence of gaps in the data or timeframe is not dispositive. *Id.,* at 342.

Finally, even if the Court were to find any of the decisions on ALPR databases compelling, none of them considered the way the instant ALPR surveillance network was leveraged here. *See, e.g., Porter*, 2022 WL 124563, at *1 (plate captured fleeing a bank robbery); *Brown*, 2021 WL 4963602, at *2 (partial plate obtained from an ALPR at the scene of the robbery); *Yang,* 958 F.3d, at 854 (plate caught on video camera while engaging in "fishing"); *United States v. Ruben*, 556 F.Supp.3d 1123 (N.D. Cal. 2021) (partial plate searched in ALPR database to determine full plate). Unlike those cases, which involved active investigations into identifiable crimes, the investigation into Mr. Zayas began with the dragnet surveillance of all drivers who passed through Westchester County over a period of two years. As detailed in the Government's motion papers, Mr. Zayas was not suspected of any crimes at all until the government began examining his travel habits over a two-year period and determined them to be "consistent with narcotics trafficking." *See Opposition to Motion to Dismiss*, at 1-2. This is the specter of modern surveillance that the Fourth Amendment must guard against in order to "assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 138 S. Ct at 2214 (*quoting Kyllo*, 533 U.S. at 34).

Furthermore, both the concurrence in *Yang* and majority in *McCarthy* recognized that while the limited use of the ALPR technology in those instances did not support a finding of a reasonable expectation of privacy, it was quite possible that future cases would support such a finding. *See Yang,* 958 F.3d at 864; *McCarthy*, 484 Mass. at 494. The concurrence in *Yang* explained that the single scan there was nowhere near the type of surveillance addressed in *Carpenter*. 958 F.3d at 863 (Bea, J., concurring). However, the decision also noted "ALPRs may

in time present many of the same issues the Supreme Court highlighted in *Carpenter*. ALPRs can effortlessly, and automatically, create voluminous databases of vehicle location information." *Id.* Similarly, in *McCarthy* the Supreme Judicial Court of Massachusetts noted that the defendant's interest in the whole of his public movements "potentially could be implicated by the widespread use of ALPRs…." 484 Mass. at 494. The court explained that "[w]ith 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 506. However, the court noted the record lacked any information regarding the number of records collected by the government, the scope of the search of those records, the number of cameras in the network, and the placement of those cameras. *Id.* at 504-09; *id.* at 515 (Gants, C.J. concurring). So, all that they were left to consider was the collection of data from four cameras at fixed locations on the ends of two bridges. *Id.* at 409.

The potential privacy concerns warned by the courts in *Yang* and *McCarthy* are manifest in the Westchester ALPR network. The RTC surveillance network includes 480 ALPR cameras—434 stationary systems and 46 mobile systems. *RTC FOIL Response*, at § 3(C).[16] Its cameras record video footage and utilize artificial intelligence to track and record the make, model, and color of the vehicles in addition to the plate number.[17] The system archives, approximately 16.2 million plates per week and retains that information for two years—creating a database of over 1.6 billion images of license plates belonging to anyone traveling through the area. *Id.* at § 3(B) & 4(A). This is not the collection of discrete data from four cameras at fixed locations on the ends of two bridges. *See McCarthy,* 484 Mass at 509. This is the systematic

[16] *See also, RTC: Westchester County, NY,* https://www.mobotix.com/en/lpr-westchester-county-ny (last visited March 3, 2023).
[17] See *RTC: Westchester County, NY, https://www.mobotix.com/en/lpr-westchester-county-ny (last visited March 3, 2023).*

development and deployment of a vast surveillance network that invades society's reasonable expectation of privacy.

The type of dragnet search conducted using the ALPR network here is more like the Baltimore "AIR program" than it is the common deployment of ALPR readers. *See e.g. Leaders,* 2 F.4th at 330.

The AIR program in Baltimore used aerial photography to track the movements of people and vehicles across the city. *Id.* at 334. To accomplish this, multiple planes mounted with camera technology known as the "Hawkeye Wide Area Imaging System" flew around the city at least 40 hours per week taking photos. *Id.* Photos were taken every second and each one covered 32 square miles. *Id.* Thereby the system captured roughly 90% of the city each day. *Id.* Each image displayed both people and vehicles as either blurred blobs or dots. *Id.* The planes then transmitted their photographs to "ground stations." *Id.* All of these images were retained for 45 days. *Id.* Although this system did not allow real-time tracking, upon an officer's request, contractors would prepare reports that tracked vehicles and people around the location of a crime both before and after the incident. *Id.* All the images and data related to each request were retained "indefinitely as necessary for legal proceedings and until relevant statutes of limitations expire." *Id.*

The government in *Leaders* attempted to distinguish *Carpenter* by explaining that the aerial surveillance program there did not target any particular citizen. *Id.* at 346. The court responded stating, "This does highlight an important distinction, but it cuts in the other direction. In *Carpenter*, service providers collected comprehensive location data from their subscribers. As Defendants point out, the government's only role was to request that data as to specific investigations. Under the AIR program, the government does both. The government continuously

records public movements. Then, the government—once officers know where (and when) to look—tracks movements related to specific investigations. Only by harvesting location data from the entire population could BPD ultimately separate the wheat from the chaff." *Id.* at 347. The court also dismissed comparisons to "aerial surveillance methods" in part because "those cases all involve some discrete operation surveilling individual targets." *Id.* at 345. They noted that the plaintiffs were not objecting to the use of aerial photography—their challenge was to the creation and use of "a retrospective database of everyone's movements across the city." *Id.*

The challenge here is similarly not about a single image or license plate observation. It is to the search of a surveillance network that allows the retrospective tracking of everyone's movements across Westchester County. The government here was not engaged in a targeted investigation into Mr. Zayas, his car, or any particular crime. Instead, the government harvested the public movements of the entire population and then searched them to analyze traffic patterns they believed were "consistent with narcotics trafficking."

Ultimately in *Leaders,* the court concluded: "The AIR program records the movements of a city. With analysis, it can reveal where individuals come and go over an extended period. Because the AIR program enables police to deduce from the whole of individuals' movements, we hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment." *Id.* at 346. The same is true here. Accessing years of historical location information harvested by the ALPR network allowed police to deduce what they were otherwise incapable of knowing: that Mr. Zayas's travel habits were "consistent with narcotics trafficking." Therefore, it was a search, and its warrantless operation violated the Fourth Amendment.

The surveillance program here, even more so than the AIR program in *Leaders*, is "a 21st century general search, enabling the police to collect all movements, both innocent and

suspected, without any burden to 'articulate an adequate reason to search for specific items related to specific crimes.'" *Id.* at 347 (quoting *Messerschmidt v. Millender*, 565 U.S. 535, 560 (2012) (Sotomayor, J., dissenting). "Allowing the police to wield this power unchecked is anathema to the values enshrined in our Fourth Amendment." *Id.* Therefore, if this court is to uphold the "central aim" of the Fourth Amendment it must "place obstacles in the way of a too permeating police surveillance[]" and require judicial oversight. *Carpenter*, 138 S. Ct. at 2214, (quoting *Di Re*, 332 U.S. at 595).

III. The Search of Mr. Zayas's Historical Location Records Required a Warrant

A warrant was required in this case because the government searched Mr. Zayas's historical location records for a period of two years.

Accessing and querying large quantities of location data is a Fourth Amendment search requiring a warrant. *See Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring); *id.* at 429–31 (Alito, J., concurring); see *also Leaders*, 2 F.4th at 346 ("[W]e hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment."); *United States v. Chatrie*, 590 F. Supp. 3d 901, 925 (E.D. Va. 2022) (denying suppression where police relied in good faith on a warrant, but noting a "deep concern" about the querying of large databases of geolocation information.); *Moore-Bush*, 36 F.4th at 341 ("[T]he government did conduct a Fourth Amendment 'search' when it accessed the digital video record that law enforcement had created over the course of the eight months in question, notwithstanding the government's contention that the record itself is merely a compendium of images of what had been exposed to public view.").

Furthermore, the nature of the initial query and its implications for privacy demonstrate a need for judicial oversight of ALPR searches. Here law enforcement, based on their "training

and experience," determined that quick trips to New York City, the largest city in the country, were indicative of narcotics trafficking such that they should initiate an investigation into the driver.[18] This was based on the officer's training and experience "that narcotics traffickers travel large distances to conduct a transaction and return quickly to their origin city…." However, there are many reasons that people may travel large distances for short periods of time. For example, a lawyer may travel long distances for a brief court appearance. A patient may travel long distances for an appointment with a specialist. A reporter may meet briefly with a distant source. Furthermore, while some interstate narcotics travelers may take long trips over short periods of time- others clearly do not. It is not unusual for interstate narcotics traffickers to have locations in multiple states where they stay for extended periods of time. This is necessary for building up and monitoring criminal networks in multiple locations. In other words, the officer's conclusion and subsequent search is obviously both underinclusive and overinclusive. However, based on nothing more than his own subjective beliefs he decided that he could search the travel patterns of everyone who has traveled through Westchester County over the course of years. With no judicial oversight this type of system operates at the caprice of every officer with access to it.

"Allowing the police to wield this power unchecked is anathema to the values enshrined in our Fourth Amendment." *Leaders,* 2 F.4th at 347. Furthermore, requiring a warrant would not eliminate the availability of such surveillance techniques to law enforcement, it merely emphasizes "that the role of the warrant requirement remains unchanged as new search capabilities arise. *Id.* Therefore, the search of two years of ALPR location records belonging to hundreds of millions of drivers required a warrant.

[18] Although defense is not in possession of the initial query that demonstrated the Chevrolet Equinox with MA 3CD192 was "exhibiting travel patterns consistent with interstate narcotics trafficking," it is clear from discovery and assertions by the government that it was based on short turnaround times of two prior trips. *See Opposition to Motion to Dismiss*, at 2.

CONCLUSION

"[P]eople have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects, and stores for… years their [location information] for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval." *Klayman*, 957 F.Supp.2d at 37. Thus, the suspicionless collection and mining of the location data of Mr. Zayas and all people passing through Westchester County over a period of two years was a warrantless search and a violation of the Fourth Amendment. Therefore, all contraband and evidence resulting from the subsequent stop and search of his car must be suppressed. *See Wong Sun v. United States*, 371 U.S. 471, 488 (1963).

Dated: March 3, 2023
White Plains, New York

Respectfully Submitted,

/s/_____

Benjamin Gold
Assistant Federal Defender
Federal Defenders of New York
81 Main Street, Suite 300
White Plains, New York 10601

Sidney Thaxter
Senior Litigator, 4th Amendment Center
NACDL
1660 L. St. NW, 12th Floor
Washington DC 20036

Attorneys for DAVID ZAYAS

Exhibit A

FOIL Reply

Section 3

All records regarding the use of ALPR technology, including

a. what types of data are obtained;
b. number of license plates scanned and/or read in a given time period (day, month, year, etc.);
c. the number of ALPR cameras, units or systems acquired;
d. the number of vehicles equipped with ALPR technology;
e. for stationary deployments, the number and physical location of ALPR units;
f. the technical capabilities of the ALPR units;

A. The following data is collected with each license plate read;
    a. Date
    b. Time
    c. Location (Lat/Long)
    d. What it believes the License Plate State (completed by machine learning)
    e. What it believes the License Plate characters are
    f. Computational data where the vehicle and plate are in the image (X,Y)
B. # of Plates scanned
    a. As of 01/30/2023, 16.2 million per week (The number fluctuates based on equipment being broken, weather, etc)
C. # of ALPR camera
    a. We manage 480 cameras currently in our system
        i. Approximately ½ of those cameras where purchased by Westchester
        ii. I can break it down by Agency but that will take some time. I have to look at each site and determine who paid for it.
D. # of Mobile Systems
    a. 46 Mobile Systems Total
        i. 23 belong to Westchester
        ii. 23 to Outside Agencies
E. # of Stationary / Locations
    a. 434 Stationary Systems
        i. Westchester County
        ii. Other Agencies
    b. Locations – Those we cannot release as it will effect current future investigations
F. Technical Capabilities
    a. Can you be more specific? What exactly are you looking for?

i. Maybe check the Rekor Website, that is the software vendor we are using. Specifically Rekor Scout.

Section 4

All records regarding the storage of data obtained using ALPR technology, including

a. how long data is stored;
b. when data must be discarded;
c. how many individual license plate scan records your agency currently stores;

A. Data Storage
   a. We follow the NYS MPTC recommendations and store data for 24 months
   b. Automatically deleted after 24 months, unless specifically attached to an investigation.
   c. Exact number is unknown, I calculate the number to be weekly reads times 104 weeks. 1,664,000,000

Section 5

All records regarding access to ALPR data, including

a. the legal justification required before an individual accesses ALPR data;
b. purposes for which the data may be accessed;
c. purposes for which the data may not be accessed;
d. who may access the data, what procedures they must go through to obtain access, and who must authorize access;
e. the existence or non-existence of any audit trails or other system that records who accesses the data and when the data is accessed;

A. According to Department Policy; it's a legitimate law enforcement purpose. Copy of Policy to be attached.
B. See above
C. See above
D. Obtain access must go thru an Intel Unit supervisor or their designee and he/she must be a sworn Law Enforcement officer or crime analyst working under direct supervision of a L/E officer.
E. System has an audit trail that tracks login, search's, alert list creation/deletion

Exhibit B

U.S. Department of Justice

United States Attorney
Southern District of New York

50 Main St. Suite 1100
White Plains, New York 10606

December 21, 2022

By Email
Ben Gold, Esq.
Federal Defenders of New York Inc.
81 Main Street, Suite 300
White Plains, New York 10601
Email: ben_gold@fd.org

Re: *United States v. David Zayas*, 22 Cr. 178

Dear Mr. Gold:

This letter provides discovery pursuant to Rule 16(a) of the Federal Rules of Criminal Procedure ("Fed. R. Crim. P.") and seeks reciprocal discovery. [1] These materials are subject to protective order. (Dkt. No. 8.)

Document Disclosure by the Government

Based on your request for discovery in this case, and per the Court's opinion and order of November 7, 2022 (the "November 7 Opinion," Dkt. No. 23), I have enclosed copies of the following materials, stamped with control numbers USAO_00152, USAO_00154-00177:

A New York State Division of Criminal Justice Services log of narcotics detection training for Officer DiRienzo and K-9 Liberty (the "Training Log");

An audit of the searches for license plate 3CD192;

LPR information regarding license plate 3CD192, including, for instance, photos of the vehicle, camera location, time, and direction of travel;

Policy statements maintained by Westchester County Department of Public Safety ("WCPD") regarding LPR usage;

[1] In addition to information provided herein, please note that this Office periodically posts content on social media platforms including Twitter, Facebook and YouTube. Members of the public may post comments in response to the Office's postings. We do not control these user-generated comments, nor do we monitor or regularly review such comments. You may directly access these social media platforms in the event you believe someone may have posted information relevant to this case.

The License Plate Readers Model Policy (March 2021), issued by the New York State Division of Criminal Justice Services; and

A slide deck (the "Driving Route Slide Deck"), prepared by Homeland Security Investigations Special Agent Michael Flanagan, showing photos from Google Maps, representing the route traveled by the defendant between two LPR readers on or about March 10, 2022, and the speed limits of the various segments of the route.

Disclosure Regarding License Plate Reader Data

By letter dated November 10, 2022 (the "November 10 Discovery Letter"), you requested certain discovery regarding license plate reader ("LPR") data.

The attached Driving Route Slide Deck shows photos of the route traveled by the defendant's vehicle on or about March 10, 2022, between two LPR readers ("LPR Location 1" and "LPR Location 2"). The defendant's Chevy Equinox passes LPR Location 1 at approximately 2:42 p.m., and LPR Location 2 at approximately 2:51 p.m. The distance between LPR Location 1 and LPR Location 2 is approximately 7.6 roadway miles, constituting three segments along which the speed limit varies. According to Special Agent Flanagan's measurements, the speed limit along that 7.6-mile route was 55 mph for approximately 3.3 miles of the distance, 50 mph for approximately 2.9 miles, and 45 mph for approximately 1.4 miles.

Apart from the information in the documents produced, WCPD does not store camera information for each camera that captured the defendant's vehicle. Nor does WCPD maintain a separate "Analytic Report" resulting in the identification of or related to the defendant's vehicle.

To the extent the November 10 Discovery Letter requests "any memorandum, emails or documents" regarding policies and procedures relating to joint investigations involving the WCPD and other agencies, this requests materials that are outside the scope of the Government's discovery obligations. In addition, the Government is unaware of any memorandum setting forth the policies of joint investigations between and among WCPD and Homeland Security Investigations and the Drug Enforcement Administration regarding the identification of vehicles "exhibiting patterns indicative of narcotics trafficking or other crime patterns."

The location of fixed LPR cameras linked to the Westchester County Real Time Crime Center is outside the scope of the Government's discovery obligations. In addition, the locations of such cameras – of which there are hundreds if not thousands – change frequently.

Production of all LPR "database records showing the number of historical vehicle scans currently in the database and the number of unique vehicle scans" would be outside the scope of the Government's discovery obligations in this case. Such records are estimated in the billions.

It is the Government's understanding that WCPD does not maintain activity reports or quarterly the use of the LPR system. WCPD likewise does not maintain "written agreements memorializing the terms of any ALPR equipment or data sharing programs between Westchester RTC and other law enforcement agencies or other public agencies."

It is the Government's understanding that WCPD does not maintain "written agreements memorializing the terms of any ALPR equipment or data sharing programs between Westchester RTC and any private agencies."

It is the Government's understanding that WCPD does not maintain "contracts, purchase orders, or agreements with ALPR hardware or software vendors."

Disclosure Regarding K-9 Liberty

The November 7 Opinion orders the Government to produce "discovery on the K-9's training, field performance, and instances of false positives." (Dkt. No. 23 at 2.) The November 10 Letter specifically seeks "[a]ll information, documentation, and data on the K-9's instances where the K-9 indicated that drugs or other contraband were present where no drugs or other contraband were recovered." (November 10 Discovery Letter at 1 n.2.)

Liberty has been deployed into the field approximately 85 times since starting work at WCPD in July 2021. She is trained to signal after detecting the odor of narcotics, an odor which may be present even if law enforcement does not recover narcotics. Such signaling when narcotics are not recovered does not indicate a "false" impression regarding the presence of narcotics, only that the odor of narcotics is present. WCPD does not keep statistics or logs regarding so-called "false positives," nor on the number of times a narcotic substance has been recovered after a positive indication. At times in the field, Liberty may be distracted by traffic, including by loud noises from cars (e.g., mufflers). Liberty's handler, Officer David DiRienzo, would then redirect Liberty back to the task. Accordingly, such distractions amount to temporary pauses in the process of narcotics odor detection rather than a factor that has prevented Liberty from signaling the presence of narcotics odor.

Liberty received training as indicated on the Training Log. In addition, Officer DiRienzo provides daily training as follows. Officer DiRienzo hides between two and four samples of narcotics, of different quantities and types. Officer DiRienzo then deploys Liberty to find each sample. When Liberty alerts, she receives a reward. Initially, this reward was food; more recently, she has come to be rewarded with time to play with a toy, typically a tug toy or ball. At times during this training, Liberty might be temporarily distracted, e.g., by birds, or the need to defecate or urinate – after which Officer DiRienzo would refocus Liberty on the drug-finding task. During this daily training, Liberty has never failed to find the hidden substance.

Liberty received training from Deputy William McKay of the Dutchess County Sheriff's Office, wmckay@dutchessny.gov. The contact information for the K9 accreditation program for the State of New York, which accredited Liberty, is below:

New York State Division of Criminal Justice Services
Ashley Sheroka
Law Enforcement Accreditation Program
Criminal Justice Program Specialist I
80 South Swan St., Albany, NY 12210
(518) 485-2838 | dcjscanine@dcjs.ny.gov

Very truly yours,

DAMIAN WILLIAMS
United States Attorney

by: __/s/_____
T. Josiah Pertz
Assistant United States Attorney
(914) 993-1966

Exhibit C

DEPARTMENT MANUAL Section 104.07

CHAPTER: Regulations			
SUBJECT: USE OF DEPARTMENT INFORMATION ASSETS			
ISSUE DATE: 5/2/2022	EFFECTIVE DATE: 5/2/2022	REVISES/SUPERSEDES: 11/29/2021 Issue	PAGE: 1 of 5

PURPOSE:

To regulate Employees' use of County or Department computer workstations, laptop computers, smart-phone devices, electronic mail ("e-mail"), databases, networks and connections (wired and wireless) to the County or other intranet, internet and any other information technology services available both now and in the future (hereinafter, "Information Assets") .

POLICY:

Employees shall use Department Information Assets primarily for the purpose of accomplishing Westchester County and Department objectives and shall not compromise the integrity or security of either the data contained therein or the equipment itself.

PROCEDURE:

COUNTY INFORMATION ASSET USE POLICY

1. Employees shall comply with the County "Security and Technology Use Policy" governing the use of Information Assets.

SUPPLEMENTAL REGULATIONS

2. Employees shall report any problems with Information Assets assigned to or used by them to the Department of Information Technology ("DoIT"):

   a. by e-mail to HelpDesk@westchestergov.com with a copy to their immediate Supervisors and to the Commanding Officer of the Information Technology Unit, or;

   b. by telephone to the help desk at (914) 995-5513 and, in the event of any significant issue, with follow-up notice to their immediate Supervisors and to the Department of Commanding Officer of the Information Technology Unit.

3. If a reported problem is not corrected in a reasonable amount of time, Employees shall contact the Department of Information Technology to follow up and ensure that the problem will be resolved.

4. Employees shall not connect any personally owned computer equipment, software or data to County or Department owned Information Assets without the express permission of the Commanding Officer of the Information Technology Unit or the

County Department of Information Technology, except that Employees may use personal devices to access the County's public networks and internet pages consistent with the rules and regulations governing same.

5. Unit Supervisors may create guidelines for their staff concerning reasonable incidental personal usage of County or Department computer systems or smart-phone devices which are no less restrictive than that which is provided for in the County Security and Technology Use Policy.

6. Employees are responsible for the security of County or Department Information Assets assigned to or used by them and shall take all reasonable precautions with respect to such equipment.

> NOTE: Reasonable precautions include, but are not limited to, maintaining the privacy of their identification codes, accounts and passwords, logging off or locking Information Assets when not actually using them, closing any software when not actually using it, and maintaining reasonable physical security for any Information Assets.

7. Employees shall not use County or Department Information Assets to access, create, transmit or delete typed language, words, symbols or data consisting of jokes and pranks.

8. Employees shall not copy any data, information or software using County or Department Information Assets for other than archive or 'back up' purposes.

9. Employees shall not use County or Department Information Assets to solicit for personal purposes, for personal gain or for the advancement of political or religious beliefs.

10. Employees shall not use any law enforcement database (including any license plate reader database and any database accessed through a Division of Criminal Justice Services portal) or disclose any information obtained therefrom for other than law enforcement purposes or authorized background investigation, or in any manner which violates the user agreement governing access to such database.

11. Employees shall not violate the integrity or security of Department Information Assets through their use thereof, and shall:

    a. change their passwords periodically, as directed, or immediately if the password may have been compromised;

    b. keep their passwords confidential and secure at all times by not sharing their passwords with others and by not using any function of their computers that allow for saving their user names and passwords on a given workstation unless such workstation is dedicated to a single user within a private office;

c. not leave any Department Information Asset unattended when data is not secured by password or other means; and

d. report to the Commanding Officer of the Information Systems Unit (with notification to their own immediate Supervisors) any attempt, or suspected attempt, at unauthorized access into Department Information Assets.

12. All data accessed, created, transmitted, or deleted by employees using County or Department Information Assets may be considered public records, and Employees are required to follow the applicable records retention procedures for same, except as may otherwise be provide for herein.

13. Notification of violations:

a. Employees who become aware of any violation of the laws, regulations or rules pertaining to the use of the Department Information Assets shall immediately notify their immediate Supervisors and the Commanding Officer of the Information Systems Unit of the facts, in writing.

b. If the Commanding Officer of the Information Systems Unit becomes aware of any violation of the laws, regulations or rules pertaining to the use of Department Information Assets, he or she shall immediately notify the violating Employee's Supervisor of the circumstances and take such other action as may be required by Department, County, Division of Criminal Justice Services and/or other applicable regulations.

CRIMINAL HISTORY RECORD INFORMATION

14. "Criminal History Record Information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release (the term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.)[1]

15. Criminal History Record Information may be obtained by authorized Employees through the Division of Criminal Justice Services (DCJS) portal, eJusticeNY, however, these provisions shall pertain to Criminal History Record Information regardless of how it is accessed.

16. The Commissioner shall designate an Employee to act as the Department's Local Agency Security Officer (LASO) who shall:

[1] As provided in 28 CFR § 20.3 which is incorporated in the DCJS Use & Dissemination Agreement for Criminal History Record Information and federal Criminal Justice Information Services data files.

a. identify users of the DCJS - approved electronic systems and ensure no unauthorized individuals or processes have access to same;

b. identify and document how the Department equipment is connected to the state system;

c. ensure that personnel security screening procedures are being followed as stated in this policy.

d. ensure the approved and appropriate security measures are in place and working as expected; and

e. support policy compliance and ensure that the DCJS Director of Audit Services is promptly informed of security incidents.

17. The Commissioner shall designate one Employee to act as the Terminal Agency Coordinator (TAC) for each segment of the Department operating under its own DCJS Use and Dissemination Agreement who shall:

a. be the point of contact for matters relating to Criminal History Record Information access;

b. administer Criminal History Record Information programs and oversee compliance with Criminal History Record Information systems policies;

c. maintain a complete, accurate, and current listing of all terminal operators and their user identifications together with copies of training and screening completion certificates;

d. notify DCJS when a user's access to Criminal History Record Information should be removed due to change in responsibilities or employment status or other reason; and

e. conduct periodic audits to ensure compliance with applicable regulations governing system use.

18. Sworn Members, Communications Operators, members of the Taxi & Limousine Commission designated by its Chairperson and other Employees as may be designated by the Commissioner are authorized to access Criminal History Record Information, provided that they have successfully completed such security screening procedures as may by required by DCJS.

19. Criminal History Record Information may be obtained only for the purposes permitted under the Use and Dissemination Agreement applicable to the Employee obtaining such information (see Appendix "A," attached).

20. Notwithstanding any contrary directive, Criminal History Record Information may not be disclosed by any Employee to another agency or individual unless specifically authorized by law.

21. When Criminal History Record Information is being used solely for licensing or employment background investigation:

a. the Criminal History Record Information shall be retained only for the duration of such investigation process, including any subsequent administrative or judicial appeal of denial of the license or employment and, thereafter destroyed in a secure manner to preclude unauthorized access or use;

NOTE: Pursuant to the above, Criminal History Record Information obtained for background investigation purposes shall be discarded by the Taxi & Limousine Commission, the Pistol Licensing Unit and Background Investigation Coordinator (relating to Department employment background investigations) within **five months** following an adverse determination.

b. the Commanding Officer of each Unit which has requested to receive reports of subsequent arrests of individuals who are the subject of a Criminal History Record Information inquiry shall, at least once per year, provide to DCJS:

i. the names and NYSID numbers of individuals whose fingerprints were sent to DCJS for identification processing and retention, but whose applications were not approved for employment or licensure by the Department; and

ii. the names and NYSID numbers of individuals who subsequently left the Department's employment or relinquished licensure.

RELATED PROVISIONS:

104.01 General Rules of Conduct

Appendix A
Authorized Inquiry Specification List

Agency Name: Westchester County Department of Public Safety

ORI Number: NY0590000

On-Line Inquiry Reason Code	Purpose of Inquiries	Enabling Authority
ARR	Can only be used by Police Departments / Agencies, Sheriff's Offices, or District Attorney's when criminal history record information is needed during arrest processing. Should not be used in lieu of an available fingerprint-based rap sheet.	Executive Law §837(6)
CJE	Can only be used to make non-finger printable inquiries for perspective employees (including vendors/contractors involved with the administration of criminal justice for the criminal justice agency), not current employees or visitors. An applicant fingerprint submission will ensure a definitive criminal history for the employee as well as provide the agency with a hit notice if the individual is arrested for a finger printable offense in New York State.	28 CFR 20.33 FBI NCIC Operating Manual
CRI	Can only be used by Police Departments / Agencies, Sheriff's Offices, District Attorney's or interstate cooperation with law enforcement officers and agencies of other states and the federal government, to request criminal history record information of an individual currently under investigation for a crime/alleged crime.	Executive Law §837(6)
DET	Can only be used by Police Departments / Agencies, Sheriff's Offices or Correctional Facilities to perform inquiries when a person is being detained but is not a sentenced offender. This includes offenders who are held under securing orders, but not a commitment order.	Executive Law 837(6)
DNA	Can only be used by Police Departments / Agencies, Sheriff's Offices, probation, parole, DOCCS, OCFS facilities, district attorney offices, and courts to verify charge information for DNA eligibility.	Executive Law 837(6)
GUN	Can only be used by Police Departments / Agencies, Sheriff's Offices, and courts in connection with firearm releases, permits, or renewals.	Penal Law §400.00(9) and (10)

Appendix A
Authorized Inquiry Specification List

Agency Name: Westchester County Department of Public Safety

ORI Number: NY0590000

HOU	Can only be used by Police Departments / Agencies or Sheriff's Offices to conduct a name-based search for a qualified Public Housing Authority (PHA). The law enforcement agency may advise the PHA if there is a hit, but may not provide a rap sheet to the PHA. If the PHA wishes to pursue this, they should submit civil fingerprints to DCJS.	Housing Opportunity Program Extension Act of 1996; Public Law 104-120
PDI	Can only be used by Police Departments / Agencies, Sheriff's Offices to request criminal history record information of an individual currently under investigation for a crime/alleged crime.	Executive Law §837(6)
WAR	Can only be used by Police Departments / Agencies, Sheriff's Offices, District Attorneys or Courts for investigations involving the issuance of a warrant or an individual's warrant status.	Executive Law §837(6)
	ARREST Adult Arrest Fingerprint Submission	Criminal Procedural Law (CPL) 160.10(1)
	ARREST Juvenile Arrest Fingerprint Submission	Family Court Act §306.1
	CORRECTION ADMISSION Correction Admission Fingerprint Submission	Correction Law §618(2)
	DCJS CRIMINAL INQUIRY 52B – 15 Days or Less Non-Finger Printable Amnesia Victim County Incar. > 1 Year Not Cons. Detention Inquiry Fugitive Inv ID Only Investigative Fingerprints Non-Finger Printable Charge Turnover to another Agency Violation of Probation Warrant Invest - PD. Sex Offender Registry	 Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) COR 6C SORA
	DCJS DEATH Death Fingerprint Card	Executive Law §837(6)

Appendix A
Authorized Inquiry Specification List

Agency Name: Westchester County Department of Public Safety

ORI Number: NY0590000

	NON CRIM FINGERPRINT CARD Police Officer Applicant Fingerprint Submission* Peace Officer Applicant Fingerprint Submission* Park Ranger Applicant Fingerprint Submission* Deputy Sheriff Applicant Fingerprint Submission* Police Department Employee Applicant Fingerprint Submission* (NY State and Federal CHRI response)	CPL 1.20 CPL 2.10 CPL 2.10 CPL 1.20 Executive Law §837-c
	NON CRIM FINGERPRINT CARD Non-Criminal fingerprint submissions pertaining to contractors, vendors, custodial workers and other support personnel with unescorted access to physically secure locations or controlled areas * (NY State and Federal CHRI response)	CJIS Site Security 5.12
	NON CRIM FINGERPRINT CARD Pistol License Fingerprint Submission* (NY State and Federal CHRI response)	Penal Law §400.00(4)

Remarks:
* Fingerprint processing fee required pursuant to Executive Law §837(8-a)

Agencies that are authorized to conduct a FBI fingerprint background check on an applicant (i.e. employment, license, permit, adoption) are obligated to ensure the applicant is provided certain notice. Refer to https://www.fbi.gov/services/cjis/compact-council for the following documents regarding the privacy protection of a non-criminal fingerprint submissions:

- Privacy Act Statement
- Guiding Principles: Agency Privacy Requirements for Noncriminal Justice Applicants
- Guiding Principles: Noncriminal Justice Applicants Privacy Rights

Appendix A

Authorized Inquiry Specification List

User Agency: Westchester County Taxi & Limousine Commission

ORI Number: NY059TL3Y

On-Line Inquiry Reason Code	Purpose of Inquiries	Enabling Authority
	NON CRIM FINGERPRINT CARD Non-criminal fingerprint submissions pertaining to the licensing of for-hire vehicles, drivers and base stations by Westchester County Taxi & Limousine Commission* (NY State CHRI response)	Westchester County Administrative Code Chapter 270 and Westchester County Local Law 9-1998
	NON CRIM FINGERPRINT CARD Non-criminal fingerprint submissions for employees who have access to NY State or Federal Criminal History Record Information (CHRI), whether hard copy or electronic form, in the course of their job duties* (NY State CHRI response)	9 NYCRR 6051.1(a)(3)

Remarks:
* Fingerprint processing fee required pursuant to Executive Law §837(8-a)

Agencies that are authorized to conduct a FBI fingerprint background check on an applicant (i.e. employment, license, permit, adoption) are obligated to ensure the applicant is provided certain notice. Refer to https://www.fbi.gov/services/cjis/compact-council for the following documents regarding the privacy protection of a non-criminal fingerprint submissions:

- Privacy Act Statement
- Guiding Principles: Agency Privacy Requirements for Noncriminal Justice Applicants
- Guiding Principles: Noncriminal Justice Applicants Privacy Rights