THE RUTHERFORD INSTITUTE

Post Office Box 7482
Charlottesville, Virginia 22906-7482

JOHN W. WHITEHEAD
Founder and President

TELEPHONE | 434 / 978 - 3888
EMAIL | staff@rutherford.org
www.rutherford.org

September 29, 2023

Via Email (council@charlottesville.gov)

Charlottesville Mayor and City Council
P.O. Box 911
Charlottesville, VA 22902

Re: Constitutional concerns about License Plate Recognition surveillance cameras

Dear Honorable Mayor and City Council:

At a time when growing numbers of unsuspecting Americans are being swept up into a massive digital data dragnet that does not distinguish between those who are innocent of wrongdoing, suspects, or criminals, The Rutherford Institute is particularly concerned about the Charlottesville Police Department's plans to implement a License Plate Recognition (LPR) system, if adopted, to "prevent, deter and solve crime."[1]

For the past 40-plus years, The Rutherford Institute has sounded the alarm whenever the government exceeded its authority, and has defended the rights of the citizenry in the face of governmental abuses.[2] As such, I can personally attest to the fact that nothing is ever as simple as the government claims it is, and unregulated or poorly regulated use of an AI-enabled system of mass surveillance cameras masquerading as crime prevention would be no exception.

Although preemptive precrime programs, driven by surveillance cameras and fusion centers, are popping up all across the country, they are not necessarily making communities any safer,[3] but they are endangering individual freedoms.[4] Indeed, while CPD may tout the supposed

[1] "CPD to Meet with Community Stakeholders to Discuss FLOCK Safety Program," Charlottesville Police News (Sept. 14, 2023), https://www.charlottesville.gov/CivicAlerts.aspx?AID=1544.
[2] The Rutherford Institute is a nonprofit civil liberties organization which seeks to protect individuals' constitutional rights and educate the public about threats to their freedoms.
[3] Jason Kelley And Matthew Guariglia, "Things to Know Before Your Neighborhood Installs an Automated License Plate Reader," *EFF* (September 14, 2020), https://www.eff.org/deeplinks/2020/09/flock-license-plate-reader-homeowners-association-safe-problems.
[4] Jonathan Hafetz, "Homeland Security's fusion centers show the dangers of mission creep," *The Hill* (Mar. 19, 2023), https://thehill.com/opinion/national-security/3900077-homeland-securitys-fusion-centers-show-the-dangers-of-mission-creep/.

benefits of Flock's LPRs in deterring and solving crime,[5] they are plagued by errors resulting in wrongful arrests and profiling of innocent individuals. As such, the potential threats posed by license plate readers to First and Fourth Amendment rights cannot be understated.

In the hands of government agents, these technologies can become a convenient tool to render null and void the Constitution's requirements of privacy and its prohibitions against unreasonable searches and seizures.

Background

Part of a public-private partnership program between police and the surveillance industry, license plate readers signal a turning point in the transition from a police state to a police-driven surveillance state. LPRs are mass surveillance tools that can photograph over 1,800 license tag numbers per minute, take a picture of every passing license tag number and store the tag number and the date, time, and location of the picture in a searchable database, then share the data with law enforcement, fusion centers and private companies to track the movements of persons in their cars.

Flock, one of the major players in the video surveillance industry which the City is specifically considering, has moved beyond merely capturing photographs of license plates to creating a vast surveillance network that crisscrosses the country, feeds data to interconnected, nationwide databases accessible by law enforcement, and combines that data with artificial intelligence and machine learning. According to the *Intercept*, "The company's 'vehicle fingerprint' technology goes beyond traditional models, capturing not only license plate numbers, but also the state, vehicle type, make, color, missing and covered plates, bumper stickers, decals, and roof racks."[6]

With LPR cameras installed in more than 1400 cities across the country, Flock claims to photograph more than a billion vehicles every month.[7] Affixed to overpasses, cop cars and throughout business sectors and residential neighborhoods, license plate readers can enable police to track vehicles and run the plates through law enforcement databases in search of stolen vehicles, shots fired calls, and homicides, as well as helping to locate missing, endangered, and wanted individuals,[8]

[5] "CPD to Meet with Community Stakeholders to Discuss FLOCK Safety Program," Charlottesville Police News (Sept. 14, 2023), https://www.charlottesville.gov/CivicAlerts.aspx?AID=1544.
[6] Georgia Gee, "License Plate Surveillance, Courtesy Of Your Homeowners Association," *The Intercept* (Mar. 22, 2023), https://theintercept.com/2023/03/22/hoa-surveillance-license-plate-police-flock/.
[7] Jay Stanley, "Fast-Growing Company Flock is Building a New AI-Driven Mass-Surveillance System," *ACLU* (Mar. 3, 2022), https://www.aclu.org/report/fast-growing-company-flock-building-new-ai-driven-mass-surveillance-system.
[8] "CPD to Meet with Community Stakeholders to Discuss FLOCK Safety Program," Charlottesville Police News (Sept. 14, 2023), https://www.charlottesville.gov/CivicAlerts.aspx?AID=1544.

The data can also be shared nationwide with other law enforcement agencies[9] and may be accessed by fusion crime centers.[10] And while the City claims the captured information will be automatically deleted after 30 days "in most cases,"[11] there is no guarantee that will be done.

Given that 83 percent of U.S. adults drive a car at least several times a week, this is a program that will have far-reaching ramifications for the entire population.[12]

LPR Surveillance Raises Significant First and Fourth Amendment Concerns

While LPRs can certainly be put to beneficial purposes, the data from these license plate readers—culled, uploaded, catalogued, analyzed by artificial intelligence programs, and combined with data pulled from other surveillance systems, aerial or otherwise—also allows government officials to identify and track individuals as they go about their personal lives, revealing intimate details relating to healthcare, mental wellbeing, relationships, religious practices, and lawful First Amendment activities such as attending political rallies and protests.

What this adds up to for government agencies that have access to such uploaded and integrated data (that is, FBI, NSA, DHS agents, etc., as well as local police) is a surveillance map that allows them to track someone's movements over time and space, which raises significant First and Fourth Amendment concerns.[13]

The U.S. Supreme Court's ruling in *Carpenter v. United States* recognized that a detailed history of a person's location reveals profoundly sensitive information.[14] Location information, the Supreme Court held, "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familiar, political, professional, religious, and sexual associations."[15]

---

[9] Jason Kelley And Matthew Guariglia, "Things to Know Before Your Neighborhood Installs an Automated License Plate Reader," *EFF* (September 14, 2020), https://www.eff.org/deeplinks/2020/09/flock-license-plate-reader-homeowners-association-safe-problems; Georgia Gee, "License Plate Surveillance, Courtesy Of Your Homeowners Association," *The Intercept* (Mar. 22, 2023), https://theintercept.com/2023/03/22/hoa-surveillance-license-plate-police-flock/.

[10] Joseph Cox, "Inside 'TALON,' the Nationwide Network of AI-Enabled Surveillance Cameras," *Vice* (Mar. 3, 2021), https://www.vice.com/en/article/bvx4bq/talon-flock-safety-cameras-police-license-plate-reader.

[11] "CPD to Meet with Community Stakeholders to Discuss FLOCK Safety Program," Charlottesville Police News (Sept. 14, 2023), https://www.charlottesville.gov/CivicAlerts.aspx?AID=1544.

[12] Ángel Díaz and Rachel Levinson-Waldman, "Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use," *Brennan Center* (Sept. 10, 2022), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations.

[13] Jon Schuppe and Bracey Harris, "Police in Jackson, Mississippi, want access to live home security video, alarming privacy advocates," *NBC News* (Dec. 2, 2020), https://www.nbcnews.com/news/us-news/police-jackson-mississippi-want-access-live-home-security-video-alarming-n1249566.

[14] *Carpenter v. United States*, 138 S. Ct. 2206, 2217-20 (2018).

[15] *Id.* at 2217 (internal quotation marks omitted).

Cell-site location information (CSLI)—the particular type of location information at issue in *Carpenter*—is "detailed, encyclopedic, and effortlessly compiled," it creates a "tireless and absolute surveillance," and its "retrospective quality" gives police access to information "otherwise unknowable."[16] For these reasons, the Supreme Court ruled that collection of CSLI for a seven-day period "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[17]

The same features that make CSLI collection so invasive are present in equal, if not greater, measure in LPRs. These LPR systems—both on their own, and in conjunction with other surveillance techniques—can create a "detailed, encyclopedic" record of the movements of a town's residents. Their "retrospective quality" allows law enforcement to look back in time to track those residents. And the LPR program "runs against everyone" in a community; no one can "escape this tireless and absolute surveillance."

In other words, an LPR program automatically creates a detailed, daily, historical record of the location information for the population of an entire American city. Yet as the U.S. Supreme Court has recognized, surveillance technologies that collect detailed records about people's movements infringe on individuals' reasonable expectations of privacy.[18]

Moreover, these wall-to-wall surveillance systems chill free speech and assembly in public places, raising serious First Amendment concerns. They have all but eliminated the notion of privacy and radically re-drawn the line of demarcation between our public and private selves.

LPRs Conduct Warrantless Searches which might Violate the Fourth Amendment

Some surveillance systems are designed with the layering of surveillance tools specifically in mind. There is no shortage of such surveillance tools, from state-of-the-art CCTV cameras and "public-private" networks of surveillance cameras (private cameras operated from an individual's home or small business that police can access when a "public safety" event occurs) to facial recognition technology, public and social media databases, and fixed and mobile automated license plate readers.

Whether considered on its own or in conjunction with other surveillance tools, LPR's persistent, expansive reach is undeniably invasive and runs contrary to the Fourth Amendment. As explained by the Supreme Court, a "central aim" of the Fourth Amendment is "to place obstacles in the way of a too permeating police surveillance" and to "assure preservation of that degree of privacy against government that existed" when the Amendment was adopted.[19]

But the LPR program dramatically reduces the degree of privacy afforded every citizen. Supreme Court precedent is clear that "warrantless searches are typically unreasonable where a

[16] *Id.* at 2216, 2218.
[17] *Id.* at 2219.
[18] *Id.*
[19] *Id.* at 2214.

search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing."[20] Exceptions to that rule are "jealously and carefully drawn."[21] Any special need justifying a suspicionless search must be beyond the normal need for law enforcement.[22]

In *City of Indianapolis v. Edmond*, the Supreme Court struck down a municipal vehicle checkpoint program that was directed at interdicting illegal drugs.[23] The Court's opinion shows that "programs undertaken to 'detect evidence of ordinary criminal wrongdoing, even where the 'gravity of the threat' is high, cannot be justified as a special need."[24] Thus, crime control—even where crime rates are high—cannot justify a program of warrantless, suspicionless searches.

There is only one possible understanding of a LPR program: it is a law-enforcement investigative and crime-control tool. The "special needs" justification, therefore, simply does not apply.

A Warrantless Mass Surveillance System Is Ripe for Abuse

Any system of mass surveillance that feeds into national databases and can be warrantlessly accessed by police is ripe for abuse, especially as it relates to protected First Amendment activities. Reports indicate that fusion centers, which feed surveillance information to law enforcement at federal, state, and local levels, may well be among those gaining access to LPR data systems.[25]

For instance, an investigative report by the Brennan Center found that "[o]ver the last two decades, leaked materials have shown fusion centers tracking protestors and casting peaceful activities as potential threats. Their targets have included racial justice and environmental advocates, right-wing activists, and third-party political candidates."[26]

One fusion center in Maine was found to have been "illegally collecting and sharing information about Maine residents who weren't suspected of criminal activity. They included gun purchasers, people protesting the construction of a new power transmission line, the

[20] *Id.* at 2221 (internal quotation marks omitted).
[21] *Jones v. United States*, 357 U.S. 493, 499 (1958).
[22] *See Delaware v. Prouse*, 440 U.S. 648, 659 n.18 (1979) (observing that a "special need" must be justified by something beyond "the general interest in crime control").
[23] *City of Indianapolis v. Edmond*, 531 U.S. 32, 48 (2000).
[24] Rachel Levinson Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 Emory L. J. 527, 591 (2017) (quoting *Edmond*, 531 U.S. at 41-42).
[25] Joseph Cox, "Inside 'TALON,' the Nationwide Network of AI-Enabled Surveillance Cameras," *Vice* (Mar. 3, 2021), https://www.vice.com/en/article/bvx4bq/talon-flock-safety-cameras-police-license-plate-reader.
[26] Michael German, Rachel Levinson-Waldman, and Kaylana Mueller-Hsia, "Ending Fusion Center Abuses," *Brennan Center for Justice* (Dec. 15, 2022), https://www.brennancenter.org/our-work/policy-solutions/ending-fusion-center-abuses.

employees of a peacebuilding summer camp for teenagers, and even people who travelled to New York City frequently."[27]

In one Florida county, police have been using their precrime program to generate "lists of people it considers likely to break the law, based on arrest histories, unspecified intelligence and arbitrary decisions by police analysts."[28] Then, according to the *Tampa Bay Times*, deputies are deployed "to find and interrogate anyone whose name appears, often without probable cause, a search warrant or evidence of a specific crime. They swarm homes in the middle of the night, waking families and embarrassing people in front of their neighbors. They write tickets for missing mailbox numbers and overgrown grass, saddling residents with court dates and fines. They come again and again, making arrests for any reason they can."[29]

Even if LPRs and other surveillance cameras are implemented with good intentions and significant restrictions on their use, once that infrastructure is in place, it can be subject to extreme abuse in the future. For example, a program in China called "Sharp Eyes" was implemented "to connect the security cameras that already scan roads, shopping malls and transport hubs with private cameras on compounds and buildings, and integrate them into one nationwide surveillance and data-sharing platform."[30] A researcher for Chinese Human Rights Defenders stated that the Chinese "government treats human rights activists, lawyers and ethnic Uighurs and Tibetans as criminals, and these people are being caught, jailed and possibly tortured as a result of this technology.[31]

Similarly, "police in Iran installed cameras in public places to identify women who are breaking the law by not wearing a hijab" and the women will be placed under arrest for a second offense.[32] Creating an infrastructure of mass surveillance which can be abused like this is not what free societies should do.

<u>Far From Infallible, LPR Technology Is Riddled with Errors and Ripe for Abuse</u>

---

[27] Michael German, "How Government Fusion Centers Violate Americans' Rights — and How to Stop It," *Brennan Center for Justice* (Dec. 15, 2022), https://www.brennancenter.org/our-work/analysis-opinion/how-government-fusion-centers-violate-americans-rights-and-how-stop-it.
[28] Kathleen McGrory and Neil Bedi, "Targeted," *Tampa Bay Times* (Sept. 3, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/.
[29] Kathleen McGrory and Neil Bedi, "Targeted," *Tampa Bay Times* (Sept. 3, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/.
[30] Simon Denyer, "China's watchful eye," *The Washington Post* (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/.
[31] Simon Denyer, "China's watchful eye," *The Washington Post* (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/.
[32] Matt Novak, "Iran Installs Cameras For Morality Police To Identify Women Defying Hijab Law," *Forbes* (Apr. 8, 2023), https://www.forbes.com/sites/mattnovak/2023/04/08/iran-installs-cameras-for-morality-police-to-identify-women-defying-hijab-law/?sh=f7fc28451657.

While the predatory effect of surveillance cameras has also yet to be fully addressed, some could be vulnerable to being hacked by third parties and abused by corporate and government employees alike.[33] In fact, one police officer was found to have used LPRs to track his estranged wife.[34] Additionally, the LPR technology and its use by human handlers is not infallible. Reports indicate the license plate scanning technology misidentifies one plate out of every ten, resulting in innocent people being detained by police, sometimes at gunpoint.

For instance, a black woman and four young children ages 6, 12, 14 and 17 were stopped by police, ordered out of the family's SUV at gunpoint, and handcuffed facedown in a parking lot after police acted on information from a license plate reader system, believing the vehicle to be stolen. As the *Denver Post* reported, "The police officers who mistakenly believed the car was stolen...failed to check information they'd received from a license-plate reader that showed it was a motorcycle with Montana plates that had been reported stolen, not an SUV with Colorado plates. While the SUV had the same plate number as the stolen motorcycle, it was completely uninvolved."[35]

Government Surveillance Creates a Suspect Society, Can Give Rise to Profiling

By subjecting Americans to surveillance without their knowledge or compliance and then storing the data for later use, the government has erected the ultimate suspect society. In such an environment, there is no such thing as "innocent until proven guilty."

LPRs also lay the groundwork for profiling based on the opinions expressed on vehicle bumper stickers and decals, which are highly personal forms of expression protected by the First Amendment.[36] Concerns have also been raised about the use of the license plate readers to track people "accessing abortion in states where it is illegal or crossing state lines to do so."[37]

Like many other mass surveillance technologies, these license plate surveillance systems have also been shown to have a disparate effect on minorities and underprivileged communities. In Electronic Frontier Foundation's review of license plate reader usage by Oakland, Calif., they were found to have been disproportionately used in low income and heavy minority population

[33] Brian X. Chen, "Your Doorbell Camera Spied on You. Now What?" *The New York Times* (Feb. 19, 2020), https://www.nytimes.com/2020/02/19/technology/personaltech/ring-doorbell-camera-spying.html.
[34] Georgia Gee, "License Plate Surveillance, Courtesy Of Your Homeowners Association," *The Intercept* (Mar. 22, 2023), https://theintercept.com/2023/03/22/hoa-surveillance-license-plate-police-flock/.
[35] Shelly Bradbury, "Family sues Aurora police over botched stolen-car response that left children handcuffed, held at gunpoint," *Denver Post* (Jan. 25, 2021), https://www.denverpost.com/2021/01/25/brittney-gilliam-lawsuit-aurora-police/.
[36] Georgia Gee, "License Plate Surveillance, Courtesy Of Your Homeowners Association," *The Intercept* (Mar. 22, 2023), https://theintercept.com/2023/03/22/hoa-surveillance-license-plate-police-flock/.
[37] Georgia Gee, "License Plate Surveillance, Courtesy Of Your Homeowners Association," *The Intercept* (Mar. 22, 2023), https://theintercept.com/2023/03/22/hoa-surveillance-license-plate-police-flock/.

areas. LPRs could also be used in the search for undocumented persons residing in the United States,[38] suggesting a certain level of profiling would need to be undertaken for such a venture.

Certainly, in an age when the government has significant technological resources at its disposal to not only carry out warrantless surveillance on American citizens but also to harvest and mine that data for its own dubious purposes, whether it be crime-mapping or profiling based on whatever criteria the government wants to use to target and segregate the populace—including race, religion or politics—the potential for abuse is grave.

Conclusion

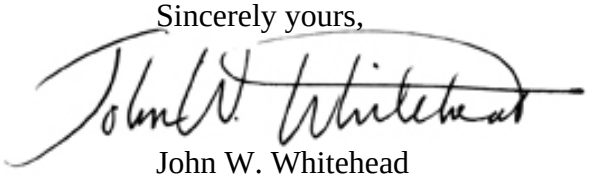
While the Fourth Amendment was created to prevent government officials from searching an individual's person or property without a warrant and probable cause—evidence that some kind of criminal activity was afoot—the founders could scarcely have imagined a world in which we needed protection against government breaches of our privacy on such a widespread, automated level.

Any attempt by a government agency to establish a system by which the populace can be targeted, tracked and singled out must be met with extreme caution. Therefore, in the hopes that Charlottesville will remain committed to the principles of transparency, accountability and privacy, we urge the City Council to oppose the adoption of any license plate readers in recognition of the potential dangers posed by governmental overreach, data leaks, and invasion of privacy.

At a minimum, should the City Council allow police to adopt an LPR system, thereby prioritizing mass surveillance disguised as precrime initiatives over the rights of the citizenry, there must be assurance that contracts will be written in such a way as to ensure that the systems are severely limited in their mass surveillance and data-sharing capabilities.

Should you have any questions about our concerns regarding these mass surveillance devices or require The Rutherford Institute's assistance in determining how best to balance security with constitutional safeguards, please don't hesitate to contact us.

Sincerely yours,



John W. Whitehead
President

[38] Georgia Gee, "License Plate Surveillance, Courtesy Of Your Homeowners Association," *The Intercept* (Mar. 22, 2023), https://theintercept.com/2023/03/22/hoa-surveillance-license-plate-police-flock/.