AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

ACLU OF RHODE ISLAND COMMENTARY ON PROPOSED PROVIDENCE POLICE DEPARTMENT POLICY ON "AUTOMATED LICENSE PLATE READERS"
July 2022

The ACLU of Rhode Island offers the following commentary on the draft "Automated License Plate Readers (ALPR)" policy as put forth by the Providence Police Department.[1]

As the Department is aware, the ACLU has, since the implementation of Flock Safety cameras began in various municipalities across Rhode Island in August of 2021, consistently opposed their installation and expressed serious concerns about the impact that this surveillance system would have on privacy, the public oversight of policing tools, First Amendment rights, and racial disparities in law enforcement. These issues were addressed in a letter sent by our organization to the Providence City Council on March 17, 2022, and they remain. For convenience, a copy of our earlier letter is attached to this commentary.

In addition, we continue to believe that, if this technology is nonetheless going to be implemented, it must be subject to restrictions *codified in ordinance* or statute, rather than solely through easily amendable departmental policy, to guarantee their enforceability. Only in this way can there be better assurances for robust protections and restrictions that allow for public security and oversight and minimization of harm to privacy rights and, just as importantly, for the availability of appropriate remedies for any violations.

[1] While we appreciate that this policy is going through a public review process, it is unclear to us how widely known it is to the general public that this process is occurring and of their opportunity to provide comments to the Department. We believe additional time should be provided for public comments and greater pro-active measures taken by the City to inform residents of this proposal. We say this while still firmly believing that setting standards on the use of a surveillance system like this should be in the hands of the City Council, not the police department.

With these caveats in mind, we offer below both general and specific concerns about the proposed policy. Unfortunately, we find it woefully deficient in numerous respects and believe it needs substantial revisions in order to protect the privacy of residents, prevent misuse of the system, and promote meaningful transparency.

- **Data Storage and Security**

  This policy puts a maximum storage time for any data collected through an ALPR at 30 days, and notes that the "ALPR vendor," or Flock Safety, will also "purge their data at the end of the 30 days of storage." Though timely and consistent deletion of data is critical, we particularly question here the security of placing such expansive and sensitive data in the hands of a private company, which may change their policies at any time and has no statutory oversight on their own responsibilities to the data that is collected.[2]

  The urgency of this problem is not hypothetical, as recent events illustrate its saliency. Mere days ago, the United States Supreme Court issued a decision that overturned *Roe v. Wade* and stripped away the constitutional right to abortion. Even before this decision came out, digital and data privacy experts noted their concerns about the way that data could be weaponized against residents who now live in one of the many states in which abortion has already been or will imminently be banned and criminalized. Notably, for residents who must now travel out-of-state for a procedure, the implementation of a widespread surveillance system – for which residents have no actual guarantee of data security or privacy – could have severe consequences.

[2] Section F.2 of the policy refers to storing data in accordance with state Records Retention Schedule LG6. It is unclear to us which particular schedule in LG6 would apply to data like this. Depending on the analogous record chosen, the Department could claim the ability to store the information for a much longer period than 30 days. In fact, Section F.3 specifically allows the Department to maintain vehicle data for longer than 30 days, so it is unclear to us exactly how meaningful this purported 30-day deletion standard, designed to protect privacy, truly is.

Imagine an Ohio resident who has family in Rhode Island and travels here to receive an abortion for that reason. Nothing prevents Flock Safety from analyzing patterns of out-of-state travel and the locations of those vehicles, and then selling that data or providing it to law enforcement officials in other states. In fact, "states that choose to criminalize abortion can start buying…consumer data…to prosecute people who get an abortion, provide an abortion or even aid someone else in obtaining an abortion."[3] This risk is not paranoid or speculative – it is instead rooted in the extraordinary violations that can and have occurred when unregulated data is provided to a private company which is under no legal obligation to maintain responsible data policies.

In addition, to the extent a request for motor vehicle information to enforce an anti-abortion statute came from a law enforcement agency in another state, nothing in the policy would hamper the Providence Police Department itself from sharing relevant information with that state. To the contrary, the policy authorizes release of the data for any "legitimate law enforcement purposes" [Section G.4], which would encompass the criminal abortion scenario noted above. The above example is provided to show how high the stakes are of collecting enormous amounts of public data as this surveillance technology does.

Even worse, the policy allows for the release of data not just for official law enforcement purposes, but "as otherwise permitted by law." [Section I.1] Since no statutory safeguards governing this type of surveillance currently exist, just about *any* release of the data would be "permitted by law." We hope that the City recognizes how insufficient these retention and deletion provisions are in light of the profound violations which can occur from the inappropriate use of this data.

[3] https://www.msnbc.com/opinion/msnbc-opinion/states-abortion-bans-can-weaponize-your-own-data-against-you-n1296591

- **Breadth of the Technology and Lack of Limitations on Use**

One of our organization's primary concerns with the installation of Flock Safety cameras is how proponents avoid descriptions of the technology that candidly describe the sheer breadth of what the technology can do. Unlike other ALPR systems, such as speed cameras or toll cameras, Flock Safety cameras are not solely limited to the capturing of a license plate nor is their use limited to a specific and narrow purpose. We believe any policy should not only make clear what the capacities of the system are, but what the limitations are on law enforcement officials in making use of the various capabilities of the cameras.

For example, Flock Safety's surveillance system allows the police to search by "vehicle type, make, color, license plate state, missing/covered plates, and other unique features like *bumper stickers*, decals, and roof racks."[4] (emphasis added) Flock Safety's website also advertises the ability to not only search by these aesthetic characteristics but additionally by "audio evidence" and "contextual evidence," which includes "screeching tires" and "associated vehicles,"[5] implying that these systems can capture audio in addition to video and utilize artificial intelligence to determine which vehicles in a certain area may be linked to one another. Both of these uses, beyond the already invasive capabilities of the video capturing, represent a profound overreach of this technology and invite over-policing and an inappropriate broadening of surveillance techniques.

Yet, most of these abilities are not specifically addressed in, much less prohibited by, this policy. We believe that to be a significant deficiency, both in failing to place

[4] https://www.flocksafety.com/lpr-vehicle-recognition/
[5] https://www.flocksafety.com/

reasonable restrictions on the use of this technology and failing to truly promote public transparency and oversight. Ultimately, the policy is misleading if its language does not explicitly and comprehensively acknowledge the extent of surveillance it is authorizing or attempting to circumscribe.

Then again, it appears that the policy is really not meant to circumscribe. It's not just the misleading nomenclature of "license plate readers" that is troubling; it's the various uses to which the technology will be put that gets seriously underplayed as well. By being available to "gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, stolen property recovery and active criminal investigations," [Policy, page 1] – and even more amazingly, by being available for use "with any routine patrol operation or criminal investigation" without *any* requirement of reasonable suspicion or probable cause [Section B.3] – meaningful restrictions on the actual use of this technology are truly illusory.

Indeed, throughout the policy, the breadth of its intended use is consistently emphasized. The section on "Investigative Personnel Responsibilities" encourages access to the database for helping to identify suspects allegedly involved in any type of criminal activity or anybody deemed a "person[] of interest." [Section D.1] The data can be accessed not only for a "specific criminal investigation," but also for any "department-related civil or administrative action," whatever that means. [Section G.3.]

- **"Permitted/Impermissible Uses"**

Section E of the policy attempts, rather weakly, to address two key issues which have concerned our organization from the outset by noting that it is "a violation of this

policy to use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law" and that it is a "violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights." [E.3 and E.5]

We appreciate the acknowledgement that the Flock Safety cameras may facilitate First Amendment violations or discriminatory policing. However, we find that the provisions to prevent it are lacking in sufficient protection, and they do not address the full spectrum of the impact that this surveillance may have on these important issues.

First, a bar on using the ALPR system based *solely* on a protected characteristic does not acknowledge the disparate approaches by which this system may be used in a racially or otherwise discriminatory manner. In the analogous context of the state's ban on "racial profiling," the term is defined as "disparate treatment of an individual on the basis, *in whole or in part*, of the racial or ethnic status of such individual…" R.I.G.L. § 31-21.2-3. It is defined that way in recognition that it is too easy for police to come up with an extraneous supplemental factor to circumvent allegations of discrimination.

In addition, this provision does not stop the Department from placing a higher concentration of cameras in lower income neighborhoods or communities of color, both of which have shouldered the brunt of surveillance policing for decades. In fact, the policy hints that that is exactly what it plans to do, by mentioning that placement of the cameras "shall be determined by crime analysis data and severity" [Policy, page 1], a way of relying on the notion of "high crime neighborhoods" to justify questionable police practices in a variety of contexts. Should this system be expanded to include facial recognition

technology in the future – again, something that the policy does not in any way foreclose – this language does not prevent its use based on the racially discriminatory features of these types of artificial intelligence technologies.

Similarly, simply banning use of the system "for the purpose or known effect of infringing upon First Amendment rights" does not necessarily prevent it from being used in ways that impact the exercise of these rights. If a small group of people engage in illegal acts during an otherwise peaceful protest, will Flock Safety be used to try to find the perpetrators? If so, police could use the system to track literally hundreds of motor vehicles (and their owners) at the protest, yet police could claim that such an activity would not violate the policy, since its "purpose" is not to infringe on First Amendment rights, and it is not "known" that its effect will do so either.

In a separate section [Section I.3], the policy purports to limit the sharing of data for immigration enforcement, but it does not actually do so. The policy fails to explain how, for example, Flock Safety-collected information provided to the FBI could not then be transferred by that agency to a federal entity like ICE for immigration enforcement purposes. The shakiness of this guarantee is further demonstrated by the policy's explicit acknowledgement that information will be gathered – and presumably shared – for "homeland security" purposes [Policy, page 1], which could include immigration enforcement.

- **Disciplinary Standards and Remedies**

The policy addresses the need for training of any law enforcement officer who accesses or uses the system, and establishes a variety of "impermissible" uses, but any

perceived remedies are largely toothless. While administrative sanctions "consistent with the collective bargaining agreement and department policies" can be administered [Section E.6], we know that this likely means, at most, a two-day suspension of a police officer to avoid drawn-out LEOBOR proceedings. And because this is merely an internal policy, rather than an ordinance or statute, any victim of a violation of the policy will have no meaningful judicial remedies to pursue independently. The policy mentions the possibility of criminal prosecution or civil liability, but fails to explain the crime that has been committed by violating the policy or from where a civil remedy would arise.

Another purported effort at accountability is the establishment of an auditing process [Section H]. But there is no provision authorizing public access to the findings of these audits, including of "data errors found." Thus, the extent of errors in, or misuse of, the system will remain hidden from any public scrutiny, making this hardly an accountability mechanism at all. It is sheer folly to believe that this database system will not be abused, but nothing in the policy gives assurance to the public that problems will be dealt with in any meaningful way.[6]

While we maintain the position overall that any implementation of these surveillance tools puts communities and residents at risk of gross privacy violations and has the capacity to inappropriately exacerbate existing disparities in policing, we urge that this policy at least be substantially amended to better address the realities of the surveillance system that Providence residents will soon be subject to and incorporate various limits on its use. In addition to addressing

[6] We have seen similar non-compliance by police officers with the Department's "body worn camera" policy, another policy purportedly designed to promote transparency and accountability. Meaningful disciplinary action against those officers has been non-existent, and we are not sanguine that there would be any different response here.

the various detailed concerns we have cited, we would suggest it include specific protections similar to those contained within 22 – H 7507 and 22 – S 2650, legislation introduced in the Rhode Island legislature this year to address this technology. A revised version of this policy should be resubmitted for further public comment.

More importantly, if the police department is serious in wanting to implement a surveillance technology like this while protecting the rights of its residents, it should join us in calling upon the City Council to adopt an ordinance that establishes the protections and remedies that are missing from this policy.

Community safety is a critical goal, but 24/7 surveillance of residents should not be a precondition for the safety that all of us seek. Though we believe that this policy must be amended, we also would urge instead the investment of the police department and the City in tangible supports that uplift and support residents rather than the implementation of largely unregulated and expansive policing and surveillance technology.

We appreciate the opportunity to provide this testimony, and thank you for your consideration of our views.

Submitted by:

Steven Brown, Executive Director
Hannah Stern, Policy Associate

AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

ATTACHMENT

March 17, 2022

Members of the Providence City Council
Providence City Hall
25 Dorrance Street
Providence, RI 02903

VIA MAIL AND EMAIL

Dear City Councilors:

At a state legislative hearing on March 10th, Chief Michael Winquist of the Cranston Police Department remarked that the Providence Police Department is actively pursuing the installation of deceptively-named automated license plate reader (ALPR) camera systems, operated by the private company Flock Safety, throughout the city. We write to you today with our deep concerns about this potential implementation.

While the ACLU of Rhode Island certainly understands the importance of public safety, the approach to safer communities cannot and should not include the use of technologies – like these cameras – which raise serious privacy issues, carry the clear potential for expanded surveillance and discriminatory implementation, and operate with absolutely no statutory safeguards in place. We urge you to reject the use of the cameras and to instead adopt an ordinance that will set standards for the deployment of any future law enforcement surveillance technology.

Though our organization has substantive concerns about the actual technology of these cameras, we are just as distressed by the possibility that these surveillance systems would be implemented without the concurrent introduction of statutory safeguards and limitations for their use. We wish to provide some context as to why the ACLU believes that Providence should reject the use of these cameras and any future implementation of surveillance technology without clear and strict safeguards.

• **The cameras capture much more than license plate numbers**. The use of other automated license plate reader systems in the state – such as those utilized for tolling purposes or to monitor traffic light violations – have generally been contained to capturing only the license plate on a vehicle, and only for a specific and narrow purpose. When the implementation of Flock Safety cameras in other municipalities began, police representatives initially assured the average motorist that they need not be worried because police are alerted only if a car's license plate number matches information in a federal national criminal database, known as the NCIC, or Amber/Silver Alert systems. This is extremely misleading.

Even leaving aside the well-known inaccuracies of the NCIC database and the problems that alone can cause, it is clear now – through the admission of the police departments – that these systems are not as narrowly tailored as residents might expect or anticipate.

As noted by both the marketing materials for these cameras and the police chiefs of the municipalities that have instituted this system, investigators may input a wide variety of vehicle characteristics into the system which range far beyond license plates. The website of Flock Safety, the company responsible for the cameras, explains further what this means: its surveillance system allows police to search by "*vehicle type*, make, color, license plate state, missing/covered plates, and other unique features like *bumper stickers*, decals, and roof racks."[7] (emphasis added) Such technological capabilities are incredibly invasive and far beyond what one conceives of when considering a technology often described as an "automated licensed plate reader."

Further, as the reference to "searches" suggests, the system does not merely operate passively. The police have the ability to input any license plate number – and presumably vehicle characteristics such as those noted above – and obtain information about a vehicle's whereabouts, if captured by a camera, for the preceding 30 days. In addition, that search will encompass photos not only from Providence, but also from any of the other municipalities that are part of the system, allowing for a statewide system of surveillance.

Based on the representation that the alert process is only triggered by motor vehicles associated with criminal activity and that innocent motorists thus have nothing to fear, one would assume that camera alerts would be few and far between. Yet, according to the "transparency portal" set up for the Cranston Police Department, those cameras have taken photographs of over *four-hundred thousand cars* within the last thirty days, information that will then be accessible for police searches for that same timeframe.[8]

At the same time, the positing that these cameras operate solely based on the visual capturing of information is also misleading. Flock Safety's website advertises the ability to not only search by the aesthetic characteristics listed above but additionally by "audio evidence" and "contextual evidence," which includes "screeching tires" and "associated vehicles,"[9] implying that these systems can capture audio in addition to video and utilize artificial intelligence to determine which vehicles in a certain area may be linked to one another. Both of these uses, beyond the already invasive capabilities of the video capturing, represent a profound overreach of this technology and invite over-policing and an inappropriate broadening of surveillance techniques.

• **It is almost inevitable that the use of these cameras will expand over time to engage in more, and more intrusive, types of surveillance**. The history of surveillance technology in this country – from wiretaps to stingrays to cameras to drones – has been a history of ever-growing uses, and those expanded uses are then used to justify and normalize even greater intrusions on privacy. Indeed, just this argument has been made in attempting to dismiss privacy concerns associated with the installation of these cameras by noting the prevalence of camera surveillance in *other* contexts. This is how our expectations of privacy become minimized and more Orwellian.

Flock Safety's cameras exemplify this "mission creep." Just a few months ago, the company announced the availability of "advanced search" features for its camera systems that will:

---

[7] https://www.flocksafety.com/lpr-vehicle-recognition/
[8] https://transparency.flocksafety.com/cranston-ri-pd
[9] https://www.flocksafety.com/

- Allow police to upload a picture of a vehicle from any source and then perform a search to see if any of the cameras have seen it;
- Allow police to enter a license plate number, and then search cameras to find vehicles that frequently travel with that vehicle, to "help identify accomplices to crimes"; and
- Give police the ability to search for vehicles that have been in multiple specified locations recently.[10]

Even if not being used in these more expansive ways today, the potential capabilities of this program are not as narrow as simply identifying and cross-checking license plate numbers, and *no state law or municipal ordinance currently prevents expanded uses in the future*. The chilling effects of the ability to track individuals in all these manners cannot be understated.

• **Separating the history of surveillance in the United States from racial discrimination is impossible because they are inextricably bound.** Communities of color in particular have most disproportionately experienced the egregious effects of expanded police surveillance activities, and this is not purely an historical lesson. In the last two years alone, First Amendment rights and racial discrimination have been entwined with the expanded use of surveillance tools. For example, municipal law departments were found to have used surveillance camera footage to inappropriately monitor activists during the Black Lives Matter protests of summer 2020.[11] In short, the abuse of surveillance technology is not hypothetical. Given the swath of current capabilities that Flock Safety advertises – and the ones which it could add in the future – we are extremely concerned that this technology could facilitate similar police activity in Providence, targeting both communities of color and protected protest activities.

• **Concerns about the normalization of increased surveillance are exemplified by the fact that some police departments have admitted that both they and Flock Safety have begun engaging in private outreach to business to develop a public-private network of these surveillance cameras.[12]** The solicitation of private partnership, for the facilitation of expanded police activity and presence, signifies an extraordinarily troubling development. An increased network of privately owned cameras for police purposes would not only provide significantly less oversight to the community regarding their actual use; it further flouts basic tenets of governmental transparency, accountability, and responsibility by creating a network of police-generated surveillance using private sources. This outreach also undermines any notion that use of these cameras is intended to be, or will stay, a limited use system. Instead, it is clearly being considered in some quarters as a significant method of future widening of policing surveillance activities.

• **In the absence of legislatively established limits on their use, the privacy rights of the public remain at the complete discretion of the police department and a private company, which can change their policies at any time.** No matter what assurances of privacy are given in policy – by either a police department or Flock Safety – there are no meaningful constraints on their ability to change the rules at any time. Today we may be told, for example, that all photos will be destroyed after 30 days, but nothing prevents the agencies or the company six months from now from extending it to 60 days, a year or a decade. The same is true for any other "safeguards" offered exclusively by police departmental policy or Flock Safety guidelines.

---

[10] https://www.govtech.com/biz/flock-safety-gives-users-expanded-vehicle-location-abilities
[11] https://www.npr.org/2021/08/20/1029625793/black-lives-matter-protesters-targeted
[12] https://www.warwickri.gov/sites/g/files/vyhlif1391/f/agendas/bid_package_2-23-2022.pdf

When police surveillance techniques like these ALPRs are promoted, they often imply a false choice between public safety and privacy. But public safety is the result of community-based tools and systems that directly and tangibly support residents – it is not, and has never been, a consequence of indiscriminate 24/7 surveillance. To suggest that such surveillance technology is only a threat to those committing crimes is dismissive of the legitimate privacy concerns that all residents have, and particularly ignores how police surveillance over the decades has often targeted communities in a racially discriminatory manner.

While the above are detailed concerns directly related to Flock Safety's cameras and the specific implementation of them in your municipality, we wish to emphasize that all surveillance technology has the capability to encourage, intentionally or not, more aggressive and unduly invasive policing and foster community distrust in policing systems. We call upon the City Council to reject the implementation of Flock Safety cameras in Providence and to further enact an ordinance that promotes community engagement, oversight, and extensive transparency for any future potential law enforcement surveillance technology.

Thank you for your consideration of these concerns. If you have any questions about our views, please feel free to let us know.

Sincerely,

Steven Brown
Executive Director

Hannah Stern
Policy Associate

cc: Mayor Jorge Elorza
Commissioner of Public Safety Stephen Paré
Police Chief Hugh Clements
Ferenc Karoly, Providence External Review Authority
Acting City Clerk Tina Mastroianni