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 THE PROPOSED PILOT PROGRAM FOR USE OF "AUTOMATED LICENSE PLATE READERS" AND PROPOSED PORTSMOUTH POLICE DEPARTMENT POLICY ON THE TOPIC

July 11, 2022

The ACLU of Rhode Island appreciates the opportunity to provide commentary on the reconsideration of the one-year pilot program for Automated License Plate Readers (ALPRs) on the Mt. Hope Bridge, and the Council's willingness to engage in that reconsideration. We respectfully ask the Council to rescind its approval of the program.

As the Council may be aware, our organization has consistently opposed the installation of these surveillance cameras, owned and operated by Flock Safety, in various municipalities across the state. In particular, we have 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.

While we strongly urge the Council to summarily reject the installation of these cameras in Portsmouth, we further believe that, if this technology is going to be implemented, it must be subject to restrictions *codified in ordinance* or statute, rather than solely through easily amendable police department policy, to guarantee their enforceability. We note this with the recognition that the Portsmouth Police Department has released a draft internal ALPR policy, which we discuss in more detail below. However, only through ordinance can there be concrete assurances of robust protections and restrictions that allow for public security and oversight, minimization of harm to privacy rights and, just as importantly, the availability of appropriate remedies for any violations.

While we understand that the question before the Council tonight is specifically whether this one-year pilot program should be approved, the program's guidelines would, from our current understanding, likely arise from this draft policy of the Police Department. For those reasons, our commentary specifically addresses how deficiencies within this policy underscore both the importance of an ordinance to regulate this type of technology and the dangers of entering into a program like this with only minimal enforceable safeguards. We therefore urge this Council to vote down this pilot program, and to instead enact an ordinance which will provide more meaningful protections than the proposed policy for any future considered use of surveillance tools.

Before delving into the particulars of the police department's draft policy, we believe one other point is worth highlighting. The use of this technology has been sold to the Council and the public as an important tool for addressing suicide prevention. At bottom, though, the use of such an expansive and intrusive – and truly Orwellian – surveillance system like Flock Safety strikes us as an incredibly ineffective and inefficient way to achieve that goal, especially when a much more direct and meaningful effort is underway to add suicide barriers on the bridge, and particularly when Flock Safety itself notes that its technology has "no specific use case for suicide prevention."[1] Further, while we do not mean to question the motivations behind it, we do think it fair to predict that well over 99% of the uses of this system will be for matters completely unrelated to suicide prevention.

Although not exhaustive, we explain below some of our specific concerns about the draft police department policy governing this surveillance technology. We hope you will agree that these concerns demonstrate why the pilot program should be rejected and why any attempts to regulate any system like this should be through ordinance, not internal policy.

- **Approval Mandatory for (ALPR) Funding Acquisition or Use**

  Despite the title of this section of the policy, it does not actually require the Portsmouth Police Department to undergo a formal approval process with the Council prior to the use of any ALPR technology. Instead, it only notes that "the Portsmouth Police

[1] Wolfang, Zane. "Portsmouth to reconsider camera system at bridge." *The Newport Daily News*, July 1, 2022.

Department *shall provide a public presentation to the Town Council* prior to engaging" in a number of actions relating to acquiring, seeking funding for, or expanding ALPR technology. Section IV(A) (emphasis added).

Though we recognize that this Council has the authority to approve or deny such programs, it is concerning that the internal police policy itself does not seek to require this type of necessary oversight. Rather, the internal policy implies that notice to the Council is sufficient to make any changes to or expansions of this invasive technology. An ordinance instead should be enacted which makes clear that any consideration of this technology, and the standards for its use, be subject to clear approval of the Council.

- **Regulated Use of Automated License Plate Reader (ALPR)**

We recognize and appreciate that this section of the policy makes sincere attempts to restrict the broad capabilities of the Flock Safety cameras. To that effect, we are glad to see provisions in this section which, for example, explicitly bar the use of this technology for biometric information identification purposes and for the recording or capturing of audio. Unfortunately, the caveats also contained in this section significantly weaken several other key provisions which seek to place limitations on the use of these invasive cameras.

This section begins by allowing for the use of this technology "to scan, detect, and identify license plate numbers" for a few very limited purposes. But it goes on to also broadly allow its use to identify any "vehicles associated with criminal investigations." (Section V(A)(4)). This sweeping allowance is problematically expansive and swallows any limitations the policy seeks to project. It becomes even more concerning when combined with a later exemption, which allows for the use of these cameras to "photograph[], or record [], or produce[] images of further identifying features of a vehicle, including but not limited to bumper stickers, paint color, or other unique aesthetic details" for any such investigation. (Section V(B)(2)).

Of course, a major concern of our organization has been the sheer volume of data and information that these cameras can capture and store on any vehicle that passes by the camera, including these specific and distinctive vehicle characteristics. Yet, allowing the

recording of these details for any vehicle merely "associated with a criminal investigation" is so vast an exemption that it barely provides meaningful boundaries on the use of the technology. It is also hard to square with the repeatedly claimed purpose of operating the technology: for the very specific goal of suicide prevention.

A similar critique applies to the language addressing the sharing of data in section V(D), which notes that "captured license plate data obtained for the purposes identified in section (A) above may be shared with another law enforcement agency for official documented law enforcement purposes or as otherwise permitted by law." But since no statutory safeguards governing this type of surveillance currently exist, just about *any* release of the data would be "permitted by law."

This section also provides a thirty-day storage time for any data collected through the ALPR system. This timeframe is repeated in a later section, V(H), which specifies the ALPR vendor as Flock Safety, and notes that this storage timeline applies to the company as well. Though timely and consistent deletion of data is critical, we do not see how an internal police department policy can prevent the company from changing its own data retention policy at any time, particularly since it is responsible for the data's maintenance. Thus, the thirty-day retention strikes us as more of a guideline than a guarantee.

The urgency of the problem surrounding the broad collection and maintenance of this data – along with sharing it with other law enforcement agencies for broadly defined purposes – is not hypothetical, as recent events illustrate its saliency. Mere weeks ago, the United States Supreme Court 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.

Imagine an Ohio resident with family in Rhode Island who travels here to receive an abortion for that reason. Nothing in law or this policy could prevent 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."[2]

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 bar the Portsmouth Police Department itself from sharing relevant information with that state. To the contrary. As noted above, the policy authorizes release of the data for any "official documented law enforcement purposes," which would encompass the criminal abortion scenario noted above. With some of the states banning abortion now considering ways to criminalize efforts by residents to cross state lines to get the procedure, we offer this example simply to show how high the stakes are in collecting enormous amounts of public data as this surveillance technology does.

A separate section of the policy, Section V(E), purports to limit the sharing of data for immigration enforcement, but we do not believe it actually does so. The policy fails to explain how, for example, collected information provided to the FBI could not then be transferred to a federal entity like ICE for immigration enforcement purposes.

Finally, we note that Section (V)(F) specifies that "Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will not be processed." Yet Section VII(A)(1) seems to directly conflict with that restriction, as it provides that "non-law

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

enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law."

In short, we hope that the Council recognizes how insufficient the policy's protections are in light of the profound violations which can occur from the inappropriate use of this data. To repeat, the policy appears to contain a number of important procedural safeguards – but the broad exemptions plastered on top of these safeguards make them functionally weak and largely ineffective.

- **Procedure**

We have emphasized that the expansive caveats and exemptions contained within the policy effectively undermine some of the safeguards the policy purports to provide. This is particularly illustrated by the provisions in this section, which allows for "an ALPR [to] be used in conjunction with *any* criminal investigation" and specifies that "reasonable suspicion or probable cause is *not* required before using an ALPR." Section VI(C) (emphasis added).

This language further seriously weakens any meaningful limitations on the technology's use. Theoretically, probable cause or reasonable suspicion should accompany a criminal investigation if fishing expeditions are to be avoided; yet the explicit release from those conditions within the policy virtually assures its use for questionable dragnet purposes.

- **Accountability and Safeguards**

As noted previously, this section states that "all non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law." (Section VII(A)(1)). With the current lack of statutory safeguards governing this type of surveillance in place, this likely makes *any* release of the data permissible to process.

- **Public Log of Use Required**

We note our sincere appreciation of and support for this section, which is one of the few policies we have seen that expresses a dedication to transparency inclusive of the location and number of cameras and any complaints or concerns received regarding the

ALPR technology. However, such a provision – like all the other safeguards – would be more appropriate in ordinance, where it may be better enforced by the public.

- **Training & ALPR Administrators**

  These two sections address training requirements for use of the ALPR system, but neither of them contains any remedies or penalties for misuse. Aside from this, because this is merely an internal policy, rather than an ordinance or statute, any victim of a violation of this policy will have no meaningful judicial remedies to pursue independently. Probably the only remedy available is the ability of the police chief to issue a two-day suspension, as we find it unlikely that the department will invoke the expensive and time-consuming procedures of the Law Enforcement Officers Bill of Rights in order to seek imposition of a more serious penalty. Yet this is hardly the vigorous type of penalty likely to deter misuse of this system.

In maintaining the overall position 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, based on the deficiencies in the proposed policy for the use of an ALPR system, the Council reject the implementation of the surveillance system in its entirety at the present time.

If the Town is serious in wanting to implement a surveillance technology like this while protecting the rights of its residents, it should adopt an ordinance that codifies the protections and remedies that are deficient in, and missing from, this policy, many of which we have outlined in this detailed testimony. An ordinance could include specific protections similar to those contained within 22 – H 7507 and 22 – S 2650, legislation that was introduced in the Rhode Island legislature this year to address this technology.

Community safety and suicide prevention are critical goals, but 24/7 surveillance of residents should not be a precondition for the safety that all of us seek. In light of all the deficiencies of the proposed policy, we urge instead the investment of the police department and the town in other measures rather than the use of and expansive policing and surveillance technology. Focusing the Town's energy on implementation of suicide barriers will go much

further in meeting the goal of protecting life, and without any damage to the privacy rights of tens of thousands of innocent drivers.

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