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

September 19, 2022

VIA EMAIL

Members of the Warwick City Council
Warwick City Hall
3275 Post Road
Warwick, RI 02886

Dear City Councilors:

We write to again urge this body to reject the proposed resolution and ordinance scheduled for consideration tonight that would provide for the City's purchase and implementation of the Flock Safety surveillance system. Consistent with our commentary and correspondence sent from our organization to you in the months of February, May, and August of this year, we continue to believe that the proposed policies, guidelines and ordinances, as well as the expansiveness of the surveillance technology itself, provide a strong basis for rejecting this program in order to preserve civil liberties for Warwick residents.

For your convenience, copies of both our February and August letters are attached. In the interest of addressing substantive issues with these proposals which we have not commented on in our prior letters, we are providing two new pieces of commentary to the Council today. First, this letter briefly addresses the newly amended components of the proposed ordinance, PCO-6-22 (Sub A). Second, and importantly, because this ordinance largely defers authority over the program to the Warwick Police Department (WPD) and its policy on Flock Safety cameras rather than imposing strict standards into the law itself, we have also enclosed detailed commentary on a draft version of WPD's policy that we were provided, and which we find is also concerningly insufficient in its scope and protections.

In noting concerns about the newly amended language in the draft ordinance, we also refer you to our attached August 15th letter, as many of the objections expressed then apply to this latest iteration.

- The language of PCO-6-22 includes a bar on using ALPR technology "without an associated Warwick Police Department case number or incident number and documented reason for the inquiry." However, with the understanding that Flock camera systems work passively – in that they are constantly photographing vehicles which drive by the cameras, and do so indiscriminately – we don't know how this provision could be followed without creating a specific case number for every single vehicle the system records. To the extent this wording is designed solely to address the circumstances when an inquiry into the system is made, it would still allow police to come up with an after-the-fact excuse for retrospectively searching the database for past "hits." This limitation is a small step, but much less restrictive than it seems.

- While we appreciate that this ordinance attempts to put in place a limitation on the length of time that data may be maintained, the exemptions contained in that provision are unacceptably vague and broad. First, while the ordinance appears to require that, except in certain circumstances, the data be purged within 30 days, it doesn't explain how this mandate can be applied to Flock Safety as opposed to just the police department itself. As a result, any claim of purging data may be completely illusory. Ultimately, the storage of the data is in the company's hands, not the Department's. Further, the ordinance references purging data in accordance with the state's Records Retention Schedule. But as we note in our commentary in opposition to the WPD policy, it is unclear to us that the state schedule ensures the purging of this type of data within the ordinance's specified time period.

- Finally, while we support the creation of a transparency portal, which Flock Safety has provided in other communities, we believe that the portal should also include the locations of cameras to ensure that residents can have oversight over any discriminatory impact that this surveillance technology may facilitate. Though we continue to oppose the use of these cameras, we note that other communities, like Bristol, in a step to try to foster at least somewhat more transparency, have made camera locations public.

As we have previously argued, a major flaw in the proposed ordinance, in our view, is that it focuses on specifying a few activities the technology cannot be used for when the thrust of any regulation should be narrowly specifying the circumstances when the surveillance system *can* be used. For the above reasons, as well as those described in the following commentary on the Department's proposed ALPR policy and our earlier stated objections to the ordinance as originally proposed, we strongly urge that this body do the right thing for civil liberties and for the residents of Warwick and reject this ordinance and the funding proposal for the technology. The purported safeguards contained in the ordinance and the policy, remain, as we have previously expressed, woefully deficient.

The ACLU of RI firmly believes that the detailed information we have previously sent you provides a substantive and comprehensive look at the dangers of this technology – and now, nearly a year into this technology appearing in Rhode Island, there is still no compelling reason why these concerns should be ignored in the pursuit of this flawed and invasive system. Your Council would not be alone in endeavoring to protect your residents by rejecting these cameras; only a few months ago, the Portsmouth Town Council rejected a similar proposal. We urge you to follow their lead.

Thank you once again for your continued time and attention to this matter.

Sincerely,

Steven Brown
Executive Director

Hannah Stern
Policy Associate

cc: Col. Bradford Connor

Enclosures

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 WARWICK POLICE DEPARTMENT POLICY ON "AUTOMATED LICENSE PLATE READERS"
September 2022

The ACLU of Rhode Island offers the following commentary on the draft "Automated License Plate Readers (ALPR)" policy as put forth by the Warwick 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 multiple letters sent by our organization to the Warwick City Council in February, May, and August of this year, and they remain. As noted previously, for convenience, a copy of both the February and August letters, which detail our substantive concerns about this technology, are attached to this commentary.

In addition, our August 2022 letter commented specifically on the merits of a proposed ordinance which was brought before the Warwick City Council to regulate this technology. Though we continue to believe, to guarantee enforceability, 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, we maintain the position that the draft

[1] We offer these comments preliminarily, as we continue to urge the Council to reject the installation of this technology altogether and, if we are unsuccessful in that regard, we are calling for much stronger regulation of the technology via ordinance. In short, we firmly believe 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. In any event, we acknowledge that this policy is just a draft.

August 2022 ordinance does not achieve these goals for the reasons enumerated in the attached letter. Only with a more detailed ordinance can there be better assurances for robust protections and restrictions that allow for public security and oversight and the minimization of harm to privacy rights and, just as importantly, for the availability of appropriate remedies for any violations.

With these caveats in mind, we offer below both general and specific concerns about the proposed policy. Unfortunately, we find it, similarly to the August 2022 draft ordinance, 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. Just a few months 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

[2] Section VIII(b) 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 VIII(c) 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.

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 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 Warwick 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 IX(d)], which would encompass the criminal abortion scenario noted above. Whatever assurances may otherwise be provided by city officials, the above example is provided to show how high the stakes are of collecting enormous amounts of public data as this surveillance technology does.

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

Even worse, the policy allows for the release of data not just for official law enforcement purposes, but "as otherwise permitted by law." [Section XI(a)] 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 Council 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.

- **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

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

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 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," [Section II(a)] – 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 VI(c)] – 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 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 IX(c)]. And while this policy generally appears to follow the one instituted by the

Providence Police Department – whose similar flaws we have also commented upon – it does diverge in one extremely concerning respect by permitting the creation of "custom hotlists by dispatchers, detectives, traffic investigators and supervisors." [Section VI(g)(5)].

Having an ALPR system which can scan existing hotlists, such as Amber or Silver alert databases is one thing. But allowing various law enforcement personnel to internally construct their own individual hotlists, in the absence of probable cause or reasonable suspicion, creates a potential for abuse of the system and the compromising of civil liberties in an expansive and particularly egregious manner. This could allow, for instance, the creation of a custom hot list for a vehicle known to be used by a prominent local activist, an act which would not be forbidden even by this policy's insufficient attempt to address First Amendment rights, the language of which is addressed in this commentary in a subsequent section. Depending on how vigorous the supervisory oversight is, an officer concerned about the comings and goings of their teenage child could add their license plate number to provide a notification every time that child drives by a Flock camera. The potential for misuse is vast, and the manner by which this policy vaguely sketches boundaries around the broad ability to create these "custom hot lists" not only could facilitate these possible abuses but *permit* them under this policy, thus not even subjecting offending individuals who use the system so inappropriately to disciplinary processes.

- **"Permitted/Impermissible Uses"**

Section VII 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." [VII(c) and VII(e)]

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. The lack of transparency surrounding the placement of these cameras only compounds this concern. And, 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 XI(c)], 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 [Section II(b)], 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 VII(f)], 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 X]. But there is no provision authorizing public access to the findings of these audits, including of "data errors found." These comprehensive audits would also only occur on a *yearly* basis and are even then only limited to "browsing inquiries." With neighboring municipalities such as Cranston reporting the photographing of over *five-hundred-and-fifty thousand vehicles* in the last thirty days,[6] the ineffectiveness and insufficiency of an annual audit for such an enormous amount of data is glaringly obvious. 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 simply too easy for this database system to be abused, and nothing in the policy gives assurance to the public that problems will be dealt with in any meaningful way.

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 Warwick residents will soon be subject to and incorporate various limits on its use. In addition to addressing

[6] https://transparency.flocksafety.com/cranston-ri-pd (accessed on 9/14/22)

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 additional 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 appropriately limiting 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

August 15, 2022

VIA EMAIL

Members of the Warwick City Council
Warwick City Hall
3275 Post Road
Warwick, RI 02886

Dear City Councilors:

We write in the strongest possible terms to urge you to reject the proposed resolution and ordinance scheduled for consideration tonight that would provide for the City's purchase and implementation of the Flock Safety surveillance system.

As you know, we first brought our concerns about Flock Safety to your attention back in February in a detailed letter that we have attached for your reference. The proposed ordinance, while providing some superficial limits on the use of the technology, fails in any meaningful way to address some of the core privacy issues that inhere to the implementation of such an invasive system of surveillance.

Structurally, the ordinance leaves almost all aspects of regulation of the technology to police department policy, which simply does not provide the safeguards, checks and oversight that a more thoroughly crafted ordinance establishing *statutory* restrictions would offer. Policies, after all, can be changed at any time and without any public notice or input.

Substantively, while the ordinance does contain certain restrictions – such as a ban on capturing audio or the photographs of individuals – the bulk of the uses by which the Flock Safety system will infringe on individual privacy are left untouched. To provide just a few examples:

• Subject only to whatever internal policy is adopted, police will remain free to track motor vehicles for *any* "law enforcement" purpose, and without the necessity of demonstrating any reasonable suspicion, much less probable cause, for doing so.

• The ordinance fails in any way to address or limit the previously announced plans by the police department to bolster the reach of the cameras through collaboration with private businesses, which will only increase the "fishing expedition" capabilities of the system.

• The ordinance contains no enforceable limits on how long the information captured by the surveillance cameras can be kept or on its use in ways that could target First Amendment activities.

• The ordinance purports to bar the use of the system for "federal immigration enforcement," but fails to explain how information provided, for example, to the FBI for a "law enforcement" purpose could not then be transferred to an agency like ICE for immigration purposes.

A major flaw in the ordinance that prevents it from ensuring adequate privacy protection for residents – especially as the capabilities of technology like this expand – is that it contains a short list of *prohibited* uses of the surveillance, as opposed to specifying in particular the narrow law enforcement circumstances when it is *allowable*. This essential latter approach was the one taken by legislation introduced this year in the General Assembly, and the only way to prevent inevitable mission creep.

In any event, while the policy ultimately adopted by the Warwick Police Department may address some of the issues cited above, the difference between a policy and a law cannot be overstated. Further, if the draft Flock Safety policy that the Providence Police Department has recently drafted, and which we critiqued in some detail, is any indication of what Warwick's policy may look like, the problems with it will be manifold and will fail to address the broader concerns about this massive surveillance system in any consequential way.

Concerns about the profound loss of privacy occasioned by the implementation of newer and more sophisticated forms of technology are often cast aside as hyperbole, but, unfortunately, they are not. They are real. It is the slow and steady erosion of our privacy through these new types of surveillance systems – even when implemented with the best of intentions – that is most insidious. To recognize this inescapable truth, we need look no further than to the fact that experts are now providing advice to women on the steps they should take to erase portions of their digital lives – information that will be sought for "law enforcement purposes" – in order to avoid the possibility of being criminally charged for seeking an abortion.[7]

For all these reasons, and for the reasons we have previously expressed, we respectfully once again call upon the Council to protect the privacy rights of its residents by rejecting the purchase of the Flock Safety surveillance system.

Sincerely,

Steven Brown
Executive Director

Hannah Stern
Policy Associate

Enclosure

[7] *See,* e.g., "Facebook turned over chat messages between mother and daughter now charged over abortion," NBC News, August 9, 2022. https://www.nbcnews.com/tech/tech-news/facebook-turned-chat-messages-mother-daughter-now-charged-abortion-rcna42185

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

February 23, 2022

VIA EMAIL

Members of the Warwick City Council
Warwick City Hall
3275 Post Road
Warwick, RI 02886

Dear City Councilors:

We are writing to express our organization's deep concerns about the potential implementation by the Warwick Police Department of deceptively-named automated license plate reader (ALPR) camera systems throughout the city. While the ACLU of Rhode Island certainly understands the importance of public safety, the approach to safer communities cannot and should not include the usage of technologies – like these cameras – which raise serious privacy issues, carry the clear potential for expanded surveillance, and could be implemented with absolutely no statutory safeguards in place. We urge you to reject the use of the cameras and to adopt an ordinance that will set standards for the deployment of any future law enforcement surveillance technology.

While 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 your municipality should reject the use of these cameras, but in any event future implementation of surveillance technology should not occur without clear and strict safeguards.

• **The cameras capture more than license plate numbers**. The use of other automated license plate reader systems – such as those utilized for tolling purposes or to monitor traffic patterns – in the state 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 to occur, 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.

But 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 may expect or anticipate. Concerns about overreach are only compounded by the acknowledgement of the expansive surveillance properties contained in, and invasive measures allowed by, these technologies.

As noted in the letter sent by Police Chief Connor in accompaniment of this budget request, 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."[8] (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 and as this same letter notes, 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 Warwick, but also from any of the other municipalities that are part of the system.

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 than *three-hundred thousand cars* within the last thirty days, information that will then be accessible for police searches for that same timeframe.[9] Particularly concerning in Warwick is the admitted outreach that the Warwick Police Department and Flock Safety have been doing to private businesses to bolster the reach of the cameras, and from which any collected data on these private cameras likely would not be included in any similar "transparency portal."

At the same time, the positing that these cameras operate solely based on the visual capturing of information is 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 such evidence as "screeching tires" and "associated vehicles,"[10] implying that these systems both 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, would be 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:

- 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;

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

- 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.[11]

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 nothing prevents expanded uses in the future. The chilling effects of the ability to track individuals in all these manners cannot be understated.

• **This concern about the normalization of increased surveillance is exemplified by the fact that the Warwick Police Department has admitted that both they and Flock Safety have begun doing private outreach to business to develop a public-private network of these surveillance cameras.[12]** The solicitation of private partnership, for the facilitation of increased police activity and presence, signifies an extraordinarily troubling action on the part of these two entities. Not only would an increased network of privately owned cameras for police purposes provide significantly less oversight to the Warwick community regarding their actual use, it flouts basic tenets of governmental transparency, accountability, and responsibility by creating a network of police-generated surveillance using private sources. This outreach also signifies that it is not the intent of the police department for this to be a limited use system – instead, it is clearly being considered as a significant method of future expanded policing surveillance activities, able to monitor the comings and goings of residents across the city, and beyond.

• **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.

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 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 proposal to implement Flock Safety cameras in Warwick and to further enact an ordinance that promotes

[11] https://www.govtech.com/biz/flock-safety-gives-users-expanded-vehicle-location-abilities
[12] https://www.warwickri.gov/sites/g/files/vyhlif1391/f/agendas/bid_package_2-23-2022.pdf

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