



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

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

VIA EMAIL

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.¹

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

¹ 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>



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

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

VIA EMAIL

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.”² (emphasis added) Such technological capabilities are incredibly invasive and far beyond what one conceives of when considering a technology often described as an “automated license 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.³ 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,”⁴ 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;

² <https://www.flocksafety.com/lpr-vehicle-recognition/>

³ <https://transparency.flocksafety.com/cranston-ri-pd>

⁴ <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.⁵

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.**⁶ 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

⁵ <https://www.govtech.com/biz/flock-safety-gives-users-expanded-vehicle-location-abilities>

⁶ https://www.warwickri.gov/sites/g/files/vyhlf1391/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