



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

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.”¹ (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.²

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,”³ 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:

¹ <https://www.flocksafety.com/lpr-vehicle-recognition/>

² <https://transparency.flocksafety.com/cranston-ri-pd>

³ <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.⁴

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 2020.⁵ 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.**⁶ 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.

⁴ <https://www.govtech.com/biz/flock-safety-gives-users-expanded-vehicle-location-abilities>

⁵ <https://www.npr.org/2021/08/20/1029625793/black-lives-matter-protesters-targeted>

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