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 30, 2022

VIA MAIL AND EMAIL

Board Members
Rhode Island Turnpike and Bridge Authority
1 E. Shore Road
Jamestown, RI 02835

Dear Members of the Board:

During RITBA's August 17, 2022 Board meeting, a discussion was held with the Bristol Police Department regarding the potential installation of two automated license plate readers at the southern end of the Mount Hope Bridge. These cameras would be stationed on the Portsmouth side of the bridge, where their use had been voted against by the Portsmouth Town Council. Because Portsmouth's participation in the program was rejected by their municipal body, the Bristol Police Department is seeking permission from RITBA to install these cameras – owned and operated by a private company called Flock Safety – notwithstanding the interests of the municipality in which the cameras would be located.

We write to RITBA today to respectfully, but strongly, urge that you reject these attempts from the Bristol Police Department to not only undermine the interests of their neighboring municipality, but to install an expansive and largely unregulated system of surveillance technology on state operated property. The ACLU of Rhode Island has consistently 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. RITBA should not take the unnecessary step of involving itself in such a program.

As an appendix to this letter, we have attached a memo that summarizes many of our broad concerns about this technology. However, the unique circumstances of Bristol's request compound these points with more specific reasons why RITBA itself should reject the police department's request to participate.

First, the use of this technology by the Bristol Police Department has been misleadingly sold to both RITBA and the public as an important tool for addressing suicide prevention. At bottom, though, the use of such an intrusive – and truly Orwellian – surveillance system like Flock Safety strikes us as an incredibly ineffective and inefficient way to achieve that goal, and not just because a much more direct and meaningful effort is underway to consider adding suicide barriers on the bridge. If police learn that a person driving a particular car may be considering suicide, it makes little sense to wait until a camera captures the car driving on the bridge to take action. Indeed, Flock Safety itself notes that its technology has "no specific use case for suicide prevention."[1] As we discuss in our appendix, this is a perfect example of "mission creep," where technology implemented for one purpose quickly gets refashioned for other intrusive uses.

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

Further, while we don't mean to question the motivations behind Bristol's request, 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. In fact, while the Bristol Police Department has communicated to RITBA a narrow purpose for these cameras, that scope of use is unsupported by the draft policy on this technology which was presented by the Department to the Bristol Town Council in May. The policy explicitly provides that an "**ALPR may be used in conjunction with any routine patrol operation or criminal investigation**; reasonable suspicion or probable cause is not required before using an ALPR." (emphasis added)

There is no basis to believe that cameras mounted on the bridge with RITBA's approval would or could be used any differently or more narrowly than any other cameras that are or eventually become a part of the police department's Flock Safety system – *that is, they would become tools for routine law enforcement purposes without any need to demonstrate cause for their use*. And regardless of Bristol's intent, access to information gathered by the cameras would also be available to every other police department in the state making use of Flock Safety.

All of this strikes us as even more problematic when one considers the cameras would be installed inside a municipality that has explicitly expressed disapproval in their installation. RITBA should not be a party to the police department's proposed usurpation.

Finally, we note, importantly, that RITBA itself has commendably recognized the critical privacy interests at stake with this type of technology. RITBA's electronic toll system is essentially a less sophisticated variation of Flock Safety's "automated license plate reader" system, but your agency's "Toll Account and Transaction Information Policy and Procedure" incorporates an array of strong privacy protections to ensure that the system's use is strictly limited and that it protects the privacy of drivers to the maximum extent possible.[2] Any assistance by RITBA in the installation of Flock Safety cameras on Bristol's behalf runs counter to the privacy-sensitive philosophy underlying your own policies.

We hope that the reasons explained above are sufficient for you to rebuff the Bristol Police Department's request, but attached are some additional substantive concerns about the Flock Safety technology which further underscore our position that RITBA should reject this bid. Thank you for your consideration of our views.

Sincerely,

Steven Brown
Executive Director

Hannah Stern
Policy Associate

cc: Lori Silviera, Executive Director
Chief Kevin Lynch, Bristol Police Department
Kevin Aguiar, Portsmouth Town Council President

Enclosure

[2] http://ritba.com/wp-content/uploads/2020/04/RITBA-Privacy-Policy-4847-6371-3362-v3.pdf

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

CIVIL LIBERTIES CONCERNS ABOUT THE FLOCK SAFETY SURVEILLANCE CAMERA SYSTEM
August 2022

• **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 Rhode Island 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. Bristol Police Department similarly touts the use of these cameras as limited to addressing potential suicidal ideation in drivers. Both claims are 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, and, importantly, the technology which Bristol is asking RITBA to be authorizing, 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."[3] (emphasis added) Such technological capabilities are incredibly invasive and far beyond what one conceives of when

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

considering a technology often described as an "automated licensed plate reader," and far beyond technology that would be appropriate to use for the expressed purpose of suicide prevention.

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 the bridge, 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 *five-hundred thousand cars* within the last thirty days, information that will then be accessible for police searches for that same timeframe.[4] It is worth noting that as we have been following this program, the number of photographs of vehicles entered into this database has only increased.

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,"[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 – and whether used now or saved for operational implementation for some time in the future – represent a profound overreach of this technology and invite over-policing and an inappropriate broadening of surveillance techniques.

---

[4] https://transparency.flocksafety.com/cranston-ri-pd
[5] https://www.flocksafety.com/

• **The gathering of such massive amounts of data is not innocuous and could have extremely harmful and inadvertent affects beyond the perceived scope of this technology.** The urgency of the problem surrounding the broad collection and maintenance of this data – along with the likelihood of sharing it with law enforcement agencies for currently undefined purposes – is not hypothetical, as recent events illustrate its saliency. Only two months 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."[6] Similarly, nothing could prevent police from abortion-banning states from directly demanding access to the vehicle information collected.

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. 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 and to emphasize that public entities and agencies, such as RITBA, should not be commencing the gathering of such potentially sensitive information.

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

• 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, as proponents note 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." In the past year, 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;
- 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.[7]

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 currently prevents expanded uses in the future*. The chilling effects of the ability to track individuals in all these manners cannot be understated. The fact that Bristol seeks to use the camera system for suicide prevention – a use that Flock Safety itself has never proposed – only highlights the validity of this concern.

• 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,

[7] https://www.govtech.com/biz/flock-safety-gives-users-expanded-vehicle-location-abilities

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.[8] 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, targeting both communities of color and protected protest 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 departments 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.

Community safety and suicide prevention are critical and laudable goals, but 24/7 surveillance of residents should not be a precondition for the safety that all of us seek. We urge instead the continued investment in other measures rather than the use of an expansive policing and surveillance technology. It is our belief that focusing on the implementation of suicide barriers, and fostering robust systems of mental health and psychological support for all residents, will go much farther in meeting the goal of protecting life and, critically, without any damage to the privacy rights of tens of thousands of drivers.

[8] https://www.sfchronicle.com/bayarea/article/Privacy-advocates-challenge-S-F-police-use-of-17375589.php