Dan Meyer

From: Fletcher Crone <fletchercrone@gmail.com>
Sent: Friday, January 2, 2026 3:36 PM
To: Dan Meyer
Subject: Highly Concerning Information regarding Flock Safety

Dear Police Chief Meyer,

Happy holidays and happy new year. My name is Fletcher Crone, a former longtime resident of Whitewater. I am writing to you with concern about the recent proliferation of Flock Safety surveillance cameras within Whitewater. I grew up in Whitewater, my parents, brother, and grandparents all live in Whitewater, and I am highly concerned about the impact that Flock cameras might have on the local community and my family.

Before I get into the reasons behind those concerns, I would like to say that I do very much understand the excitement surrounding their implementation. If the City of Whitewater was pitched that Flock cameras solved 10% of nationwide crime, and resulted in an up to 70% reduction in crime in certain communities, it's obvious to see why Flock Safety seemed like a silver bullet solution. However, according to reporting from Forbes and 404 Media, their claims of widespread crime reduction are downright false and misleading. Forbes showed that crime has actually increased in the community where Flock claimed a 70% decrease. To date, there have been no conclusive and comprehensive studies which show that Flock's cameras decrease crime.

Beyond the company's false claims, I have two main concerns regarding use of their cameras which I feel are strong enough to warrant their removal.

First, I'd like to address their main advertised purpose; catching criminals. Many people have posed the question: "If you aren't committing any crimes, what do you have to worry about?" It turns out, there is a lot to worry about. According to data from the Northern California Regional Intelligence Center, Flock Cameras have been wrong 1 in 10 times. There have been numerous cases across the country in which families and individuals have been held at gunpoint or handcuffed because License Plate Reader cameras simply misidentify the plate or individual associated with it (1)(2)(3). A $1.9 million dollar lawsuit was recently settled in Colorado for a family with small children who were held at gunpoint because a camera misidentified their license plate. With a 10% failure rate, it seems that it is only a matter of time before Flock Cameras lead to the wrongful detention of an innocent family in Whitewater.

We can also ask the question, what if you are a "criminal"? There have been countless examples of Flock Cameras being used by ICE, CBP, and DHS agents to target, arrest, and deport undocumented immigrants. As we all know, Whitewater is a city filled with immigrants, many of whom are in the country illegally. While none of those agencies have direct access to the network of Flock cameras, the company itself has acknowledged that CBP has accessed 82,000 Flock cameras through data-sharing agreements with local police departments. This means that nearly every Flock camera in the nation is accessible to CBP. Have Whitewater's 13 cameras been used against our immigrant community? Do we even have a way of knowing if or when they are used by CBP?

Along with these data-sharing agreements, it has been shown that local departments have been conducting searches of the Flock database on behalf of ICE. Just a few hours south of Whitewater, Danville, Illinois cameras were searched by police departments from all across the U.S. with search reasons including "immigration," "ICE," and "ICE+ERO," meaning ICE Enforcement and Removal Operations. In a similar vein, an analysis of Flock queries done by the Wisconsin Examiner found that the top two reasons listed for searches of their system were "investigation" and "inv," accounting for 30,000 searches. This further shows a

lack of transparency around the use of Flock's database which could be exploited by departments conducting searches on behalf of ICE.

Aside from immigration, Flock cameras have been used to track people for getting abortions that are illegal in their home state. Documents obtained by the Electronic Frontier Foundation show that Flock cameras from across the country were accessed under the reason "had an abortion, search for female" as part of an investigation into a "death investigation." I do assume that Whitewater intends to use their network of Flock cameras to help solve trafficking crimes and property crimes, but with these examples, it isn't clear if the city can prevent other agencies and departments from using their cameras for purposes that don't align with our laws and morals.

Another reason that I strongly oppose the use of these cameras is the myriad security vulnerabilities that Flock has been exposed as having, some of which are hilariously glaring. Again reported on by 404 Media, one such vulnerability included the exposure of at least 60 cameras' live feeds and administrator control panels (including the ability to download 30 days of camera footage and change camera settings) to the open internet without any sort of security. These control panels were publicly available, and spanned cameras from coast to coast. Technology researcher Benn Jordan unearthed feeds which included farmers markets and even children's playgrounds. Jordan even demonstrated how footage security vulnerabilities like these could be abused with commercially available investigation technologies to identify the people in the video feeds.

These public feeds are just the tip of the iceberg. Further research from Jordan and cybersecurity researcher John Gaines revealed nearly 50 security issues related to Flock Safety cameras and their databases. To list just a handful of these issues, we can get a picture of a wholly vulnerable, dangerously exposed public surveillance system. Firstly, there is the documented sale of law enforcement Flock Safety accounts, allowing bad actors to purchase access to the entire network of Flock cameras and their databases.

Another vulnerability involved the ability to obtain direct access to the devices through a series of button presses on the Flock Falcon camera, which causes the device to put out a wifi signal which can be connected to, and through which one can access the files and programs on the camera. All of this can be done within mere seconds. In a video detailing this, and other vulnerabilities, Benn Jordan explains how access to a Flock camera and its files could theoretically be used to replace or modify footage or images taken by the camera, calling into question the legitimacy of their use in court. In that same video, Jordan points out that access to the Flock system doesn't even require law enforcement to use Two-Factor Authentication. This glaring vulnerability has led U.S. Senator Ron Wyden to request an FTC investigation into the company on the grounds of national security. I highly recommend watching Jordan's video to get a clear demonstration and explanation of the many basic security vulnerabilities that are present in Flock Safety's ecosystem.

It is my hope that the City of Whitewater and the Whitewater Police Department take the time to reconsider the adoption and expansion of Flock technology. In our current political climate, it seems to me irresponsible to proliferate a technology of mass surveillance which has so many times been used to target immigrants, with and without the approval of local law enforcement. It further seems irresponsible to continue to use Flock's products when they have been routinely exposed for more-than-horrible security practices. I welcome further discussion on the topic as you consider what I have presented.

Best,
Fletcher Crone

fletchercrone@gmail.com