

We are “really, really very reliable”

Quote from EPD Chief Skinner’s “Copy Up” podcast: 07/11/25 episode

Eugene OR – On July 10, 2025 over two dozen community members attended a Eugene Police Commission meeting to express outrage over the Eugene Police Department’s recent installation of Flock Safety cameras across town. In the meeting, commissioners reviewed EPD’s Policy 1204 concerning their contract with Flock Safety, a Georgia-based company that advertises their automatic license plate readers (ALPR) to police departments nationwide.

Commissioners read the policy and questioned EPD Captain Jake Burke about how the cameras operate and Flock’s security practices. However, the commissioners neglected to interrogate Burke’s PR-coached reassurances derived from Flock’s own talking points. Despite the Police Commission’s express purpose to hold EPD accountable, the commissioners took Burke’s lies at face value.

Lie #1: We own the data



Captain Burke stressed that he and Chief Chris Skinner confirmed with Flock that EPD, and EPD alone, own the data. The contract states that the captured data is stored for 30 days in cloud storage, and Burke claims that after those 30 days the data disappears forever if it is not saved as evidence

But that's not how data works. And as concerned citizens conveyed in the Police Commission meeting, Burke is not a cybersecurity expert and it shows with his weak technical arguments.

Actual cybersecurity expert, software engineer, and Springfield resident Rob Sheldon has been in the tech and cybersecurity field since 1998 and is speaking out against Flock in Eugene. Sheldon met with Dissonant Times to debunk some of the misinformation EPD is spreading about Flock Safety.

EPD's understanding of Flock's practices derives solely from their contract and public messaging. Flock emphasizes that end users, like EPD, are the sole owners of any data collected via the cameras. The issue with this assertion is that Flock's very design guarantees that Flock can access their own infrastructure at any point.

According to Sheldon, end-to-end encryption is the tech world's gold standard for data security and the only form of encryption that guarantees users own their private data (such as text messages sent over the app Signal). Flock does not use end-to-end encryption, though per Sheldon, it would have been quite easy for them to. Instead, they use two less secure forms of encryption called transport layer security and encryption at rest.

Transport layer security is what our browsers do when we visit websites, they protect things like our browsing activity from internet service providers. Encryption at rest, simply put, is where data is protected when it's stored in the data centers it ultimately ends up in. Most service providers today do not operate their own data centers, those roles fall to companies like Amazon, who own around a third of data centers worldwide.

Data held in these centers can be hacked more easily than in end-to-end encryption. Flock's use of these forms of encryption suggest that the company values retaining access to the data its cameras collect (which end-to-end encryption would prevent) more than the digital security of innocent commuters' every move.

If EPD is truly only using the data to catch "bad guys" on the NCIC hot lists, then Eugene could do what states like New Hampshire require and delete data after three minutes if no crime matches a recorded license plate.

So no, Flock's architecture does not guarantee safekeeping of sensitive data, and 30 days is actually the longest possible

window to store ALPR data using Flock's services. Both of these facts alone puts innocent people's privacy at risk.

Lie #2: We are not legally required to cooperate with the federal government if they subpoena our data, and there are no backdoor avenues for this to happen

Burke claims that EPD would need to authorize the release of its data if Flock was subpoenaed by federal agencies such as ICE, which is happening in cities across the country. To this point, Flock assures its skeptics that there is neither a digital nor legal backdoor into their data.

But Rob Sheldon points out that the 2001 Patriot Act authorized a tool called a **national security letter**, that if issued, service providers such as Flock Safety would be required to provide whatever the federal government requests—and may be issued a gag order to boot. For example, if the Trump administration federally outlawed gender-affirming healthcare, the FBI could in theory seek out any practitioner or recipient of such care within EPD's jurisdiction and EPD would potentially not even know about "their" data being used this way.

Despite Flock Safety and EPD's claims, the federal government can force Flock to cooperate, assuming Flock isn't already friendly with the feds—something their funding sources indicate a strong possibility of. Flock is a venture capital (VC) funded start up, meaning their Silicon Valley investors expect a large return on their investment. One could argue their millions of start up capital implicitly demand Flock founders' loyalty to venture capitalists such as Peter Thiel.

Palantir founder, Trump advisor, and real-life sci-fi villain Peter Thiel's own VC firm the Founders Fund is one of Flock's largest funders. We already know we can't trust Palantir: the biggest name in private security that's contracted with ICE since the Obama administration. Currently valued at \$7.5 billion, can we trust Flock's leadership to hold the public

interest above some of the biggest names in the private security sector?

Lie 3: Flock is transparent and so are we

Flock founder Garret Langley once wrote, *"We strongly believe that LPRs...are best used in concert with responsible policies...That is why I have a team at Flock that has stood in front of more than a thousand city councils to answer their questions before voting to approve using our technology."*

More than a thousand city councils had this opportunity, but not Eugene's. According to the memorandum of understanding between Flock and EPD, the only bureaucrats that appear to have known about and/or authorized the installation of the cameras was then city manager Sarah Medary and the Eugene Police Department. The public wasn't informed of Flock cameras until they starting popping up in our neighborhoods.

Beyond this breach of public trust, EPD reportedly took down the portion of their transparency page (which has since been reinstated) that showed which other non-Oregon departments they shared data with. But before public records requests flooded in and they took down that portion of the page, their transparency page hosted on Flock's website showed that they shared data with 38 other jurisdictions as far as Nevada (which is not a sanctuary state).

There have been no neutral third party audits of EPD's handling of Flock data so far, instead, this task is left to the public. But hey, Flock's transparency page is useful for *some* things, like showing us the average number of database searches in a given 30 day period. EPD averages between 1,100-1,300 searches a month. Meanwhile in West Sacramento, there were only 236 searches over the same time period according to Sheldon's research. Eugene is a much smaller place than Sacramento, so why does EPD need to search the database so frequently?

These are the kinds of questions the Police Commission didn't think to ask.

EPD's deal with Flock demonstrates poor risk assessment in a risky time for our most vulnerable community members. If the police commission won't hold EPD accountable to these tougher questions and they continue to pull the wool over the eyes of the public, what measures of accountability are left to ensure EPD handles AI-powered surveillance responsibly?

Learn how to take action at <https://eyesoffeugene.org/>

1) <https://open.spotify.com/show/li9eMyYSpaQyfzaQl8TAAC>

2) <https://dissonanttimes.org/lets-leave-the-flock/>

3) <https://eyesoffeugene.org/>

4) <https://www.cloudzero.com/blog/cloud-computing-market-size/>

5)

<https://www.aclu.org/news/privacy-technology/how-to-pump-the-brakes-on-your-police-departments-use-of-flocks-mass-surveillance-license-plate-readers>

6) https://www.law.cornell.edu/wex/national_security_letter

7) Behind the Bastards Peter Thiel episode:
<https://www.youtube.com/watch?v=mfXbyQ9KFdg>

8)

https://www.crunchbase.com/funding_round/flock-safety-series-f-12aa3413

9)

<https://truthout.org/articles/security-wars-inside-the-militarys-big-messy-fight-with-palantir-the-company-they-pay-to-spy-on-you-online/>

10)

<https://www.govtech.com/biz/flock-safety-offers-new-tools-as-i>

t-tries-to-rebut-critics

11) <https://eyesoffeugene.org/why-flock-is-bad/>

12) <https://transparency.flocksafety.com/eugene-or-pd>