# Surveillance, Profits, and the Police:

## Implications of the Growing Role of For-Profit Companies in the Heart of American Police Departments

*By Jay Stanley with Lauren Yu*

*June 24, 2026*

In early 2025, two of the biggest police-surveillance tech companies, Axon and Flock, ended their cooperative relationship in a nasty public breakup that involved dueling accusatory CEO letters, and went to war with each other. Axon, the company formerly known as Taser, is a major vendor to police departments and sells not only the electric stun devices but also body camera and evidence storage products. Flock is the most prominent provider of automatic license plate reading (ALPR) technology.

This falling out may have been inevitable, as both companies are expanding their law enforcement offerings. Both sell license plate readers, surveillance cameras, drones, 911 services, and "real time crime centers." Both are aggressively seeking to leverage the new capabilities of AI. And ultimately, both have the ambition of becoming the leading provider of an "operating system for police departments."

Before this happens, Americans, policymakers, and the policing profession itself need to grapple with the implications of such a shift toward the corporatization of policing. What would it mean to have private companies playing a central, operating system-like role at the heart of a police department? What are the implications of having police data flowing through the hands of a for-profit private company that isn't subject to the checks and balances that apply to government agencies?

**What is the "operating system" of a police department?**
The companies are not very specific about what they mean by the "operating system" concept. With a computer or phone, an operating system is of course the software (such as Windows, Linux, iOS, or Android), that everything else runs on top of. Not only does it typically have visibility into what every app is doing, but also control; the entire system can't even function without the OS.

Axon talks about "integrating hardware devices and cloud software solutions" in "the Axon ecosystem" and connecting "every officer, responder and agency." Flock claims that the company's "unified platform" combines "License Plate Recognition, video, audio, drone capabilities, and 911 audio into one system." A third contender, Motorola Solutions (a spin-off from the former cell phone manufacturer), doesn't speak about providing an "OS" or "operating system" but appears to have similar ambitions. Motorola's products include the ALPR company Vigilant, body cameras, 911 and dispatch services, and, like Axon, an AI police report drafting product. The company offers "command center public safety software," a "public safety software suite," and an "AI assist suite" that aims to "synthesize multiple sources of data from across an agency — 911 audio, body and in-car camera footage, radio transcripts and more — into a unified thread of intelligence."

All three companies are established police vendors who have an extensive network of police department contacts and relationships to leverage, giving them a major advantage over many competitors in trying to become a general police platform.

Overall, the vision seems to be an extension of the real-time crime center concept: collecting, managing, controlling, analyzing, and optimizing the flow of data from disparate sources and allowing the exploitation of synergies from those sources. That would, without conscious efforts to the contrary, give these companies significant access to law enforcement data, including sensitive data about millions of Americans. Policymakers, the public, and police leaders need to recognize the direction in which things are moving and the potentially significant implications of such a shift, and take steps to head off the predictable problems this will create.

It is true that corporate-vendor access to institutional data is happening in fields far beyond police departments; a wide variety of operating system, cloud services, and platform providers can access data that they hold and/or process on behalf of clients of all kinds, including many other government agencies. However:

1. This is a problem; many organizations are exposed to privacy and security risks through such practices that have not been sufficiently recognized. And we are seeing a growing interest in end-to-end encrypted and locally hosted services to address such risks.
2. Law enforcement is different. That's because the data it holds can be incredibly sensitive; to take just one example, the fact that police are investigating you (and the

information they might collect during such an investigation, including potentially even such data as wiretap recordings) can be ruinous for someone's reputation. Police frequently investigate people they never arrest or charge, in the process storing troves of sensitive information about individuals and even their families, neighbors, coworkers, and friends. The police context both highlights why any corporate control of data can be a problem, and presents a particularly acute example.

3. Even the use of everyday corporate products (such as Microsoft's) could be a problem in the law enforcement context without specific safeguards. But the issues at stake rise to new and more intense levels insofar as companies like Axon, Flock or Motorola approach their goal of becoming operating systems for police departments, given the breadth and sheer volume of the data they could access and control.

## *I. Police-corporate entanglement has a long history*

Uncomfortably close alliances between police and corporations have been happening since the dawn of industrial capitalism, when American law enforcement worked closely with companies during the labor battles of the late 19th and early 20th century. It includes the Cold War reliance by law enforcement and security agencies on private groups and companies to collect information about leftists, and the corporate sharing of bulk data about Americans' communications during the Cold War and after 9/11.

In his 1990 book *Protectors of Privilege,* Frank Donner argues that "A strong case has been made for the thesis that in the course of the past hundred years urban police have served as the protective arm of the economic and political interests of the capitalist system." He details how the hunt for and blunt repression of anti-capitalist radicals, subversives, and dissenters was a primary activity of law enforcement from the Haymarket bombing of 1886 until curbed by constitutional reforms in the 1930s, only to reemerge in the guise of Cold War police "intelligence" units that engaged in surveillance, dirty tricks, intimidation, and harassment of ideologically defined "subversives" of various kinds.

At the peak of the labor movement we also saw how the existence of intertwined business and political elites allowed the legal system to criminalize labor activism. Elements included the use of private-sector guard forces and "detectives" such as those from the infamous Pinkerton agency, and the tendency by police to engage in mass arrests and violence and to look the other way when it came to violence against strikers.

After 9/11, we saw a new drawing together of government and companies as the two cooperated in carrying out aggressive new surveillance programs. In 2004, the ACLU published a report on the upsurge in such cooperation entitled "The Surveillance Industrial Complex." That level of cooperation only partially diminished with the negative global

reaction to the 2013 revelations about the National Security Agency and the activities of tech firms that Edward Snowden brought to light.

This history is the context in which the incipient corporatization of police departments is happening. Today, business and political elites remain as intertwined as ever, and the tendency toward blurring the lines between corporate and government surveillance continues through the activities of companies like Palantir, Ring, and the data broker industry, among many other examples. All in a context where many prominent tech companies have reverted to a stance of what appears to be enthusiastic cooperation with the government despite the Trump Administration's blatant violations of the Constitution and human rights.

## *II. Why the corporatization of police departments is happening*

Despite law enforcement's long record of cooperating with companies, in the past departments largely performed most police functions themselves. Departments may have purchased police equipment from private vendors — including, more recently, software — but those vendors didn't have live, remote control over those products or access to their data, and didn't centralize data from thousands of departments across the nation. The role of private companies in gathering, holding, sifting, analyzing, and managing data for police departments puts the issue of police-corporate cooperation in a stark new light, and threatens to intertwine companies and law enforcement in ways that we have never seen before.

There are several factors behind the shift.

### 1. The increasing flow of data from novel surveillance technologies

New surveillance devices and technologies are bringing novel and often enormous flows of data into today's police departments. Body cameras, for example, have been adopted by 82% of US law enforcement agencies, according to one source, and each camera generates potentially hours of video data each day — data that must be copied off the cameras, stored somewhere, and made available for evidentiary or training purposes, or for (problematic) AI analytics. Video data also pours in from dashcams, drones, fixed surveillance cameras, and license plate readers (which are starting to collect video along with time/place/plate data). Private parties such as businesses and doorbell camera owners also sometimes submit video to police departments.

**Examples of digital-age police data**

- Video
- Purchased commercial data
- License plate reads and hotlists
- Gunshot detection alerts
- Open-source data (e.g. social media tips and evidence)
- Geospatial/address data (GIS)
- "Smart city" sensor feeds such as speed sensors
- Cell-site/location records and other lawful telecom returns
- DNA profiles and lab submissions/results
- Digital forensics extractions from phones, other computers, and cloud accounts

And of course, video is just one source of digital data flowing into police departments today. Perhaps one of the most significant is commercial data that law enforcement agencies buy from private-sector data brokers. Flock, for example, is planning to plug its system into commercial data brokers that offer services such as "people lookup."

**2. The increasing digitization of legacy police data**

On top of all this data from relatively new technologies, departments increasingly store in digitized form information of the kind they have long collected, including audio and other data from 911 calls, dispatch, officer communications audio and other records, jail bookings and releases, field interview cards, citation/e-ticketing systems, warrants, protection orders, court dispositions, suspicious activity referrals, public tip lines, and many others. This kind of data has long been stored in police Records Management Systems (RMS) — a product that Axon, Flock, and Motorola all now offer, and which they presumably envision being swallowed up by the larger "operating system" concept.

**3. The growth of centralized corporate cloud services**

An important part of the picture here is the move to cloud services. Cloud services and the drive to make everything a subscription instead of an outright sale, while sometimes offering real advantages, can also become an avenue for ongoing extraction from and control of customers. It also raises new questions when this model is introduced into policing. Cloud services:

- **Centralize data.** When a company sells a product such as a camera, the cloud model funnels the data from all its products into its own servers. Flock, for example, nationalizes the collection and then the search of license plate data, which used to be collected much more locally. Such centralization increases the security and privacy risks of such data compared to when it is decentralized and dispersed. And what other kinds of data will the OS model, cloud processing, and corporate consolidation also nationalize? Already Flock is moving to centralize video. We probably can't imagine today all the ways in which the centralization of various data sources could create sweeping new powers for law enforcement and enable new abuses.
- **Increase control.** The cloud/subscription model allows companies to control its products even after they've been purchased and deployed. For example, it can let a company brick a customer's camera if they stop paying fees or in the case of a dispute, and they can block undesired parties from using and independently evaluating their products. Flock, for example, has been able to prevent the security research company IPVM from testing its products — IPVM can't just go out and buy a Flock product off the shelf, because Flock controls its deployment through the cloud.
- **Reduce market choice.** Cloud networks can create network effects that reward companies that have more customers, creating feedback loops that produce market

concentration or monopoly. As security industry analyst and IPVM founder John Honovich puts it, "The trajectory of video surveillance points toward greater concentration of power…. As cloud adoption increases, a small number of companies are becoming dominant providers of connected surveillance platforms. What was once fragmented across thousands of local recorders is steadily consolidating into large, centralized systems." This is why Flock, with its thousands of cameras collecting data on millions of people and its nationwide search capabilities, is attracting many millions from top Silicon Valley venture capital investors. The upshot is that more data is held in fewer hands, increasing the power of surveillance — and the potential consequences of abuse.

**4. The seductive allure of AI**

With all of this data, vendors are pushing AI hard on their law enforcement customers as a shortcut to squeezing value out of data. Examples include video analytics, AI-assisted police reports, and algorithmic inspection of license plate reader data for "suspicious" movement patterns. The promise of AI, especially large language models and vision language models, is that it can crunch the oceans of data now being generated and lead to smart, efficient, and rapid police actions.

There are reasons to be deeply skeptical of that promise — AI-assisted police reports, for example, are a terrible idea — but meanwhile it incentivizes the compilation and centralization of large amounts of data for training and analytics and the purchase of products that funnel it all to a single company, and rewards vendors who can boast about their supposed "cutting-edge" capabilities. Like cloud surveillance, it rewards companies that have more customers and more products across different categories; that lets them collect more data, which in turn allows them to promise better AI.

## *III. How Providers of Police "Operating Systems" Could Exploit Their Special Access to Police Data*

The oceans of video and other data flowing into a police department together with the role of private companies in managing and analyzing that data raise a number of policy questions. Perhaps the biggest is what the implications will be of private corporate vendors having access to so much sensitive data about millions of Americans.

**1. How could companies abuse special insider access to police information?**

Possibilities include:

A) **Critics and journalists.** Some companies would no doubt love to get their hands on confidential information about critics, activists, and journalists' interactions with law enforcement, potentially including compromising information about them or their families. In 2011, for example, documents obtained by the hacking group

Anonymous found that plans were circulated among companies including Palantir and Bank of America and the US Chamber of Commerce for a surreptitious sabotage campaign against critics, progressive groups, and unions. In 2014, a top Uber executive discussed engaging in an opposition research campaign to look into the press — "your personal lives, your families." And we've seen face recognition used in a retaliatory fashion by the billionaire owner of Madison Square Garden.

B) **Regulators and lawmakers.** For the same reasons, a company might also take advantage of access to inside law enforcement information about a vexatious government regulator or lawmaker working to regulate them in ways that could curb their profits.
C) **Competitors.** Police databases could well contain non-public information about a vendor's competitors that allow that vendor to gain unfair advantages over such a rival.
D) **Labor unions.** It's not hard to imagine a police vendor involved in a labor battle where the police get involved, especially if the labor movement continues to regain breadth, vigor, and militancy. In the case of any strife, Americans expect the police that serve them to be neutral, disinterested parties when there's a dispute or unrest — not for the employer to have inside access to everything the police are seeing, hearing, and doing.
E) **Investigations into themselves.** What happens when a vendor or a parent or affiliated company itself becomes the focus of law enforcement investigation? Companies like Flock and Motorola Solutions also have hundreds or thousands of employees; what happens if police suspect one of those people of a serious crime? How will agencies dependent upon technology run by a company keep investigatory materials hidden from that company?

Companies may claim that the terms and conditions in their contracts with police departments prohibit such conduct, and their websites try to assure potential customers that the data is protected against possible misuse. Axon states it won't access data "without the explicit authorization from the customer." Flock declares, "Flock will not share, sell, or access your data," and that "Flock employees do not access customer data except in tightly controlled, audited circumstances for support or maintenance." The problem is the lack of barriers to violating these promises and the near impossibility of discovering if those clauses are violated because of how easy it is to copy, transfer, and share data without leaving any fingerprints, especially within an opaque private company. When companies build and maintain software, they can also build and maintain means of accessing that software without leaving a trace visible to their customers.

In fact, documents obtained through open records requests by a resident of Dunwoody, Georgia, indicated that Flock employees had unfettered access to live video feeds from the company's cameras and were regularly watching them, including video from the fitness studios, pool, and gymnastics area at a local Jewish Community Center, adding to the already intense controversy in the city council over whether to approve a contract with the company.

Agencies that entrust sensitive law enforcement information to private entities are taking an enormous risk that could compromise safety, the integrity of criminal investigations, and the privacy and security of millions of Americans.

**2. How can companies profit from the data?**

Companies that collect and centralize data from across the United States may seek to profit from it like data brokers. Even a vendor that doesn't outright sell law enforcement data might sell inferences derived from that data — to insurance companies, law firms, private detectives, or others. A vendor, for example, might know that a person or company was the subject of a non-public law enforcement investigation that did not result in charges, and use that as part of a "background check score" even as it never explicitly cites that data or its source. Flock says it does not sell customer data, but such a restriction doesn't mean they do not or will not find ways to monetize data. Although Facebook doesn't sell user data, it nonetheless profits off it.

**3. How can this data be abused for personal purposes?**

The problem of police officers abusing law enforcement databases for personal purposes (such as searches on love interests) is a perennial one, with officers regularly found engaging in such abuses of data, and an unknown but likely much larger number of abuses that are never discovered or made public. The problem is not new: in the 1990s, a high-ranking DC police official used a database to blackmail closeted patrons of gay bars — a practice apparently common enough that it had an offensive name among some officers: "fairy shaking." Today, the extension of police database access to unknown numbers of corporate employees, subject to unknown controls and audits, risks expanding such abuses beyond police departments into private companies. Axon says that "a small team of Axon system administrators" has access, and that those system administrators are monitored, but that still gives us little insight into what safeguards are truly in place. And we know of numerous other examples (besides Flock) of companies that casually allowed employees to access user data, regardless of the risks.

**4. How can this data be exploited in financial and prediction markets?**

In the late 1800s, not long after the robber baron Jay Gould took over Western Union in 1881, there were "widespread suspicions, albeit never proved, that he was monitoring messages to score gains on the stock market," according to historian Paul Starr. A company today with inside access to non-public law enforcement data might be able to similarly leverage that information for financial gain in the markets — cheating other investors who lack such scoops. With the rise of prediction markets, there are even more temptations to and opportunities for employees to trade on inside information.

**5. What stops a vendor from altering or deleting data?**

In addition to abusing *access* to information, is there anything stopping a vendor from actually *altering* evidentiary data that it is entrusted with, or outright erasing it, based on the same kinds of motivations discussed above?

Evidence management is an entire field within the criminal legal system, and various practices have emerged for maintaining the integrity and chain of custody of digital documents. But it's a very complex area, and complexity is bad for security. Techniques such as hashing can be used to prove that a digital file hasn't changed — but if the vendor is the one storing the hash, as under some systems, that wouldn't prevent abuse.

A more subtle way that a vendor could manipulate data to steer the outcome of a case is through the manipulation of AI. Police agencies are starting to use AI to sift through large volumes of data to search for evidence of guilt and decide whether there's enough to file charges. That is itself problematic, but also raises the prospect that a vendor could manipulate an AI product to make sure it doesn't find such evidence, or bias it in favor of finding such evidence only for particular people or groups of people.

Overall, what is required is an airtight techno-human system for storing digital data that is built to resist abuse from any direction and doesn't rely on trusting any potentially interested parties — even while allowing data to be accessible to those who need it, modified into derivative products (such as redactions or excerpts), and erased according to a deletion schedule. Can we trust that such a difficult and complex task will be done properly? That there won't be cracks through which a big, monopolistic company could get away with altering data?

## *IV. Other issues raised by the corporatization of law enforcement*

In addition to questions around the misuse of access to law enforcement data by companies, the incipient new role of vendors raises other significant policy issues:

**1. Profit-driven distortion of decisionmaking.**

Policing and profit are not a good mix. For all the problems with American policing, officers are not generally motivated by profit (with the shameful exception of civil asset forfeiture). Putting for-profit corporations at the heart of police departments threatens to change that.

For example, when red light cameras were first being introduced around the US, the camera vendors often received a cut of ticket revenue, and critics charged that cameras were sited to maximize revenue rather than to maximize safety, and that yellow light times were shortened to trap more drivers in violations. Similar or more subtle pro-profit biases — in favor of their own company, or companies with which they are cooperating, allied, jointly owned, or hoping to curry favor with — are entirely predictable.

It's not entirely clear how companies running a police department platform could tilt police activity in their favor, but it seems likely there would be many ways — perhaps some too subtle to easily detect. Again, Americans expect police to be neutral, disinterested

parties when there's a dispute, yet businesses can have a strong financial interest in how they carry out their duties.

**2. Lack of checks and balances.**

Private companies are not subject to many of the transparency requirements and other measures that have evolved over time to serve as checks and balances on government power. That includes the federal Privacy Act and Freedom of Information Act (FOIA) and state and local equivalents, email and other data retention requirements, and the budgetary and policy oversight of democratically elected city councilmembers, oversight boards, internal affairs bureaus, and other officials.

There's also a larger democratic accountability problem: elected officials can be tossed out of office if people are unhappy with them, but private companies can't — especially if they're locked into a long-term contract. And you can't use voter pressure to make a bad private company "resign" the way a sheriff might if they do something bad. Making matters worse, many companies are under enormous pressure to continuously increase revenue, often at the expense of the public interest.

**3. Use by government as end-run.**

Precisely because such checks and balances don't apply to companies, government agencies have long attempted to outsource their activities to private companies as an end-run around public visibility and control. Examples today include New Orleans police's use of a private organization to do face recognition in avoidance of local regulations, and the reliance by law enforcement on private companies to maintain dossiers about Americans not suspected of wrongdoing as a means of doing an end-run around the Constitution and laws that would make that otherwise illegal.

Police and prosecutors have also attempted to evade their pre-trial disclosure obligations to people accused of crimes by claiming that information created using proprietary technologies is a trade secret, or is immune from disclosure because it is stored in a private company's files rather than the government's.

**4. Bias toward prosecution.**

Vendors in the law enforcement space have an incentive to demonstrate that their products are great at helping police catch criminals. That means they have a financial interest in being able to say their products led to a high number of arrests and convictions — they gain no marketing advantage when crime is low or people go free. But showing that your product has a high rate of helping to catch and convict criminals is not the same thing as showing that your product advances justice. When high arrest rates and high conviction rates equal high profits, that threatens to further distort our already highly unjust criminal legal system.

Companies in this space also have an incentive to distort the frequency and seriousness of crime in order to boost overall demand for their products — fear-mongering that distorts

the public discourse and threatens to drive public resources toward policing over more-proven public safety solutions.

**5. Cybersecurity honeypots.**

The more data collection is centralized and nationalized, the more it becomes a "honeypot" attracting hackers, and the worse the consequences of a successful breach. With law enforcement data, that could create significant national security risks as well. It's a fact of life that in our current moment in history, cyber-defense is simply harder than cyber-offense. Worsening the situation is the fact that good cybersecurity costs money, and yet most costs of breaches often fall not on the company but on ordinary people, creating a disincentive to protect data and a significant market failure. Certainly in the case of Flock, the company has not seemed to prioritize cybersecurity as a number of failings have been uncovered.

## *V. Cloud platforms also deserve scrutiny*

There is another set of players that raise many of the same concerns: Cloud computing platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, which store the data for companies like Axon and Flock.

Anyone who thinks about privacy knows that, as the saying goes, "There's no such thing as the cloud — it's just somebody else's computer." So do Amazon and Microsoft have access to all the same data that Axon and Flock collect on behalf of their law enforcement clients? If so, that would raise some of the same issues that attach to police department "operating system" vendors.

National standards for the handling of criminal legal information are set by the FBI's Criminal Justice Information Services (CJIS) division through its CJIS Security Policy. That policy does not require agencies to use end-to-end encryption when storing such data with a cloud services provider. To its credit, the CJIS policy notes that it "does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI" and that end-to-end encryption "with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data." However, it acknowledges that "it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task" and permits cloud service providers to have access and control over encryption keys (PDF p. 370). What it requires of those cloud service providers is that the cloud service provider encrypts the data and that its personnel who can access the keys undergo security awareness training and meet personnel security requirements.

Amazon states that it does not access or use data stored in AWS for any purpose without the customer's agreement, and that it doesn't use the data for marketing or advertising purposes. In the AWS Customer Agreement, Amazon states that it does not access or use customer data except in providing its services and "as necessary to comply with the law or

a binding order of a governmental body." However, that's not to say that Amazon *couldn't* access the data in other situations. Axon states that it uses AWS for storing customer data. Flock shares a little more detail in its FAQ and privacy policy, revealing that it uses Amazon's S3 service for storage, which by default encrypts data at rest using encryption keys managed by S3. That gives Amazon the ability to decrypt the data stored on its servers because it manages the keys.

Flock appears to have gone one step beyond the default route by using encryption keys managed by AWS Key Management Service (KMS) and AWS Identity Access Management (IAM) to manage access to AWS resources. That would make it more difficult to access Flock's data without Flock knowing, but Amazon still holds the keys. Flock's promise to safeguard customer data through IAM blocks unauthorized Flock employees and outsiders from accessing data, but not Amazon, which is responsible for vetting the identities of the parties requesting access. Although we know less about Axon's setup, the same principles apply. If Amazon has the keys, then the only thing blocking Amazon from accessing Axon or Flock's data is Amazon's promise not to do so.

Microsoft presents a similar story. Microsoft's policies restrict access to customer data, except as necessary for providing its services and when legally compelled to produce data. Access to customer data is logged and regularly audited by both Microsoft and third parties. But again, just because Microsoft says it won't access customer data doesn't mean that it can't. By default, data in Azure Storage is encrypted using Microsoft-managed keys. Azure Storage also allows customer-managed keys, but if Axon manages its own encryption keys, it still has to store them using an Azure key store. Either way, the encryption keys lie with Microsoft. Ultimately, the barrier to Microsoft not accessing Axon's data is Microsoft's promise not to do so.

And if Amazon or Microsoft did improperly access Flock or Axon's data, it isn't clear who, if anyone, would find out. Both Flock and Axon say they monitor for suspicious activity, but we don't know if unexpected activity from Amazon or Microsoft would be flagged as suspicious. It could also be possible for Amazon and Microsoft to cover their tracks, assuming that Flock and Axon are dependent on logging files stored in AWS and Azure to monitor access to data.

As discussed above, the cloud platforms are widely used by a variety of institutions, not just those serving law enforcement. Still, the data access that cloud storage can enable is a problem — one that could become important in many of the scenarios we discuss above, such as a company becoming embroiled in intense battles with union organizers or trading accusations of criminal conduct with a competitor that is investigated by the police.

## *VI. Alternative arrangements are possible*

Putting aside the question of whether police departments should be collecting large volumes of surveillance data at all, police departments could in theory reduce or solve many potential problems by hosting all their data themselves on their own servers. But few think police departments can, will, or should become experts at data storage and handling — that's just not their core competency. And neither is cybersecurity; even given the market failures there, a large company is likely to be much better at securing data than any but perhaps the very largest police departments.

What vendors could very well do, however, is provide data services to police departments on an end-to-end encrypted basis. Take body camera video, for example. When an officer wearing a bodycam finishes their shift, they typically plug it in to a dock, where the videos are uploaded to a cloud storage service run by a vendor. That data could be encrypted at the police station before it's uploaded using encryption keys that only the department holds, so that it's impossible for the company hosting the data to decrypt or view it. Such "zero knowledge" end-to-end encryption is becoming increasingly common among cloud storage and password manager vendors.

End-to-end encryption does mean that vendors holding end-to-end encrypted data can't perform many operations on that data, such as search, translation, or AI analysis. (There are advanced encryption techniques that could allow some blinded operations, such as "oblivious RAM" and "deterministic encryption", and fancy hardware techniques like "Trusted Execution Environments," but these are either prohibitively expensive, rest on shaky theoretical grounds, or both.)

What vendors could do, however, is provide software to departments that they run on their own local computers to perform such operations. Despite years of hype-cycle boasting and investment, not all data analysis needs to be carried out as a cloud service — and for organizations such as police departments, there are compelling reasons not to do so. Open-source AI that can be run locally is getting more powerful by the day (lagging cloud frontier models by only a year according to some analyses). The data operations that can be done locally should be more than enough for any police needs; that's doubly true considering that many uses of AI in law enforcement are highly suspect from a civil liberties perspective anyway.

## *VII. How policymakers can fight back*

This trend can be stopped and its consequences blunted by policymakers. Among the steps that can be taken:

A) **Mandate the use of local rather than cloud services.** Policymakers should create contracting requirements or other mechanisms to ensure police departments restrict their sharing of law enforcement data and limit its handling and analysis to hardware and/or software that does not make that data available to private vendors. It's certainly nothing new for policymakers to regulate law enforcement technology; many police departments, for example, have been prohibited from using Chinese drones.

B) **Limit commercial end runs around the Constitution**. Passage of the Fourth Amendment is Not For Sale Act, or similar federal or state legislation, would limit the inclusion of information purchased from commercial data brokers in policing. This measure has broad bipartisan support, having passed the US House in 2024 (before dying in the Senate).

C) **Bring antitrust authorities to bear.** Exercise of anti-trust authorities in markets providing products for police departments would help reduce the concentration of data and power in the hands of a corporate monopoly, duopoly, or oligopoly.

D) **Increase transparency.** Vigorous policymaking to ensure the transparency of data collection and analysis practices in police departments and their contractors is necessary for policymakers to evaluate the ongoing evolution of this area.

E) **Enact CCOPS.** Community Control Over Police Surveillance laws require police departments to get permission from their community, through their elected city council representatives, before deploying surveillance technology. That helps guarantee local communities maintain transparency into and democratic control over the technologies used by the police departments that serve them.

F) **End mass surveillance**. Reducing the amount and sensitivity of the data that flows into police departments can also help reduce the stakes around the corporatization of police departments. Not collecting data about entire communities and how they're living their lives through mass surveillance systems such as Flock's ALPR network is a big way to reduce such data.

###