The Center for Just Journalism
Electronic Frontier Foundation
IPVM

Selling Safety: A Journalist's Guide to Covering Police Technology

Selling Safety: A Journalist's Guide to Covering Police Technology

Introduction

Sold as modernization, reform, and a "tough on crime" fix, police technology[1] and its uses are increasingly diffuse. The industry regularly churns out new surveillance tools, often at the expense of privacy and civil liberties, not to mention taxpayer dollars. While some of these purchases are funded through federal grants and private donors, they are also becoming a larger portion of local and state budgets.

Ask a police department or a vendor and you'll often hear confident claims of measurable safety gains and bias reduction. When encountering those claims, it's important to bear in mind that policing technology is a multibillion dollar industry with sophisticated public relations teams built to win procurement fights and shape media coverage of their products. When an agency signs a contract – or even starts a trial – vendors often provide that agency with prewritten press releases, case studies, and talking points that present the tool as a proven success. When journalists parrot these police statements without verification, they risk turning the newsroom into a distribution channel for the surveillance industry.

This guide helps journalists see through the spin. It breaks down how policing technology companies market their tools and how those sales claims – which are often misleading – get recycled into media coverage. We offer tools for asking better questions, understanding incentives, and finding local accountability stories in your community.

[1] In this guide, "police technology" means digital tools or devices specifically designated to help a department combat crime. These usually involve surveillance–collecting information from the public via physical devices (e.g., cameras) or operations that provide access to phones, smart-home devices, or digital platforms. These technologies can also involve analysis (e.g., facial recognition tools or predictive algorithms that claim to anticipate where crime will happen or who will commit it). Many products combine collection and analysis (e.g., automated license plate readers or acoustic gunshot detection software).

How Police Technology Is *Marketed and Acquired*

Authors: *Matthew Guariglia* and *Beryl Lipton*, *Electronic Frontier Foundation*

Marketing

Police technology companies have a number of strategies to convince potential customers to consider, try, and buy their products. Companies seed news stories, shape existing customers' talking points, and pay public officials to attend demos (e.g., this offer from Verkada for a $200 gift card for booking a demo).

Vendors also work the conference circuit—the International Association of Chiefs of Police (IACP), the National Sheriffs' Association, assignment-specific gatherings (e.g., campus policing and tactical units), and broader security expos. Companies set up booths, run demos, hand out branded trinkets, and host parties and happy hours (e.g., a 2018 IACP party featuring Shaquille O'Neal).

Press releases announcing acquisitions or trumpeting a crime "solved" with a new product are often prewritten by vendor marketing teams. For police departments, access to polished PR is a perk of the contract, but it's also advertising for the vendor, which often gets repeated uncritically by local news. Flock Safety, an automated license plate reader (ALPR) vendor, previously distributed a toolkit to its police customers offering "resources and templates for public information officers." A Flock draft press release reads:

"The ___ Police Department has solved [CRIME] with the help of their Flock Safety camera system... ____ Police installed Flock cameras on [DATE] to solve and reduce crime in [CITY]."

The AI Hook

Companies often market their products as artificial intelligence (AI) in an effort to tap into AI's reputation for being advanced and sophisticated. This practice exploits public unfamiliarity with new technologies and masks the limits of certain products.

For example, a popular AI-powered safety technology, a weapons detection system made by a company called Evolv, was rebuked by the Federal Trade Commission (FTC) for deceptive advertising. Evolv claimed that its scanners used artificial intelligence to tell the difference between weapons and harmless items (like phones or keys). When the system was piloted in the New York City subway, it didn't detect any firearms, and out of 2,749 scans, it found just twelve knives – and triggered 118 false positives. In Utica, NY, a high school student was stabbed with a large tactical knife that went undetected by the company's technology.

In the proposed FTC settlement, Evolv would be banned from continued "unsupported claims" about its products' ability to detect weapons by using artificial intelligence. (This was part of a larger FTC action against deceptive use of or claims around AI in marketing called Operation AI Comply.) Evolv's founder publicly apologized, but the product continues to be sold, including to hospitals run by the Department of Veterans Affairs.

Flock, SoundThinking, and other companies selling gunshot detection systems, many of which rely on AI, claim to have very high accuracy rates, but independent data from cities (including San Jose and New York) shows far lower confirmation rates. Alerts are often triggered by sounds like fireworks or cars backfiring. In some cases, audits have found that only a very small fraction of alerts are confirmed shooting incidents, prompting Chicago, Champaign (IL), and other cities to cancel contracts.

Companies often hide the limits of their AI security technologies behind the label of "proprietary." A state audit in Utah found that Banjo, a company with a multimillion dollar contract to provide what it called real-time AI monitoring of public data and video feeds, "lacked the advertised AI technology" altogether and that the work could have been done by a "skilled operator."

It's not an isolated case. Amazon's heavily publicized "Just Walk Out" stores, which supposedly use AI to recognize the products its customers pick up and automatically charge them for it, was actually powered by humans in India watching video footage of the stores. (See the following section of this report for information about the risks of surveillance technologies that actually do use AI.)

Police Officers as Sales Reps

What looks like word of mouth ("one town credits a new technology with a drop in crime and neighbors want in") is often engineered. Vendors may recruit officers to leverage their relationships with other departments, asking current or former police officers to introduce sales teams and join pitch meetings. Many sales reps are ex-police who built their sales skills on the job.

In one email, obtained through a public records request, a Colorado police officer told a major vendor he was "already doing sales," listing demos of their products he'd run for other departments. Another example is the Atlanta Police Department's Chief Administrative Officer, Marshall Freeman, who was found to have violated ethics codes by working for Fusus, a subsidiary of body camera vendor Axon, in exchange for stock.

Officers who demonstrate that they can market and demo tools to other agencies also burnish credentials for private sector jobs. Some firms even publish guides for moving from law enforcement into private sector roles, tightening the close relationship between the two industries.

Incentives and Perks

The surveillance technology market is shot through with unseen incentives. Even when these technologies (e.g., Flock ALPRs or Amazon Ring cameras) are sold to non-police customers, the companies may offer no-cost portals that make it easy for police departments to request customer footage. When, for example, an HOA installs Flock cameras, police officers often can pull data from Flock's private systems at no charge. These arrangements incentivize police to steer communities towards brands offering the most convenient law enforcement tools.

The incentives can also be personal. Reporting by the Los Angeles Times and EFF showed that, in 2016, Amazon gave LAPD officers personalized Ring Doorbell Camera discount codes; when residents used an officer's code, the officer earned rewards like free devices. That raises an obvious question: is a police officer's recommendation to acquire a certain technology about public safety or financial self-interest? (Ring has since changed aspects of its program, and its relationship with police departments has waxed and waned over the years.)

Acquisition

Police departments have several methods for purchasing these tools. They often tap federal grants that pay for equipment or enable transfers, like the Department of Justice's grants for body cameras and the Pentagon's 1033 program for surplus equipment transfer. Police foundations and corporate donors also underwrite purchases. Most commonly, agencies buy technologies directly with their operating or capital budgets – meaning the community pays for it.

Grants

Grants are a common way to pay for tools that might not survive local budget scrutiny. Vendors don't want a tight budget or hesitant city council to kill a sale, so many offer grant-writing assistance to find outside money. Flock Safety, for example, advertises no-cost help for automatic license plate reader grants; similar programs exist at Teledyne, Motorola Solutions, Axon, and others. While grants may fund the initial purchase or installation of police technology, they do not always cover the future costs of the technology. Some products have "lock-in" systems that make it difficult to switch vendors or render equipment inoperable unless agencies continue to make payments. Security vendors like Verkada use a subscription-like model, licensing software for a certain term – often one or three years. When licenses expire, customers must either purchase new licenses or their cameras, door locks, and other devices will no longer work. As Verkada's chairman Hans Robertson once observed, customers cannot easily switch: "you, like, literally bolted the hardware to your ceiling so like you're not taking it down."

Specialized Public Funds

When specialized state or federal funds are in play, vendors may rebrand to match the moment. In 2020, during COVID's peak, several crime prevention products were repackaged as public health tools (e.g., facial recognition for contact tracing and drones for fever detection). This rebranding allowed technology companies to keep sales up during a period of heightened skepticism towards police and helped police departments acquire technology they might not have been able to purchase with their own funds. In Mesa, Arizona, for example, a staggering $3.3 million dollars of federal COVID response money went to building a massive surveillance center the city had previously been trying to fund. These systems outlive the crises used to justify them. Today's "retail theft" drone can become tomorrow's protest surveillance.

Assessing the Efficacy of Police Technologies

Author: Conor Healy, IPVM

When a new policing technology arrives in our communities, officials often neglect the most foundational questions: Does it work? Who says so? How do they know? A multitude of past examples show us we should never assume these questions have been satisfactorily answered, or even asked.

Security vendors often rely on a culture of technical mystique and public urgency, assuming few will probe the underlying evidence. But an honest debate over privacy, civil liberties, or budgetary trade-offs depends first on knowing whether the promised benefits are even real. Moreover, inaccurate information about how well a technology performs doesn't just mislead the public, it misleads police officers too. When police do not seek to understand a technology's limitations, they may arrest innocent people based on faulty results while wasting investigative resources – and, in numerous cases, they have.

Consider these newspaper headlines:

- Arrested by AI: Police ignore standards after facial recognition matches, The Washington Post
- I Was Wrongfully Arrested Because of Facial Recognition Technology. It Shouldn't Happen to Anyone Else, Time
- NC police errors with license plate cameras brought wrongful arrests, $70K to women, The News & Observer
- A 61-year-old man sues Macy's, saying he was jailed and assaulted after being falsely identified as a store robber by facial recognition, Business Insider

Technologies that rely on AI, as many new security technology tools do, pose a particular risk because they are probabilistic rather than deterministic. Put simply, there is always an element of guesswork to AI's analysis, such as when used to classify or detect patterns in data, images, or videos, from faces to license plates to crowd movements.

Every deployment is an experiment with an outcome that depends on myriad factors – lighting, angles, demographics, image quality, even climate – that marketers often don't disclose. "AI-powered" does not mean "reliable." It means "unproven until verified." (See the previous section of this report for more on situations in which technologies marketed as AI aren't actually AI at all.)

Vendors often make unsubstantiated claims, manipulate statistics, and engage in misleading marketing to justify expensive surveillance purchases. Even the Security Industry Association (SIA), an industry advocate, acknowledges the pattern. In 2024, SIA's CEO said on a manufacturer podcast:

"One of the main challenges I think we see, from the association perspective, is the amount of marketing spin that's out there professing that a certain solution is going to do a certain thing. And, anecdotally, it really doesn't turn out that way sometimes. Right? And that's not good for the image of the security industry, let alone the manufacturer or the solution provider."

For example, misleading claims concerning the accuracy of facial recognition might appear to rely on independent statistics, but they often don't. Companies routinely advertise "over 99% accuracy," citing evaluations from the National Institute of Standards and Technology (NIST). Vendors and law enforcement alike frequently invoke such figures as proof of reliability.

But NIST's tests are conducted in highly controlled laboratory conditions. In the real world, surveillance cameras are subject to indirect angles in untrained environments, constantly changing lighting and weather, and infinite combinations of other confounding factors. The real world is not a NIST lab.

That's why substituting NIST's results for real world performance expectations is like deeming an airplane fit for flight because it aced a wind tunnel test. For journalists, the correct question is not, "What's the accuracy rate?" but "Under what conditions was that rate achieved, and do those conditions match how our community is using the technology?"

Examples:

- **Clearview AI**: Clearview takes the sleight-of-hand a step further. On its "Principles" page, the company says it "only provides results for human review using the same algorithm and match threshold settings that achieved 99% or better accuracy on key tests" and that results that fall below that threshold are withheld. That sounds like each result you see is "99% accurate" but this isn't the case. This actually means only that Clearview is optimizing a bit more for what worked under controlled test conditions.
- **Flock Safety**: In the ALPR space, Flock Safety exemplifies this pattern of misrepresentation. Flock has aggressively marketed claims that their technology can help "eliminate crime" and that 10% of reported crime in the U.S. is solved using their tools. Six academic reviewers consulted in a Forbes investigation of Flock described the company's claims as "problematic" and "bordering on ludicrous." Even Flock's own FAQ page contradicts itself—claiming in one section to help solve "2,200+ crimes per week" and in another, on the same page, "1,000+ per day." Flock also refuses to permit independent testing of its technologies.
- **Evolv Technology**: Evolv markets AI-driven weapons detection systems to schools, stadiums, and hospitals under the promise of superior safety. When the company publicized results from an ostensibly "independent" evaluation by the University of Southern Mississippi's National Center for Spectator Sports Safety and Security, it appeared to offer verification. But a joint investigation by IPVM and the BBC later uncovered the full, unredacted test report, revealing that Evolv had collaborated with the lab to conceal failures and inflate effectiveness claims. The company simultaneously refused to allow IPVM direct access to its hardware for independent testing.

Obstruction of independent testing is a recurrent problem. A growing number of surveillance technology companies simply deny researchers, journalists, or local governments the ability to verify whether their products work at all. Without independent testing, public agencies buy on faith, guided only by the claims of those who profit from the procurement.

Far from seeking verification, police departments routinely amplify unsubstantiated vendor marketing claims when justifying surveillance technology purchases to city governments and the public. The reality is that law enforcement officials often lack the expertise to independently assess what vendors say about their products, creating an environment in which false promises go unchallenged, public money is wasted on ineffective technology, and "safety" is scaffolded not by genuine innovation but a dangerous false sense of security. When police agencies not only overlook unverified claims, but coopt them as official promises, the implications extend far beyond wasted budgets: the public bears the risk.

Opportunities for Reporting

Authors: *Beryl Lipton*, *Electronic Frontier Foundation*, and *Hannah Riley*, *The Center for Just Journalism*

This section highlights concrete ways to investigate the use of police technologies. It includes story ideas for examining community impact, vendor influence, procurement processes, and scope creep; key questions that help reporters understand what data is collected, how it is used, who can access it, and what risks it creates; and targeted public records to request.

Story Ideas

- **Report on community impact**. Talk to community members about their experiences with police technologies. Map racial and economic patterns of deployment. Ask public defenders how these tools show up in cases.

- **Follow the money**. These tools are often introduced via public-private partnerships, with little debate. Track lobbying, campaign contributions, and close-knit relationships between officials and vendors.

- **Analyze procurement processes and contracts**. Investigate whether there were competitive bids for the contract. Determine what the renewal terms for the contract are and whether there is a “free trial” hook. Find out if there are training obligations for the people using the technology. Find out who owns the data collected by police.

- **Report on scope creep**. Pilot programs often expand quietly once they are established. Determine whether the program has evolved from the original stated purpose (e.g., ALPRs being used for ICE surveillance or tracking abortion seekers).

- **Help people understand vendor influence**. Investigate whether vendors are shaping public policy behind the scenes. For example, have any of your community’s former police chiefs or city officials gone to work for police technology companies?

- **Learn more about places where the technologies have failed**. Identify cities that have rolled back or stopped using these products. Find out why and what lessons might apply more broadly.

- **Go beyond policing**. Many of these systems also operate in schools, hospitals, public housing, and transit. Investigate how these technologies function in those spaces.

Questions to Ask Along the Way

- **What data are the technologies collecting?** The data being collected by police departments and the companies they work with can come in many forms. Video, audio, biometrics, vehicle information, mobile location, social media posts, information made available through data breaches, etc... There is so much information out there, and police can gather and access it through devices they host or platforms to which they purchase access.

- **How and where is the data being collected?** The methods by which police gather data and the points of collection can be very telling. If police want to place license plate readers in your city, are there particular neighborhoods where fixed cameras will be installed? And why were those locations chosen? If they want mobile ALPRs, do police plan to keep them running constantly as they patrol, vacuuming up information from parked cars and other vehicles they encounter? Or do they intend to deploy that technology on drones or in other ways? If they are using a so-called “intelligence platform” to integrate and analyze data, does that platform provide access to mobile phone information or information made available through data breaches?

- **For how long will the data be stored? Is there a specific retention period in place, and what is the justification for it?** The longer data, like ALPR scans, is stored, the more vulnerable it is to abuse, inappropriate access and sharing, and unintended integration with other data systems. It’s important to understand whether the data will be deleted at some point. Try to find out if third-parties are able to copy and share that information, especially as data increasingly feeds into artificial intelligence training systems.

- **With whom is the data shared? For example, will it go to other police departments, state agencies, or federal law enforcement, like ICE?** It can be difficult to ensure that data is only being accessed by authorized parties, especially if there isn’t clear policy around who those parties are and police authorities do not know how to set up the proper permissions for access or penalties for access violations.

- **Will vulnerable communities (e.g., Black, LGBTQ+, immigrant, and activist residents) be impacted by this surveillance, and how will potential harms be mitigated?** It is important for communities to think through the intended uses of surveillance and the potential for unintended harms. Will these tools be deployed in communities of color or against peaceful protestors? Will AI-driven analyses use data from flawed, biased policing practices or make assumptions about behavior or individuals in an unfair way?

- **Have the purposes for which the system may be accessed or used been clearly defined?** What are those definitions, and how will authorities ensure that officers are abiding by them? Without clearly defined reasons for using surveillance technology, officers may not understand the appropriate limits of their access or may not face any consequences when clear misuse occurs. Unfortunately, police officers have used surveillance and data systems inappropriately and for abusive purposes, and it's crucial for the public and police officers to understand what is permissible. Can officers access data for any crime (or whim), or is access only appropriate for specific investigations? Must officers show reasonable suspicion or probable cause that crime has occurred? Must they obtain permission from a supervisor, department executive, or a judge?

- **Who will be permitted to access the tools and data? How will these people be trained, and who will be doing that training?** Absent a clear policy around who is actually allowed to use a system, a police agency may be facilitating random access to any officer or employee. Password sharing, unclear access guidelines, and even access by tech company employees can occur. Be sure to get clarity on which individuals and roles are actually allowed to use these tools, how they'll be trained in appropriate use, and what discipline they receive if they violate those protocols.

- **How will the system be audited, and will the results of those audits be made public?** If there is no process by which access and use are reviewed, abuse and misuse can go undetected, creating serious harm and undermining the mission of public safety. Ask about how agencies intend to review engagement with surveillance tools and whether there will be transparency with the community about any failings that are identified.

- **Have data breaches or unauthorized access previously occurred with this technology or company?** It is important to understand if and how data breaches occurred in the past. How are the vendor and the police department preventing unauthorized access to this information? If there were violations of access or breaches, how were they addressed and how will they be prevented in the future?

- **How much does the system cost and how will it be funded?** Surveillance tools and systems rarely involve a one-time cost. Increasingly, surveillance systems or access to certain devices rely on regular subscription and other ongoing costs. What will these costs be, today, this year, next year, and for the foreseeable future?

- **How will the effectiveness of the technology be measured and evaluated?** Too often, grand claims about a tool's effect on crime or clearance rates are touted as justifications for its use without any plan for substantiating those claims and evaluating their validity. Ask your local officials how they intend to gauge the impact of surveillance on their operations.

Accessing Public Records About Police Technology

You can surface a lot of information about how tools are actually used—and whether they work the way they are promised to—through public records.

General Records and Resources

- **Procurement:** Monitor city and state bid portals and contract databases (e.g., "Current Bid Opportunities" and "Current/ Expiring Contracts"). Once awarded, look for contracts, specs, and deliverables. The federal usaspending.gov portal is a useful complement. Paid aggregators (e.g., GovSpend) can help but aren't comprehensive; learn your local systems.

- **Policies:** Internal policies reveal guardrails (or gaps), audit expectations, and what records should exist.

- **Training & user manuals**: Manuals are gold for targeted requests. (EFF used an ALPR manual to pinpoint exactly where sharing lists were downloadable, enabling precise FOIA language.)

- **MOUs & data-sharing agreements**: These documents show who gets access and on what terms (e.g., agencies, vendors, fusion centers).

- **Communications**: Target named individuals and ranges of dates. Emails often reveal sales funnels (the path someone takes from first hearing about a product to eventually buying it), efficacy claims, and internal skepticism.

Specific Records to Request

User manuals and agency- or jurisdiction-specific policies and information will help you to craft more effective public records requests. Here are some ideas for the kinds of specific information you can request, along with sample request language at the link following each category.

- **Pilot programs and trial use:** Before fully rolling out a tool, a department might run a pilot program or a vendor might grant access to the technology as part of a trial. Understanding what a department measures and doesn't track during these trial periods can be enlightening. (Sample record request here.)

- **Automated license plate readers (ALPRs):** ALPRs rely on a wide data-sharing network that can cross state lines and blend jurisdictional information, sometimes against state law. To understand that network, request data-sharing agreements and information that details the other entities with which a particular agency shares and receives data. (Sample record request here.)

- **Automated police reports:** Audio and video can be fed through AI to generate police reports, raising concerns about accuracy and the effect such automated police work will have on the fair application of the law. (See here for EFF's Guide to Getting Records About Axon's Draft One AI-Generated Police Reports.)

- **Body-worn cameras (BWCs):** BWCs capture video and audio that can be used in lots of ways, including in the automated generation of police reports and in the way prosecution or police accountability play out. Footage and other details can be made available via public records request. (Sample record request here, along with other examples on MuckRock.)

- **Cell-site simulators (CSS):** CSS can capture data transmitted via mobile phones from individuals within a particular area. As one of the more obviously invasive technologies police might use, it is often one they are more likely to avoid disclosing information on. However, procurement rules still require disclosure of some information (see this example from Massachusetts), and more specific information may be made available via a public records request. (Sample record request here.)

- **Drones and drone-as-first-responder programs (DFR):** Drone and DFR use is growing a lot. Many police departments have webpages that host information on drone flights, the reasons for flying, and other details on their deployment, but they may not include all of the relevant information. (Sample record request here.)

- **Face recognition technology (FRT):** FRT can be added to devices or applied to photos and video retroactively. In addition to inaccuracies that can result in wrongful arrests, the application of FRT may also be unfairly targeted toward particular demographics. (Sample record request here.)

- **Axon Fusus:** Fusus lets police tap into private cameras, including doorbell footage, and puts real time crime center tools on police officers' phones, which makes it easy for surveillance to expand far beyond what departments may have intended. One report found that use of Fusus resulted in disproportionate surveillance of a playground at a housing development. (Sample record request here.)

- **Gunshot detection:** Gunshot detection typically relies on the placement of microphones in neighborhoods, which may be recording audio at all times. (Sample record request here.)