

Ban ALPRs

ALPRs Compromise Privacy

The nationwide privacy debate surrounding tracking technology is clear: mass surveillance is a threat to civil liberties [22, 17]. Flock’s product, Freeform, exemplifies this danger [19]. The slogan “Type What You Know. Find What You Need.” and example searches such as “blue shirt and cowboy hat” or “woman with red handbag”, reveal a tool that is as invasive as possible. When paired with ubiquitous street cameras, these wide nets ensure that every one of us is eventually tracked, cataloged and scrutinized.

ALPRs Compromise National Security

Data from a hacked border-crossing database allowed European journalists to unmask a GRU spy who was attempting to infiltrate NATO [21]. While this intelligence provided a defensive benefit, imagine that database was in the hands of a hostile nation. Flock is constructing an exponentially more detailed record of *everyone’s* movements across the country. The threat isn’t limited to opportunistic criminals; the most sophisticated actors are state-sponsored groups operating on behalf of rival nations [10, 23].

Data Attracts Hackers

Hackers love large, centralized databases. The value they can generate from selling data, or otherwise exploiting it, grows with the amount of data they obtain. This simple fact means *anywhere* that data is centralized will be subject to frequent attacks. 170m social security numbers were exposed in the National Public Data breach [1]. Cambridge Analytica exploited Facebook to gain data on 32m US users [1]. 40m payment card records were exposed in a Target hack [1]. Recently, 153m drivers licenses were exposed when an identity verification service was hacked [11, 20]. Flock is yet another company putting our data at risk for their profit.

Flock Is Insecure

In 2025 a single security researcher found multiple, significant vulnerabilities in Flock’s Falcon cameras [8, 5, 7, 4, 3, 6]. In 2026, hackers successfully breached the data within a Flock camera [13]. The logs they recovered revealed that the camera system was tracking *people*, not just license plates. The rate of vulnerability discovery isn’t going to slow down any time soon, in fact AI is speeding it up. Security researchers are seeing a growing storm of new vulnerabilities and hacks [18].

Flock Will Expand Their Capabilities

As roadside installations become saturated, Flock will naturally expand its capabilities to maintain growth. The rapid pace of AI development will only accelerate this expansion. AI enables Flock to engineer new products faster and, more critically, it enhances their tracking power. Leonardo, another mass surveillance company, is already capable of tracking the identity of *individuals* in a passing car [16]. This ongoing increase in capability makes Flock an irresistible target for hackers, ensuring that any major breach will have catastrophic fallout.

Flock Is Not Unique

Insight LPR, which is partnered with Axon, and Motorola Solutions both have mature ALPR systems available [12, 9, 14]. OpenALPR is an open source ALPR suite [15]. Open source software can easily be copied or directly used by another company. That means that Flock’s core business, automatic license plate readers, doesn’t have much, if any, technological moat. Simply banning Flock leaves room for another company to creep in and do the same thing.

Ban ALPRs

ALPR technology erodes privacy and will always be lucrative to hack. To protect our community, Frenchtown must adopt an ordinance similar to Ypsilanti’s ordinance 1401 and ban automatic license plate reader technology [2].

References

- [1] Kyle Chin. *Biggest Data Breaches in US History*. 2026. URL: <https://www.upguard.com/blog/biggest-data-breaches-us>.



- [2] CITY OF YPSILANTI NOTICE OF ADOPTED ORDINANCE *Ordinance No. 1401*. 2022. URL: <https://cityofypsilanti.com/ArchiveCenter/ViewFile/Item/743>.



- [3] gainsec. *Flock Safety admin API unauthenticated*. CVE-2025-59403. 2025. URL: <https://www.cve.org/CVERecord?id=CVE-2025-59403>.



- [4] gainsec. *Flock Safety DataDog API key exposed*. CVE-2025-59405. 2025. URL: <https://www.cve.org/CVERecord?id=CVE-2025-59405>.



- [5] gainsec. *Flock Safety Java Keystore and password recoverable*. CVE-2025-59407. 2025. URL: <https://www.cve.org/CVERecord?id=CVE-2025-59407>.



- [6] gainsec. *Flock Safety LPR hardcoded system password*. CVE-2025-47823. 2025. URL: <https://www.cve.org/CVERecord?id=CVE-2025-47823>.



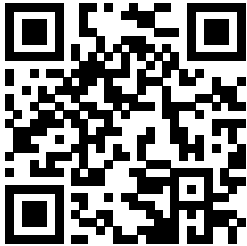
- [7] gainsec. *Flock Safety OAuth secret exposed*. CVE-2025-59406. 2025. URL: <https://www.cve.org/CVERecord?id=CVE-2025-59406>.



- [8] gainsec. *Flock Safety Wi-Fi credentials stored in plaintext*. CVE-2025-59409. 2025. URL: <https://www.cve.org/CVERecord?id=CVE-2025-59409>.



- [9] *Insight LPR - Axon.com*. URL: <https://www.axon.com/partners/insight-lpr>.



- [10] Mohammed Khalil. *State-Sponsored Hacking: Global Trends and How to Defend in 2025*. 2025. URL: <https://deepstrike.io/blog/state-sponsored-hacking-apt-threats-2025>.



- [11] Brian Krebs. *FBI Probes Service Selling 153M+ Drivers Licenses*. 2026. URL: <https://krebsonsecurity.com/2026/09/fbi-probes-service-selling-153m-drivers-licenses/>.



- [12] *License Plate Recognition Technology | Insight LPR*. URL: <https://insightlpr.com/>.



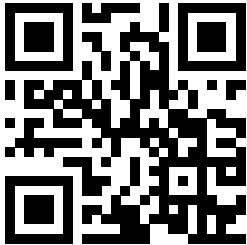
- [13] Dhruv Mehrota and Joseph Cox. *Hackers Got Inside a Flock Camera. Its Data Shows How the System Really Works*. 2026. URL: <https://www.wired.com/story/hackers-flock-camera-data-shows-how-system-works/>.



- [14] *Motorola Solutions License Plate Readers*. URL: https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems.html.



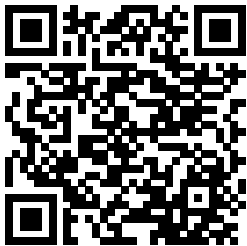
- [15] *OpenALPR*. URL: <https://www.openalpr.com/>.



- [16] *SignalTrace(tm): Investigative Evidence From Electronic Devices*. URL: <https://www.leonardocompany-us.com/lpr/elsag-signaltrace>.



- [17] *Street Level Surveillance: Automated license plate readers*. 2023. URL: <https://sls.eff.org/technologies/automated-license-plate-readers-alprs>.



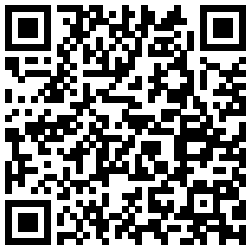
- [18] *The AI Vulnerability Storm*. 2026. URL: <https://www.sonatype.com/resources/research/ai-vulnerability-storm>.



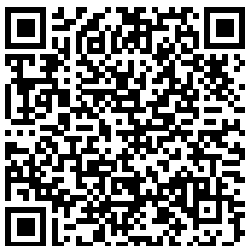
- [19] *Type What You Know. Find What You Need*. URL: <https://www.flocksafety.com/products/flock-freeform>.



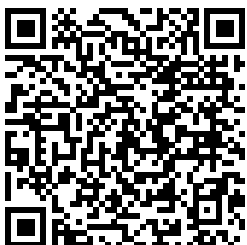
- [20] Tom Uren. *America's Driver's License Breach is a National Security Disaster*. 2026. URL: <https://www.lawfaremedia.org/article/america-s-drivers-licence-breach-is-a-national-security-disaster>.



- [21] Tom Uren. *Bellingcat and Cyber Partisans Burn GRU Illegal*. 2022. URL: <https://news.risky.biz/the-case-against-western-propaganda-65c0eb42a0e6da001a37dfef/#bellingcat-and-cyber-partisans-burn-gru-illegal>.



- [22] *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*. 2013. URL: <https://www.aclu.org/documents/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements>.



- [23] Miles Yu. *The Great Chinese Data Heist*. 2026. URL: <https://www.hudson.org/foreign-policy/great-chinese-data-heist-miles-yu>.

