

United States Senate
WASHINGTON, DC 20510-2509

September 2, 2026

Filip Kaliszan
Chief Executive Officer
Verkada
406 E. 3rd Ave
San Mateo, CA 94401

Dear Mr. Kaliszan:

As Chairman of the Senate Judiciary Subcommittee on Crime and Counterterrorism, I am investigating your company's collection, retention, and dissemination of the data generated by its artificial intelligence surveillance cameras.

On August 26th, I wrote to your competitor Flock Safety to express my concerns regarding the size and pervasiveness of its network and demanding answers as to reports of abuse and costly errors from its technology. However, Flock does not stand alone in this industry; you and others are building large camera networks, assisted by artificial intelligence, that intrude on the privacy of all Americans.

Taking Flock alone, in a few short years, Flock has assembled an unprecedented national surveillance network. Flock boasts more than 120,000 cameras across 49 states and more than 20 billion vehicle scans every month.¹ The overwhelming majority of the Americans captured in those records did nothing wrong. Instead of serving discrete local investigations, as contemplated by our constitutional processes and safeguards, these camera networks harness artificial intelligence to pool what they capture into a national database that customers can search.²

Recent examples of abuse and misuse of personal data reveal the woeful lack of safeguards in these systems. Last month in Missouri, the St. Charles County Police Department terminated its contract with Flock after an audit revealed that a civilian employee had run Flock searches for personal reasons, completely unrelated to his or her law enforcement duties.³ Sadly, my home state is not an outlier. In Milwaukee, prosecutors charged a police officer who allegedly used Flock to search his girlfriend's license plate 124 times and her former boyfriend's plate 55 times, entering "investigation" as his justification each time. Worse still, the officer was not caught by Flock's audit systems—he was caught because a private citizen looked up his own plate on a public website.⁴

Errors and false positives add insult to injury. A Florida woman spent 13 days in jail and faced eight felony counts, including three counts of vehicular homicide, after investigators arrested an owner based on their search of Flock's network for a vehicle description. Prosecutors dismissed the charges seven months later when law enforcement discovered the error and arrested a different person.⁵ One California police department found that a staggering 71% of Flock alerts were wrong, and the Los Angeles Police Department

¹ <https://www.flocksafety.com/blog/the-price-of-free-lpr>

² <https://www.wired.com/story/flock-safety-os-investigate/>

³ <https://www.kcur.org/news/2026-08-23/flock-cameras-misuse-missouri-st-charles-county-police>

⁴ <https://reason.com/2026/08/13/flock-cameras-and-license-plate-readers-are-everywhere-can-we-trust-cops-with-them/>

⁵ <https://www.yahoo.com/news/us/articles/florida-woman-spent-13-days-170100471.html>

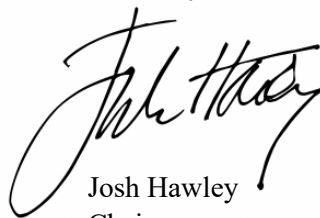
dropped its Flock contract after an audit showed officers had stopped 161 vehicles incorrectly flagged as stolen in the space of two months.⁶

Furthermore, once cameras collect driver data, uncertainty abounds in how your company and its customers can sell or use data. The multi-billion-dollar valuations that are common among your peer companies come with enormous pressure to find new commercial applications. Americans demand a full accounting of how their driver data is stored or sold.

To be sure, I want law enforcement to have tools to catch offenders and keep the public safe. But the surveillance network your company has constructed raises legitimate concerns about how little-known corporations possess intimate knowledge of Americans' lives, fueled by invasive artificial intelligence algorithms. The Supreme Court recognizes that a comprehensive, retrospective record of a person's movements is different in kind from ordinary observation in public,⁷ and Congress never authorized the network your industry has built. Your company's internal policies are, in practice, the only safeguards for hundreds of millions of Americans. People across the country are now discovering that fact and demanding answers from their elected officials.

The American people want to know who has access to their personal data and how. This investigation will seek those answers. To facilitate that, please produce all documents and information specified in the attached annex no later than **September 16, 2026**. If you have questions about the scope of these requests, please contact my office to discuss.

Sincerely,

A handwritten signature in black ink, appearing to read "Josh Hawley", with a stylized flourish at the end.

Josh Hawley
Chairman
Subcommittee on Crime and Counterterrorism
Committee on the Judiciary

⁶ <https://reason.com/2026/08/13/flock-cameras-and-license-plate-readers-are-everywhere-can-we-trust-cops-with-them/>

⁷ See *Carpenter v. United States*, 585 U.S. 296, 309-10 (2018).

ANNEX

DEFINITIONS

1. **“Document”** means any recorded information in any format, medium, or form, whether written, printed, typed, electronically stored, photographed, filmed, or otherwise preserved, including: emails, text messages, ephemeral messages (e.g., Signal, Telegram, etc.), Slack, Microsoft Teams, Discord, any internal messaging platform, instant messages, source code, application logs, moderation logs, user-report records, dashboards, slide presentations, spreadsheets, financial models, board minutes, board packages, audit reports, legal memoranda, contracts, agreements, regulatory correspondence, engineering specifications, product roadmaps, and design documents, in final and draft form, wherever they may be.
2. **“Company”** means Verkada Inc., d/b/a Verkada, together with each of its predecessors, successors, parents, subsidiaries, divisions, affiliates, joint ventures, and any entity in which it holds a controlling interest, whether foreign or domestic; each of its present and former officers, directors, employees, contractors, consultants, agents, attorneys, and representatives acting on its behalf; each entity operating under a trade name or product name used by the Company; and any other person or entity acting for or on behalf of any of these entities. Where a request concerns documents or information in the Company’s possession, custody, or control, that phrase includes documents and information held by any third party from which the Company has the practical ability to obtain them, including cloud service providers and any entity that hosts, processes, or stores data on the Company’s behalf.
3. **“Relevant Period”** means January 1, 2021, through the present, unless a specific request states otherwise.

INTERROGATORIES

Please answer each of the following in writing. If your company declines to answer any question in whole or in part, state the basis for that refusal. If your company lacks information sufficient to answer, describe the efforts undertaken to obtain it.

1. State the parameters under which your customers can conduct a statewide or nationwide search of vehicle or driver data, as well as whether those features are enabled by default.
2. State the default retention period for each category of data your company collects, and identify every change to that default since January 1, 2021, including the date of each change and the reason for it. State the maximum period a customer may select, whether your company’s approval is required to exceed the default, and how many customers currently retain data beyond the default.
3. State the total number of confirmed instances of misuse of your company’s systems or data known to your company, by year, since January 1, 2021. For each, state whether the misuse was first identified by your company’s own monitoring, by the customer, or by a third party.
4. Describe what a user must enter to justify a search. State whether that entry is validated against any external record, whether a supervisor must approve it, and whether a search proceeds if the field is left blank or filled with generic text such as “investigation.”

5. Describe every restriction your company imposes on the purposes for which its systems may be searched. State whether your company has assessed whether those restrictions can be circumvented and, if so, the result of that assessment.
6. State your company's measured accuracy at the level of a complete and correctly attributed vehicle identification. Identify the testing that produced that figure and state the rate at which alerts are later determined to be incorrect.
7. Identify every category of data that your company's deployed devices capture, including still images, video, audio, wireless signals, and any biometric identifier. For each, state the date on which your company began capturing it and whether customers may decline.
8. State whether your company links data captured by its devices to any external data source, and identify each such source, including commercial data brokers and public records aggregators. State whether your company has ever ingested, licensed, evaluated, or tested data obtained from a security breach.
9. State whether multi-factor authentication is required of all users and, if it has not always been required, when it became mandatory.
10. Describe in detail whether your company has the capability to biometrically track individuals and explain what physical or technical limitations exist or are imposed on such biometric tracking.

DOCUMENT REQUESTS

1. All policies, procedures, and training materials governing the process by which a law enforcement agency or other entity obtains access to your company's systems or data, including any vetting, accreditation, written policy, supervisory, or training prerequisites, and all documents concerning the waiver of any such prerequisite.
2. All documents concerning the siting of cameras and sensors, and all documents concerning notice to or approval by local governing bodies or the public before installation, including model ordinances, public-notice templates, signage specifications, and communications with local officials regarding whether public approval is required.
3. All policies and technical documentation concerning when your company's devices record or transmit data, whether recording can be suspended or disabled, who may do so, and whether any such change is logged.
4. All data retention schedules and policies, including default retention periods, the extent to which customers may extend or shorten them, the treatment of backups and of derived data such as vehicle fingerprints or model embeddings, procedures for verifying deletion, and the disposition of data upon termination of a contract.
5. All policies and technical documentation governing who may query your company's systems and the default geographic scope of a query, together with all documents concerning the sharing of data with other law enforcement agencies, federal agencies, foreign governments, private entities, or data brokers.

6. All policies and technical documentation governing the justification a user must supply to run a search, including whether that field is validated or free text, whether a warrant or supervisory approval is required for any category of search, and a description of every audit capability available to customers and to your company, including whether audit records are complete, immutable, and exportable.
7. All documents concerning any known or suspected misuse of your company's systems or data from January 1, 2021 to the present, including internal investigations, audit findings, notifications to customers, notifications to affected individuals, referrals to law enforcement, and any resulting change in policy or product design.
8. All documents concerning the accuracy of your company's products, including internal and third-party testing of character-level and plate-level read accuracy, false-positive rates for alerts, confidence thresholds and how they are displayed to users, representations made to customers or the public about accuracy, and all documents concerning any stop, detention, or arrest of an individual later determined to have been misidentified.
9. All documents concerning the security of your company's systems, including multi-factor authentication requirements, credential compromise, unauthorized access or exposure of camera feeds or stored data, penetration testing and remediation, the location and ownership of data storage infrastructure, and access to production systems by personnel or contractors located outside the United States.
10. All contracts, master service agreements, terms of service, data-processing agreements, and end-user license agreements executed with any governmental customer, together with all price lists, fee schedules, and documents concerning pilot programs, discounted or donated equipment, and any assistance your company has provided to customers in obtaining federal, state, or private grant funding.
11. All documents concerning categories of data other than license plate images that your company collects, ingests, licenses, or links to its camera data, including audio, video, facial or other biometric identifiers, commercial data-broker records, public records, and any data derived from a breach; and all documents concerning the use of customer or third-party data to train your company's models.
12. All documents concerning your company's sources of revenue and capital, including investors holding more than five percent of any class of equity, revenue derived from federal, state, and local government funds, the federal grant programs through which customers have financed purchases, lobbying expenditures, and political contributions.