RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–5244

United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

October 16, 2025

Mr. Garrett Langley
Chief Executive Officer
Flock Group, Inc.
1170 Howell Mill Road NW, Suite 210
Atlanta, GA, 30318

Dear Mr. Langley

On July 25, 2025, I announced that Flock had agreed to implement additional privacy protections for Oregonians to prevent abuses by federal and out-of-state agencies related to abortion and immigration enforcement. At the urging of concerned constituents, I conducted further oversight and have determined that Flock cannot live up to its commitment to protect the privacy and security of Oregonians. Abuse of Flock cameras is inevitable, and Flock has made it clear it takes no responsibility to prevent or detect that. For that reason, I must now recommend that communities that have installed Flock cameras reevaluate that decision.

Flock operates the largest network of surveillance cameras in the United States, reportedly contracting with more than 5,000 police departments, 1,000 businesses, and numerous homeowners associations across 49 states. When a vehicle passes by a Flock camera, Flock records license plate information, vehicle characteristics, and when and where the vehicle was spotted. Flock's network of surveillance cameras generate and store billions of vehicle scans each month. Flock reportedly then enables law enforcement to search not just by plate number, but also by make, model, or even bumper stickers.

Flock has been the subject of significant press attention, community activism and oversight by federal and state officials, because of a number of incidents in which law enforcement agencies accessed Flock-collected data in connection with immigration enforcement and to enforce state laws criminalizing abortion. Flock has not taken responsibility for the harms it has enabled, and has instead attempted to spin the facts and shift the blame to others.

My office questioned Flock about these incidents, and sought detailed information about how, why and with whom sensitive data is shared. Based on that research, it is my view that Flock has built a dangerous platform in which abuse of surveillance data is almost certain. In particular, the company has adopted a see-no-evil approach of not proactively auditing the searches done by its law

enforcement customers because, as the company's Chief Communications Officer told the press, "it is not Flock's job to police the police."

By default, data generated by Flock cameras can only be accessed by the customer that paid for the cameras. But most Flock customers do not stay with this default. In August, Flock informed my office that 75% of its law enforcement customers have enrolled in the "National Lookup Tool," which permits any other enrolled customer to search data collected through their cameras. There are two likely reasons for the high enrollment rate for such data sharing. First, Flock only permits agencies to access this search tool if those agencies also share data from their own cameras. Second, to address concerns that license plate data might be abused by federal immigration authorities, Flock has assured its state and local law enforcement customers that the company does not provide access to the Department of Homeland Security (DHS).

With this representation about DHS access to Flock data, Flock deceived its law enforcement customers. In August, 9 News in Denver revealed that Flock granted U.S. Customs and Border Protection (CBP) access to its systems, enabling the agency to search data collected by Flock's cameras, including using the National Lookup Tool. Officials from Flock subsequently confirmed to my office in September that the company provided access to CBP, Homeland Security Investigations (HSI), the Secret Service, and the Naval Criminal Investigative Service as part of a pilot earlier this year. Flock told my office that during the pilot, which has now ended, CBP and HSI conducted approximately 200 and 175 searches respectively. Flock also confirmed that it misled its state and local law enforcement customers, telling my office that "due to internal miscommunication, customers were inaccurately informed that Flock did not have any relationship with DHS, while pilot programs with sub-agencies of DHS were briefly active."

In addition to the direct access that Flock intentionally granted to federal agencies, activists and the press have documented numerous instances of Flock searches run by or for federal agencies on other customers' accounts. In several cases, local law enforcement personnel shared their Flock passwords with federal agents, who then used their access to conduct searches for immigration-related purposes. In several other cases, local law enforcement ran searches at the request of federal agents, again, for immigration-related purposes.

In response to these troubling press reports this summer, my office began conducting oversight into Flock. After the first meeting with my staff, Flock committed to providing additional privacy protections for Oregonians' data. Specifically, Flock agreed to apply software filters to data collected by cameras in Oregon that it had already enabled for data collected in Illinois, California, Colorado, and Washington, which are supposed to prevent out-of-state police searches related to abortion or immigration. However, subsequent oversight by my office revealed that these filters are easy to circumvent and do not meaningfully protect the privacy of Oregonians.

Flock requires its law enforcement customers to provide a reason for a search, which by default, they are prompted to enter into a text box into which any text can be entered. Flock has confirmed to my office that it does not require its law enforcement users to enter a case-specific reason, nor does Flock prohibit law enforcement customers from entering meaningless, generic reasons such as

"investigation" or "crime." Data recently provided to my office by the Electronic Frontier Foundation — from a dataset of 11.4 million Flock nationwide searches for a six-month period obtained through a public records request — reveals that more than 14% of the search reasons contained just the word "investigation" without a case number.

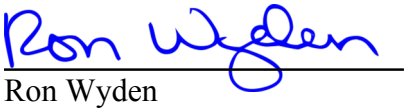
Flock customers can change their default settings to require that their own employees be presented with a drop-down menu of predefined reasons; but importantly, Flock customers cannot control the reasons provided for searches of their data by other law enforcement customers. Additionally, until recently, Flock customers could enable a different opt-in setting to require a case number for searches; if enabled, employees of those agencies would not be required to document any reason at all when submitting searches of other agencies' data. Flock confirmed to my office on August 19, that it removed this option the day before, on August 18, shortly after receiving questions about it from my office.

The privacy protection that Flock promised to Oregonians — that Flock software will automatically examine the reason provided by law enforcement officers for terms indicating an abortion- or immigration-related search — is meaningless when law enforcement officials provide generic reasons like "investigation" or "crime." Likewise, Flock's filters are meaningless if no reason for a search is provided in the first place. While the search reasons collected by Flock, obtained by press and activists through open records requests, have occasionally revealed searches for immigration and abortion enforcement, these are likely just the tip of the iceberg. Presumably, most officers using Flock to hunt down immigrants and women who have received abortions are not going to type that in as the reason for their search. And, regardless, given that Flock has washed its hands of any obligation to audit its customers, Flock customers have no reason to trust a search reason provided by another agency.

I now believe that abuses of your product are not only likely but inevitable, and that Flock is unable and uninterested in preventing them. Cities around the country, including in Oregon, are currently reevaluating their decision to install Flock cameras. I commend and support this reexamination. In my view, local elected officials can best protect their constituents from the inevitable abuses of Flock cameras by removing Flock from their communities.

Thank you for your attention to this important matter. If you have any questions about this letter, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator