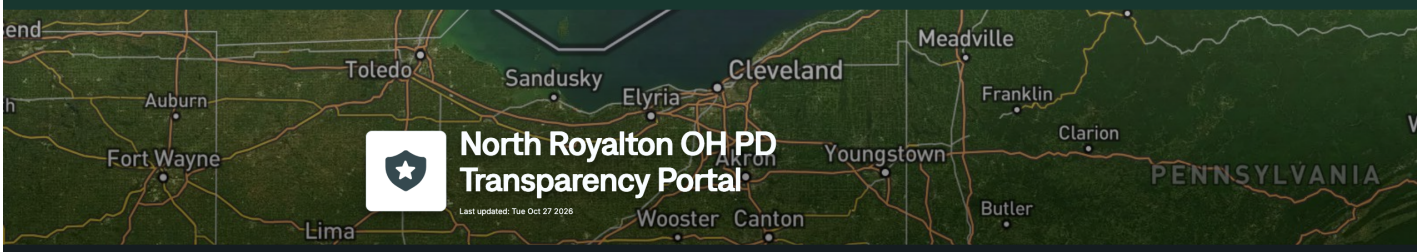

North Royalton OH PD Transparency Portal

Last updated: Tue Oct 27 2026

Overview

North Royalton OH PD uses Flock Safety technology to capture objective evidence without compromising on individual privacy. North Royalton OH PD utilizes retroactive search to solve crimes after they've occurred. Additionally, North Royalton OH PD utilizes real time alerting of hotlist vehicles to capture wanted criminals. In an effort to ensure proper usage and guardrails are in place, they have made the below policies and usage statistics available to the public.

Community Impact

Featured Success Stories

Recent Success Story

Data & Usage Summary

Data Retention
The number of days data is retained.

30 days

Vehicles detected in the last 30 days
Number of unique plate reads over the last 30 days.

201,536

Number of Searches
Total user search sessions over the last 30 days.

34

Hotlists Alerted On
National and statewide hotlist sources.

NCIC, NCMEC Amber Alert

Number of Hotlist Hits
Total hotlist hits over the last 30 days.

438

Policy & Trust

What's Detected

License Plates, Vehicles

What's Not Detected

Facial recognition, People, Gender, Race

Acceptable Use Policy

Data is used for law enforcement purposes only. Data is owned by North Royalton OH PD and is never sold to 3rd parties.

Prohibited Uses

Immigration enforcement, traffic enforcement, harrassment or intimidation, usage based solely on a protected class (i.e. race, sex, religion), Personal use.

Access Policy

All system access requires a valid reason and is stored indefinitely.

Hotlist Policy

Hotlist hits are required to be human verified prior to action.

Public Search Audit
Download to view searches performed over the last 30 days.

Download CSV

SOC 2 Type II

Independently audited controls covering security, availability, and confidentiality.

ISO 27001

Information security management aligned with international standards.

Adherence to Key Privacy Principles

Built to focus on data minimization, purpose limitation, and transparency.

Myth vs. Fact

Myth
Flock has been hacked.

Fact
Flock's cloud environment has never been breached. Flock invests in a strong security posture, including adhering to NDAA, SOC2 (Type II), ISO 27001, ISO 27018 FedRAMP 20x, and Higher Education Community Vendor Assessment Tool (HECVAT) compliance. Additional security precautions include Role-Based Access Controls, data encrypted at-rest and in transit, required Multi-Factor Authentication, and regular penetration testing.

Myth
Flock sells and/or shares customer data.

Fact
Your community owns 100% of your data and it will never be sold. Only your agency decides who to share your data with, not Flock. Flock Safety does not publicly release agency search data. Flock does not operate or support any public-facing searchable database of law enforcement lookups, and we do not provide license plate search histories to websites or third parties without the agency's knowledge and authorization. Other agencies who you share footage with have been responding to FOIA requests and sharing this search data.

Myth
My data is fed into a national database.

Fact
Each agency controls access to its own data. Agencies may choose to share information through a broader network, but nothing is shared automatically. Participation is opt-in, governed by defined agreements, and limited to lawful investigative purposes.

Myth
Flock cameras use facial recognition.

Fact
Flock cameras do not use facial recognition technology. Searches are based on vehicle characteristics, and not identity. Flock cannot recognize, identify, or track individuals. It is purpose built for specific public safety investigations, not to monitor people.