Frequently Asked Questions

Commerce City Safeguards for Use of Emerging Technologies

Q: Does CCPD have a policy regarding the use of Automated License Plate Reader (ALPR) Systems?

A: Yes. CCPD Policy 420 addresses the use of automated license plate readers.

Q: Does Policy 420 prohibit certain uses of ALPR technology?

A: Yes. Policy 420.5 addresses prohibited use.

> 420.5 PROHIBITED USE OF ALPR
>
> The use of ALPR is prohibited as outlined below.
>
> (a) Invasion of Privacy: Except when done pursuant to a court order or search warrant, it is a violation of policy to utilize the LPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate is visible from a place to which members of the public have access).
>
> (b) Harassment: It is a violation of this policy to use the LPR system to harass any individual. An ALPR shall not be used to seek data on any individual or organization based solely on their religious, political, social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, age, disability, gender, gender identity, sexual orientation, or other classification protected by law.
>
> (c) Personal Use: It is a violation of this policy to use the LPR system or associated scan files or hot lists for any personal purpose.
>
> (d) Use of the ALPR system for minor traffic violation enforcement and immigration enforcement is prohibited.

Q: Does CCPD have a policy regarding data collection and retention with respect to its use of ALPR systems?

A: Yes. Policy 420.7 addresses this issue.

> 420.7 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by the ALPR are for the official use of the Commerce City Police Department and because such data may contain confidential information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The database retention period for all data collected by ALPR hardware and stored on the ALPR cloud storage system shall not exceed 30 days. The ALPR system permanently deletes every 30 days on a rolling basis by default. The exceptions are if it is of evidentiary value in a criminal action or is subject to a lawful action to produce records. In such circumstances, the applicable data should be downloaded from the applicable ALPR network into the corresponding case file on evidence.com. Mass downloading of ALPR data via the ALPR cloud storage system is prohibited.

Q: Can a CCPD employee use the LPR system for non-law enforcement related or personal inquiries?

A: No. CCPD Policy 420.4 states in part "An ALPR shall only be used for official and legitimate law enforcement business."

Q: Does CCPD have reciprocal sharing agreements with other law enforcement agencies and if so, how are we certain our data is not shared with federal authorities for purposes like immigration enforcement which is contrary to Colorado law?

A: Yes, CCPD does have sharing agreements in place, but we only share data with other Colorado agencies who are bound by the same laws regarding immigration investigations as CCPD. The information that CCPD shares through Flock with other agencies is completely controlled by CCPD. CCPD owns all data collected by CCPD Flock cameras. Outside agencies cannot see our data unless we share with them. CCPD can also stop sharing at any point with any agency. While not maintaining reciprocal sharing agreements with other entities outside the state of Colorado could prevent us from obtaining and using valuable information, it also safeguards our compliance with Colorado law.

Q: Does CCPD maintain audit logs of LPR information shared?

A: No. At present we do conduct audits to ensure we are compliant with our policy, but do not warehouse this information in any manner after the review is complete.

Q: If an audit uncovers noncompliance what steps are taken?

A: CCPD Policy 420.9.1 requires that any discrepancies, problems or misuse be reported to the Chief of Police. So, while CCPD does not warehouse audit findings, clear guidance is in

place with regard to reporting problems or misuse uncovered. To date, no such misuse has been reported to the Chief of Police.

Q: Does CCPD use Facial Recognition?

A: No. Colorado law has strict requirements for adopting the use of facial recognition technology, and at the present time CCPD has not pursued adoption of such.

Q: Does CCPD use drones?

A: Yes. CCPD uses drones in the field with certain personnel who are trained to deploy and fly them safely and we use them as part of a Drone as First Responder Program where trained personnel fly them remotely to support public safety operations.

Q: Can CCPD drone pilots use the drones for whatever reason they see fit?

A: No. CCPD addresses prohibited use of drones

> 606.6 PROHIBITED USE
>
> The UAS video surveillance equipment shall not be used:
>
> • To conduct random surveillance activities.
>
> • To target a person based solely on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.
>
> • To harass, intimidate, or discriminate against any individual or group.
>
> • To conduct personal business of any type.
>
> The UAS shall not be weaponized.

Q: Are there rules in place for the retention of data obtained by drones?

A: Yes. CCPD policy 606.7 states “Data collected by the UAS shall be retained as provided in the established records retention schedule.”

Q: Does the city restrict and control access to Surveillance and other Public Safety system?

A: Yes. Commerce City PD partners with the IT department to establish managed and controlled access and authentication methods for all PD systems. This is in accordance with industry best practices and meets Criminal Justice Information Servies (CJIS) and other compliance standards.