

Surveillance Systems in Utah

Utah Civic Compact

Utah Privacy Commission · Automatic License Plate Reader Technology

September 8, 2026

THE NUMBER

Ten cameras in Weber County produced data for the Flock system that was part of 5.1 million network queries.

3,343

agencies ran those queries

~97%

from outside Utah (about 4.9 million)

WHAT THE COUNTY BOUGHT

§ 41-6a-2002 (2)

“...cameras used in combination with computer algorithms to convert an image of a license plate into computer-readable data.”

Order form

“...license plate recognition camera with Vehicle Fingerprint™ technology (proprietary machine learning software) and real-time alerts for unlimited users.”

DEFINITIONS, VERBATIM FROM THE WEBER COUNTY CONTRACT

§ 1.3

Customer Data

“the images, audio and/or video segments made available to Customer through the Web Interface... **For clarity, Customer Data does not include the underlying raw Footage captured by the Flock Hardware or any Flock IP (as defined in Section 1.9).**”

§ 1.9

Flock IP

“...Flock's technology, patents, trade secrets, trademarks, algorithms, data models, machine learning methods... **For clarity, Flock IP also includes any derivative works, intermediate or final outputs, analyses, reports, models, or other results generated by or through the Flock Services.** Except for the limited ability to access and download Customer Data within the applicable Retention Period, no rights are granted to download, extract, export, or otherwise create or retain copies of such derivative works, outputs, or other elements of the Flock IP.”

§ 1.11

Footage

“still images, video, audio, and other raw data captured by the Flock Hardware or Customer Hardware via the Flock Services.”

WHAT THE LAW SAYS • RETENTION

§ 41-6a-2004(1)(c)

“...may not be preserved for more than nine months **by a governmental entity...**”

§ 1.15

“‘Retention Period’ means the time period that the **Customer Data** is stored within the cloud storage, as specified in the applicable Order Form.”

The Weber County Order Form states a 30 day retention period.

WHAT THE LAW SAYS • WHAT A RECORD IS

§ 63G-2-103(25) (a)

“‘Record’ means... documentary material... that is prepared, owned, received, or retained **by a governmental entity...**”

§ 1.18

“the Web Interface does not include APIs, or any other automated, programmatic data transfer method.”

WHAT THE LAW SAYS • PROTECTED RECORD

§ 41-6a-2004(1)(a)

“...is a protected record... if the captured plate data is maintained **by a governmental entity**”

§ 1.3

“Customer Data does not include the underlying raw Footage... or any Flock IP.”

WHAT THE LAW SAYS • DESTRUCTION

§ 41-6a-2004 (4) (a)

“...**a governmental entity** shall destroy as soon as reasonably possible, in an unrecoverable manner, plate data obtained pursuant to this chapter that is not specifically necessary...”

§ 41-6a-2004 (4) (b)

“Subsection (4)(a) applies to data a governmental entity **obtains**: (i) from a nongovernmental entity pursuant to a warrant; or (ii) from an automatic license plate reader system owned or operated **by a governmental entity**.”

§ 1.9

“Except for the limited ability to access and download Customer Data within the applicable Retention Period, **no rights are granted to download, extract, export, or otherwise create or retain copies of such derivative works, outputs, or other elements of the Flock IP.**”

§ 10.2 Flock Hardware is owned and shall remain the exclusive property of Flock.

§ 72-1-212 (8)

“...the installation, maintenance, data collection, and removal are the responsibility of the law enforcement agency that obtains the special use permit.”

The contract

- Hardware is Flock's property § 10.2
- Flock holds final discretion to veto a location § 10.3
- Footage is “captured by the Flock Hardware” § 1.11

NO-SALE OF CUSTOMER DATA

§ 4.1

“As between Flock and Customer, all right, title and interest in the **Customer Data**, belong to and are retained solely by Customer... **Flock does not own and shall not sell Customer Data.**”

§ 5.2

“Flock and its licensors retain all right, title and interest in and to the **Flock IP**... Customer further acknowledges that **Flock retains the right to use the foregoing for any purpose in Flock's sole discretion.**”

§ 7.3 Section 5 survives termination. Section 4 does not.

THE LAW AND THE PURCHASE

THE LAW DESCRIBES

A plate reader,
run by a government agency,
whose data that agency holds.

WHAT FLOCK SOLD

- A non-exclusive, non-transferable right of access through a web interface, for the length of the term § 2.1
- Plate detection, alerts, audio detection, image search and video § 1.10
- Ten Flock-owned cameras the county may not reposition or take possession of § 10.2

ACCESS TO THE NETWORK

WHAT THE AGREEMENT GOVERNS

- Who may hold an account: officers, employees, or agents of the Customer § 3.1
- Distribution to a third party, on a Customer-requested integration § 4.4
- Flock's own disclosure of Customer Data, on its good-faith belief § 5.3

WHAT UCC COULD NOT LOCATE

- Any term describing a **network search** by another agency
- Any term naming who else may query data captured by these cameras
- Any term limiting how many agencies may do so

WHERE THE TWO DEFINITIONS MEET

§ 41-6a-2002 (3)

“‘Captured plate data’ means the **global positioning system coordinates, date and time, photograph, license plate number**, and any other data captured by or derived from an automatic license plate reader system.”

§ 1.3

“the images... **made available to Customer through the Web Interface**... together with the metadata... (e.g., **license plate number, timestamp of capture, and geospatial coordinates**).”

PERMITTED PURPOSE

§ 41-6a-2003(2)(a)

“...by a law enforcement agency to access captured license plate data: (i) as part of an active criminal investigation; (ii) to apprehend an individual with an outstanding warrant; (iii) to locate a missing or endangered person; or (iv) to locate a stolen vehicle”

§ 1.14

“‘Permitted Purpose’ means legitimate public safety **and/or business purpose**, including but not limited to the awareness, prevention, and prosecution of crime; investigations; and **prevention of commercial harm**, to the extent permitted by law.”

BETTER SYSTEMS EXIST

Network sharing “should not be the default behavior.”

Steve Lindsey, LiveView Technologies, Utah County.
Military.com, “Flock cameras are taking over, but many Americans are pushing back”

- Sharing off unless an agency turns it on

LINDSEY

- Turned on by something closer to a subpoena

LINDSEY

Persistent Identifying System

means a system that:

- (a) captures, generates, or resolves an identifier, meaning any data that **distinguishes an individual, a vehicle or other property of an individual, or a device from others of its kind**, including a license plate number, a device or network address, facial geometry, gait, voice, and the combination of visible features by which a vehicle or object is distinguished;
- (b) does so **without the individual knowingly presenting the identifier for that purpose**; and
- (c) records the identifier in a form that allows the same identifier to be **recognized on later, separate occasions**.

Persistent Identifying Data

means, **without regard to the form in which it is held, the party that holds it, or its characterization as proprietary information, a trade secret, or the property of a person other than the individual identified:**

- (a) an identifier captured, generated, or resolved by a persistent identifying system;
- (b) any image, video, audio, or other data captured by the system in connection with that identifier, and any record of the time or location of capture; and
- (c) any data derived from anything in (a) or (b), including any output, analysis, profile, alert, score, report, or model.

The contract, order form, and other files obtained through GRAMA are available at

utahciviccompact.org

Utah Civic Compact