

**Second Regular Session
Seventy-fifth General Assembly
STATE OF COLORADO**

INTRODUCED

LLS NO. 26-0597.01 Christopher McMichael x4775

SENATE BILL 26-071

SENATE SPONSORSHIP

Zamora Wilson,

HOUSE SPONSORSHIP

(None),

Senate Committees
Judiciary

House Committees

A BILL FOR AN ACT

101 **CONCERNING THE REGULATION OF LAW ENFORCEMENT SURVEILLANCE**
102 **TECHNOLOGIES TO PROTECT CITIZENS.**

Bill Summary

(Note: This summary applies to this bill as introduced and does not reflect any amendments that may be subsequently adopted. If this bill passes third reading in the house of introduction, a bill summary that applies to the reengrossed version of this bill will be available at <http://leg.colorado.gov>.)

The bill establishes the "Surveillance Accountability and Freedom Ensured (SAFE) Act" (SAFE Act). On and after July 1, 2027, the SAFE Act requires a law enforcement agency to use surveillance technology only for lawful purposes directly related to public safety or for an active investigation.

If a law enforcement agency uses surveillance technology to

Shading denotes HOUSE amendment. Double underlining denotes SENATE amendment.
Capital letters or bold & italic numbers indicate new material to be added to existing law.
Dashes through the words or numbers indicate deletions from existing law.

collect surveillance data, the law enforcement agency must comply with certain requirements related to the collection, storage, sharing, and destruction of the data.

The law enforcement agency must ensure that:

- Facial recognition systems are only used after a warrant is obtained or in exigent circumstances when there is an imminent threat to public safety;
- Traffic cameras and automated license plate readers must only be used in public spaces and for specific enforcement purposes, such as traffic violations or identifying stolen vehicles; and
- Drone cameras are operated in compliance with federal aviation administration regulations.

A law enforcement agency may store data collected by surveillance technology only for a specified amount of time depending on the type of technology used and how the data is collected or until an active investigation is concluded.

A law enforcement agency shall not sell any data that is collected from its surveillance technologies, but the law enforcement agency may share the surveillance data with another law enforcement agency if the data is related to an active investigation and the other law enforcement agency agrees to comply with the requirements of the SAFE Act. A law enforcement agency must also ensure that surveillance data is permanently destroyed at the end of an applicable retention period or once the data is no longer needed for the matter. The bill creates civil penalties for violations of these provisions.

The bill also requires a law enforcement agency to make certain information related to the law enforcement agency's compliance with the SAFE Act available to residents who request it at no cost to the resident.

The bill requires the attorney general to conduct an audit of a law enforcement agency every 2 years and authorizes the attorney general to bring a civil action to enforce the SAFE Act.

1 *Be it enacted by the General Assembly of the State of Colorado:*

2 **SECTION 1. Short title.** The short title of this act is the
3 "Surveillance Accountability and Freedom Ensured (SAFE) Act".

4 **SECTION 2. Legislative declaration.** (1) The general assembly
5 finds and declares that:

6 (a) The use of surveillance technologies by law enforcement
7 agencies, including the use of speed cameras, automated license plate

1 readers, red-light cameras, pole-mounted cameras, drones, and facial
2 recognition systems, can enhance public safety by aiding in the
3 prevention, detection, and investigation of crimes;

4 (b) However, the unchecked deployment and use of surveillance
5 technologies pose significant risks to the privacy, civil liberties, and
6 constitutional rights of Coloradans, including the potential for
7 surveillance without a warrant, misuse of data, and disproportionate
8 impacts on marginalized communities;

9 (c) It is necessary to establish clear guardrails on the use,
10 collection, storage, access, sharing, and destruction of data obtained
11 through surveillance technologies in order to strike a proper balance
12 between protecting privacy and promoting public safety; and

13 (d) These guardrails must include mechanisms for public
14 transparency and accountability with minimal bureaucratic hurdles to
15 ensure compliance and build public trust.

16 **SECTION 3.** In Colorado Revised Statutes, **add** part 15 to article
17 31 of title 24 as follows:

18 **PART 15**
19 **SURVEILLANCE ACCOUNTABILITY FOR LAW**
20 **ENFORCEMENT AGENCIES**

21 **24-31-1501. Definitions.**

22 **AS USED IN THIS PART 15, UNLESS THE CONTEXT OTHERWISE**
23 **REQUIRES:**

24 (1) "AUTHORIZED PERSONNEL" MEANS AN EMPLOYEE OF A LAW
25 ENFORCEMENT AGENCY WHO HAS BEEN TRAINED AND CERTIFIED IN THE
26 PROPER USE AND HANDLING OF SURVEILLANCE DATA, AS DETERMINED BY
27 THE LAW ENFORCEMENT AGENCY'S POLICY DEVELOPED IN COMPLIANCE

1 WITH THIS PART 15.

2 (2) "INVESTIGATION" MEANS AN ACTIVE INQUIRY INTO A SPECIFIC
3 ALLEGED VIOLATION OF LAW BASED ON REASONABLE SUSPICION OR
4 PROBABLE CAUSE.

5 (3) "LAW ENFORCEMENT AGENCY" HAS THE SAME MEANING AS
6 "STATE OR LOCAL LAW ENFORCEMENT AGENCY" AS DEFINED IN SECTION
7 24-33.5-115 (4)(b).

8 (4) "SURVEILLANCE DATA" MEANS INFORMATION COLLECTED,
9 RECORDED, OR GENERATED BY SURVEILLANCE TECHNOLOGY, INCLUDING
10 IMAGES, VIDEOS, METADATA, LICENSE PLATE NUMBERS, FACIAL SCANS,
11 LOCATION DATA, OR DERIVED ANALYTICS.

12 (5) (a) "SURVEILLANCE TECHNOLOGY" MEANS AN ELECTRONIC
13 DEVICE OR SYSTEM USED BY A LAW ENFORCEMENT AGENCY FOR THE
14 PURPOSE OF MONITORING, RECORDING, OR ANALYZING INDIVIDUALS,
15 VEHICLES, OR PUBLIC SPACES.

16 (b) "SURVEILLANCE TECHNOLOGY" INCLUDES:

17 (I) SPEED CAMERAS;

18 (II) AUTOMATED LICENSE PLATE READERS;

19 (III) RED-LIGHT CAMERAS;

20 (IV) POLE-MOUNTED CAMERAS;

21 (V) DRONES OR OTHER UNMANNED AERIAL VEHICLE
22 SURVEILLANCE SYSTEMS;

23 (VI) FACIAL RECOGNITION SOFTWARE OR SYSTEMS; AND

24 (VII) OTHER TECHNOLOGY USED BY A LAW ENFORCEMENT
25 AGENCY TO CAPTURE VISUAL, AUDIO, OR LOCATION INFORMATION.

26 **24-31-1502. Restrictions on surveillance data collection by law**
27 **enforcement agencies - public impact assessment.**

1 (1) A LAW ENFORCEMENT AGENCY MAY USE SURVEILLANCE
2 TECHNOLOGY ONLY FOR LAWFUL PURPOSES DIRECTLY RELATED TO PUBLIC
3 SAFETY, INCLUDING TRAFFIC ENFORCEMENT, CRIME PREVENTION, OR AN
4 ACTIVE INVESTIGATION.

5 (2) A LAW ENFORCEMENT AGENCY THAT USES SURVEILLANCE
6 TECHNOLOGY TO COLLECT SURVEILLANCE DATA SHALL:

7 (a) USE THE SURVEILLANCE TECHNOLOGY ONLY IN A MANNER
8 THAT IS TARGETED AND MINIMIZES INCIDENTAL CAPTURE OF
9 NONRELEVANT INDIVIDUALS OR ACTIVITIES;

10 (b) USE FACIAL RECOGNITION SYSTEMS ONLY AFTER OBTAINING A
11 WARRANT OR IN EXIGENT CIRCUMSTANCES WHEN THERE IS AN IMMINENT
12 THREAT TO PUBLIC SAFETY;

13 (c) CONFIGURE AUTOMATED LICENSE PLATE READERS, SPEED
14 CAMERAS, RED-LIGHT CAMERAS, TRAFFIC CAMERAS, AND OTHER
15 SURVEILLANCE TECHNOLOGY USED IN TRAFFIC ENFORCEMENT TO CAPTURE
16 SURVEILLANCE DATA ONLY FROM PUBLIC SPACES AND FOR SPECIFIC LAW
17 ENFORCEMENT PURPOSES, SUCH AS IDENTIFYING STOLEN VEHICLES OR
18 ENFORCING TRAFFIC LAWS; AND

19 (d) OPERATE DRONES OR OTHER UNMANNED AERIAL VEHICLE
20 SURVEILLANCE SYSTEMS ONLY IN COMPLIANCE WITH FEDERAL AVIATION
21 ADMINISTRATION REGULATIONS AND SHALL INCLUDE REAL-TIME LOGGING
22 OF FLIGHT PATHS AND SURVEILLANCE DATA COLLECTION SCOPES.

23 (3) (a) BEFORE A LAW ENFORCEMENT AGENCY PURCHASES,
24 CONTRACTS FOR OR RENEWS A CONTRACT FOR, DEPLOYS IN A NEW WAY OR
25 LOCATION, OR UPGRADES A SURVEILLANCE TECHNOLOGY, THE LAW
26 ENFORCEMENT AGENCY SHALL:

27 (I) CONDUCT A PUBLIC PRIVACY IMPACT ASSESSMENT THAT

1 INCLUDES COMMUNITY INPUT AND AN OPPORTUNITY FOR PUBLIC
2 TESTIMONY; AND

3 (II) OBTAIN APPROVAL FROM THE GOVERNING BODY OF THE STATE
4 OR LOCAL GOVERNMENT ENTITY THAT OVERSEES THE LAW ENFORCEMENT
5 AGENCY.

6 (b) THE REQUIREMENTS OF SUBSECTION (3)(a) OF THIS SECTION
7 APPLY TO A LAW ENFORCEMENT AGENCY THAT CURRENTLY USES
8 SURVEILLANCE TECHNOLOGY WHENEVER THE LAW ENFORCEMENT
9 AGENCY:

10 (I) RENEWS A CONTRACT FOR THE USE OF SURVEILLANCE
11 TECHNOLOGY;

12 (II) PURCHASES OR DEPLOYS A NEW TYPE OF SURVEILLANCE
13 TECHNOLOGY;

14 (III) DEPLOYS AN EXISTING SURVEILLANCE TECHNOLOGY IN A NEW
15 MANNER OR IN A NEW LOCATION; OR

16 (IV) UPGRADES THE LAW ENFORCEMENT AGENCY'S EXISTING
17 SURVEILLANCE TECHNOLOGY SYSTEMS.

18 **24-31-1503. Surveillance data - storage and retention of data**
19 **- destruction of data - access and sharing of data - prohibition on sale**
20 **of data.**

21 (1) A LAW ENFORCEMENT AGENCY THAT COLLECTS SURVEILLANCE
22 DATA SHALL ENSURE THAT THE SURVEILLANCE DATA IS STORED SECURELY,
23 INCLUDING ENSURING THAT THE SURVEILLANCE DATA IS ENCRYPTED OR
24 OTHERWISE RENDERED UNREADABLE TO AN UNAUTHORIZED USER BY
25 USING A METHOD OR TECHNOLOGY GENERALLY ACCEPTED IN THE FIELD OF
26 INFORMATION SECURITY.

27 (2) UNLESS THE SURVEILLANCE DATA IS PART OF AN ACTIVE

1 INVESTIGATION:

2 (a) SURVEILLANCE DATA COLLECTED FROM TRAFFIC CAMERAS,
3 SPEED CAMERAS, RED-LIGHT CAMERAS, AND AUTOMATED LICENSE PLATE
4 READERS MUST NOT BE STORED FOR LONGER THAN THIRTY DAYS;

5 (b) SURVEILLANCE DATA COLLECTED FROM POLE-MOUNTED
6 CAMERAS, DRONES, OR OTHER UNMANNED AERIAL VEHICLE SURVEILLANCE
7 SYSTEMS MUST NOT BE STORED FOR LONGER THAN NINETY DAYS; AND

8 (c) SURVEILLANCE DATA COLLECTED FROM FACIAL RECOGNITION
9 SOFTWARE OR SYSTEMS MUST NOT BE STORED FOR LONGER THAN SEVEN
10 DAYS.

11 (3) IF SURVEILLANCE DATA IS PART OF AN ACTIVE INVESTIGATION,
12 THE SURVEILLANCE DATA MAY BE RETAINED UNTIL THE MATTER IS
13 RESOLVED, INCLUDING THE CONCLUSION OF ANY APPEALS, BUT MUST BE
14 REVIEWED ANNUALLY FOR NECESSITY AND DESTROYED IF THE DATA IS NO
15 LONGER RELEVANT TO THE MATTER.

16 (4)(a) A LAW ENFORCEMENT AGENCY SHALL ENSURE THAT ACCESS
17 TO SURVEILLANCE DATA IS LIMITED TO AUTHORIZED PERSONNEL AND THAT
18 SURVEILLANCE DATA IS ACCESSED ONLY FOR LEGITIMATE LAW
19 ENFORCEMENT PURPOSES.

20 (b) WHEN AUTHORIZED PERSONNEL ACCESSES SURVEILLANCE
21 DATA, THE AGENCY SHALL ENSURE THAT INFORMATION RELATED TO THAT
22 ACCESS IS COLLECTED, INCLUDING:

23 (I) THE NAME OF THE PERSON THAT ACCESSED THE SURVEILLANCE
24 DATA;

25 (II) THE DATE AND TIME THE PERSON ACCESSED THE
26 SURVEILLANCE DATA; AND

27 (III) THE PURPOSE FOR WHICH THE SURVEILLANCE DATA WAS

1 ACCESSED.

2 (c) THE LAW ENFORCEMENT AGENCY SHALL RETAIN THE
3 INFORMATION COLLECTED IN ACCORDANCE WITH SUBSECTION (4)(b) OF
4 THIS SECTION FOR AT LEAST FIVE YEARS AFTER THE DATE THE
5 SURVEILLANCE DATA WAS ACCESSED.

6 (5) A LAW ENFORCEMENT AGENCY MAY SHARE SURVEILLANCE
7 DATA WITH ANOTHER LAW ENFORCEMENT AGENCY IF:

8 (a) THERE IS A SPECIFIC, DOCUMENTED NEED FOR THE OTHER LAW
9 ENFORCEMENT AGENCY TO ACCESS THE SURVEILLANCE DATA AND THE
10 NEED IS RELATED TO AN ACTIVE INVESTIGATION; AND

11 (b) THE LAW ENFORCEMENT AGENCY THAT RECEIVES THE
12 SURVEILLANCE DATA AGREES, IN WRITING, TO COMPLY WITH THE
13 REQUIREMENTS OF THIS PART 15.

14 (6) (a) A LAW ENFORCEMENT AGENCY OR AN EMPLOYEE OR
15 CONTRACTOR OF A LAW ENFORCEMENT AGENCY SHALL NOT SELL, LICENSE,
16 OR OTHERWISE MONETIZE SURVEILLANCE DATA COLLECTED BY THE LAW
17 ENFORCEMENT AGENCY.

18 (b) A LAW ENFORCEMENT AGENCY OR AN EMPLOYEE OR
19 CONTRACTOR OF A LAW ENFORCEMENT AGENCY THAT VIOLATES
20 SUBSECTION (6)(a) OF THIS SECTION MAY BE SUBJECT TO CIVIL PENALTIES
21 IN ACCORDANCE WITH SECTION 24-31-1505.

22 (7) (a) A LAW ENFORCEMENT AGENCY SHALL PERMANENTLY AND
23 SECURELY DESTROY SURVEILLANCE DATA AT THE END OF THE RETENTION
24 PERIOD DESCRIBED IN SUBSECTION (2) OF THIS SECTION OR WHEN THE
25 SURVEILLANCE DATA IS NO LONGER NEEDED FOR AN ACTIVE MATTER.

26 (b) A LAW ENFORCEMENT AGENCY SHALL ENSURE THAT
27 SURVEILLANCE DATA IS DESTROYED IN A MANNER IN WHICH THE

1 SURVEILLANCE DATA CANNOT BE RECOVERED.

2 (c) A LAW ENFORCEMENT AGENCY SHALL COLLECT INFORMATION
3 RELATED TO THE DESTRUCTION OF SURVEILLANCE DATA, INCLUDING THE
4 DATE AND METHOD OF DESTRUCTION, AND SHALL MAINTAIN A RECORD OF
5 THAT INFORMATION FOR AT LEAST FIVE YEARS AFTER THE DATE THE
6 SURVEILLANCE DATA WAS DESTROYED.

7 **24-31-1504. Verification of compliance and transparency.**

8 (1) A RESIDENT OF THE JURISDICTION SERVED BY A LOCAL LAW
9 ENFORCEMENT AGENCY, OR A RESIDENT OF THE STATE FOR THE COLORADO
10 STATE PATROL OR COLORADO BUREAU OF INVESTIGATION, MAY REQUEST
11 INFORMATION FROM THE LAW ENFORCEMENT AGENCY REGARDING THE
12 AGENCY'S USE OF SURVEILLANCE TECHNOLOGY AND THE AGENCY'S
13 COLLECTION, STORAGE, AND DESTRUCTION OF SURVEILLANCE DATA THAT
14 DEMONSTRATES THE LAW ENFORCEMENT AGENCY'S COMPLIANCE WITH
15 THIS PART 15. THE LAW ENFORCEMENT AGENCY SHALL PROVIDE THE
16 INFORMATION REQUESTED FREE OF CHARGE TO THE RESIDENT.

17 (2) A REQUEST SUBMITTED BY A RESIDENT IN ACCORDANCE WITH
18 SUBSECTION (1) OF THIS SECTION MAY BE SUBMITTED TO THE LAW
19 ENFORCEMENT AGENCY THROUGH EMAIL, THROUGH AN ONLINE PORTAL,
20 OR BY MAIL. A LAW ENFORCEMENT AGENCY THAT RECEIVES A REQUEST
21 SHALL SEND A RESPONSE TO THE RESIDENT WITHIN TEN BUSINESS DAYS
22 AFTER RECEIVING THE REQUEST.

23 (3) A LAW ENFORCEMENT AGENCY MAY DEMONSTRATE
24 COMPLIANCE WITH THIS PART 15 IN RESPONSE TO A REQUEST SUBMITTED
25 PURSUANT TO THIS SECTION BY PROVIDING THE REQUESTING RESIDENT THE
26 FOLLOWING INFORMATION:

27 (a) CONFIRMATION THAT SPECIFIC SURVEILLANCE DATA RELATED

1 TO THE REQUESTOR'S PERSONAL IDENTIFYING INFORMATION HAS BEEN
2 DESTROYED;

3 (b) ACCESS TO ANONYMIZED LOGS THAT DEMONSTRATE WHETHER
4 SURVEILLANCE DATA RELATED TO THE REQUESTOR WAS ACCESSED,
5 SHARED, OR DESTROYED; AND

6 (c) REPORTS ON THE LAW ENFORCEMENT AGENCY'S OVERALL
7 COMPLIANCE WITH THIS PART 15, INCLUDING ANY ANNUAL REPORTS OR
8 AUDITS CONDUCTED PURSUANT TO SUBSECTION (4) OR (5) OF THIS
9 SECTION. THE LAW ENFORCEMENT AGENCY SHALL ENSURE THAT ALL
10 PERSONAL IDENTIFYING INFORMATION HAS BEEN REDACTED FROM A
11 REPORT BEFORE SENDING THE REPORT TO THE REQUESTING RESIDENT.

12 (4) A LAW ENFORCEMENT AGENCY THAT USES SURVEILLANCE
13 TECHNOLOGY SHALL PUBLISH AN ANNUAL REPORT ON ITS PUBLICLY
14 ACCESSIBLE WEBSITE THAT INCLUDES THE FOLLOWING INFORMATION:

15 (a) THE TYPES OF SURVEILLANCE TECHNOLOGIES USED BY THE LAW
16 ENFORCEMENT AGENCY;

17 (b) AGGREGATE AND ANONYMIZED INFORMATION RELATED TO THE
18 COLLECTION, RETENTION, ACCESS, SHARING, AND DESTRUCTION OF
19 SURVEILLANCE DATA; AND

20 (c) ANY COMPLAINTS RECEIVED BY THE LAW ENFORCEMENT
21 AGENCY OR VIOLATIONS COMMITTED BY THE LAW ENFORCEMENT AGENCY
22 IN RELATION TO THE USE OF SURVEILLANCE TECHNOLOGY OR THE
23 COLLECTION, STORAGE, AND DESTRUCTION OF SURVEILLANCE DATA AND
24 HOW THE COMPLAINTS OR VIOLATIONS WERE RESOLVED.

25 (5) (a) THE ATTORNEY GENERAL SHALL CONDUCT AN
26 INDEPENDENT AUDIT OF A LAW ENFORCEMENT AGENCY THAT USES
27 SURVEILLANCE TECHNOLOGY AT LEAST EVERY TWO YEARS AND PUBLISH

1 THE RESULTS OF THE AUDIT ON THE ATTORNEY GENERAL'S PUBLICLY
2 ACCESSIBLE WEBSITE.

3 (b) THE ATTORNEY GENERAL'S AUDIT OF A LAW ENFORCEMENT
4 AGENCY CONDUCTED PURSUANT TO SUBSECTION (5)(a) OF THIS SECTION
5 MUST INCLUDE:

6 (I) VERIFICATION THAT THE LAW ENFORCEMENT AGENCY IS USING
7 SURVEILLANCE TECHNOLOGY IN A MANNER THAT COMPLIES WITH THIS
8 PART 15;

9 (II) VERIFICATION THAT THE LAW ENFORCEMENT AGENCY IS
10 STORING, RETAINING, SHARING, AND DESTROYING SURVEILLANCE DATA IN
11 COMPLIANCE WITH THIS PART 15; AND

12 (III) A REVIEW OF OTHER RELEVANT INFORMATION OR
13 DOCUMENTATION THAT THE ATTORNEY GENERAL DETERMINES IS
14 NECESSARY TO VERIFY THE LAW ENFORCEMENT AGENCY'S COMPLIANCE
15 WITH THIS PART 15.

16 **24-31-1505. Enforcement and penalties - admissibility.**

17 (1) THE ATTORNEY GENERAL OR AN INDIVIDUAL AFFECTED BY A
18 VIOLATION OF THIS PART 15 MAY BRING A CIVIL ACTION AGAINST A LAW
19 ENFORCEMENT AGENCY.

20 (2) IF A LAW ENFORCEMENT AGENCY IS FOUND TO HAVE VIOLATED
21 THIS PART 15, THE COURT MAY ORDER:

22 (a) INJUNCTIVE RELIEF;

23 (b) CIVIL PENALTIES OF UP TO FIVE THOUSAND DOLLARS PER
24 VIOLATION;

25 (c) REASONABLE ATTORNEY FEES AND COSTS; AND

26 (d) DISCIPLINARY ACTION AGAINST LAW ENFORCEMENT AGENCY
27 PERSONNEL, INCLUDING TERMINATION.

1 (3) IF THE COURT ORDERS CIVIL PENALTIES TO BE PAID BY A LAW
2 ENFORCEMENT AGENCY IN ACCORDANCE WITH SUBSECTION (2)(b) OF THIS
3 SECTION IN AN ACTION BROUGHT BY THE ATTORNEY GENERAL, THE CIVIL
4 PENALTIES SHALL BE CREDITED TO THE GENERAL FUND.

5 (4) SURVEILLANCE DATA ACCESSED IN VIOLATION OF THIS PART 15
6 IS NOT ADMISSIBLE AS EVIDENCE IN ANY CRIMINAL OR CIVIL PROCEEDING
7 OR ANY OTHER JUDICIAL, QUASI-JUDICIAL, OR ADMINISTRATIVE HEARING
8 OR PROCEEDING; EXCEPT THAT THE SURVEILLANCE DATA IS ADMISSIBLE
9 AGAINST A LAW ENFORCEMENT AGENCY IN A CIVIL ACTION BROUGHT
10 AGAINST THE LAW ENFORCEMENT AGENCY PURSUANT TO SUBSECTION (1)
11 OF THIS SECTION.

12 **SECTION 4. Act subject to petition - effective date -**
13 **applicability.** (1) This act takes effect July 1, 2027; except that, if a
14 referendum petition is filed pursuant to section 1 (3) of article V of the
15 state constitution against this act or an item, section, or part of this act
16 within the ninety-day period after final adjournment of the general
17 assembly, then the act, item, section, or part will not take effect unless
18 approved by the people at the general election to be held in November
19 2026 and, in such case, will take effect July 1, 2027.

20 (2) This act applies to conduct occurring on or after the applicable
21 effective date of this act.