

STATE OF NEW YORK

9062

2025-2026 Regular Sessions

IN ASSEMBLY

September 5, 2025

Introduced by M. of A. CRUZ -- read once and referred to the Committee on Governmental Operations

AN ACT to amend the civil rights law, in relation to prohibiting access to video and audio recordings from smart surveillance devices without a warrant and voiding contractual provisions permitting such access

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

1 Section 1. The civil rights law is amended by adding a new article 8-A
2 to read as follows:

ARTICLE 8-A

SMART SURVEILLANCE DEVICE PRIVACY ACT

Section 86. Short title.

86-a. Definitions.

86-b. Access to surveillance information; warrant requirement.

86-c. Warrant requirements.

86-d. Emergency access and judicial review.

86-e. Notice to users.

86-f. Voluntary disclosures by operators.

86-g. Suppression, enforcement, and immunity.

86-h. Admissibility.

86-i. Severability.

15 § 86. Short title. This article shall be known and may be cited as the
16 "smart surveillance device privacy act".

17 § 86-a. Definitions. As used in this article, the following terms
18 shall have the following meanings:

19 1. "Adverse result" means danger to the life or physical safety of a
20 person, flight from prosecution, destruction of or tampering with
21 evidence, intimidation of potential witnesses, or serious jeopardy to an
22 investigation or undue delay of a trial.

EXPLANATION--Matter in italics (underscored) is new; matter in brackets
[-] is old law to be omitted.

LBD13638-01-5

1 2. "Authorized possessor" means the owner of a smart surveillance
2 device or a person authorized by the owner to possess and control the
3 device.

4 3. "Government entity" means any state, local, or federal law enforce-
5 ment agency, or any individual acting on behalf of such an agency,
6 including but not limited to police departments, sheriffs' offices,
7 district attorneys, immigration enforcement agencies, the federal bureau
8 of investigation, or any political subdivision of the state.

9 4. "Operator" means any person, company, or entity that manufactures,
10 sells, leases, or provides services to users of smart surveillance
11 devices, or maintains, stores, or has the ability to access data
12 collected by such devices.

13 5. "Specific consent" means consent given directly to the government
14 entity seeking access to surveillance information, provided voluntarily
15 by the authorized possessor.

16 6. "Smart surveillance device" means any internet-connected video or
17 audio recording device, including but not limited to video doorbells,
18 home security cameras, or similar systems, that records, transmits, or
19 stores video or audio of the exterior or interior of a residence or
20 other private property.

21 7. "Surveillance information" means any video, audio, or associated
22 metadata, including location data, timestamps, and device identifiers,
23 created, stored, or transmitted by a smart surveillance device.

24 § 86-b. Access to surveillance information; warrant requirement. 1. A
25 government entity shall not compel the production of surveillance infor-
26 mation from an operator, nor directly access a smart surveillance
27 device, except:

28 (a) pursuant to a valid search warrant issued by a neutral magistrate
29 based on probable cause;

30 (b) with the specific consent of the authorized possessor of the
31 device;

32 (c) in the case of a reported lost or stolen device, with the specific
33 consent of the owner for the purpose of identifying or contacting the
34 authorized possessor; or

35 (d) in a bona fide emergency involving imminent danger of death or
36 serious physical injury, provided the government entity applies for
37 judicial authorization within seventy-two hours of such access.

38 2. Any provision of a contract, terms of service, memorandum of under-
39 standing, or other agreement between an operator and a government entity
40 that permits access to surveillance information without a warrant or
41 specific consent is void and unenforceable as against public policy.

42 § 86-c. Warrant requirements. 1. A warrant issued under this article
43 shall describe with particularity:

44 (a) the specific surveillance information sought;

45 (b) the time period covered by the request;

46 (c) the targeted device or account; and

47 (d) the location of the device, if known.

48 2. Any surveillance information obtained that is unrelated to the
49 objectives of the warrant shall be sealed and may not be accessed,
50 retained, or disclosed without a separate court order upon a showing of
51 good cause.

52 § 86-d. Emergency access and judicial review. 1. If surveillance
53 information is accessed under paragraph (d) of subdivision one of
54 section eighty-six-b of this article, the government entity shall apply
55 for a warrant or judicial approval within seventy-two hours.

1 2. If judicial approval is denied or the court determines that the
2 emergency did not justify the access, it shall order the destruction of
3 all such information and immediate notification to the authorized
4 possessor.

5 § 86-e. Notice to users. 1. Except as provided in subdivision two of
6 this section, a government entity obtaining surveillance information
7 shall notify the authorized possessor contemporaneously with execution
8 of the warrant, or within seventy-two hours of emergency access.

9 2. A court may delay notice for up to ninety days upon a showing that
10 immediate notice may result in an adverse result. Extensions may be
11 granted upon motion and good cause shown.

12 3. Upon expiration of a delay, the government entity shall provide the
13 authorized possessor with a copy of the warrant or statement of emergen-
14 cy access, and a summary of the information obtained.

15 § 86-f. Voluntary disclosures by operators. 1. An operator may
16 disclose surveillance information voluntarily only when not otherwise
17 prohibited by law.

18 2. A government entity receiving such information voluntarily shall
19 destroy it within ninety days unless:

20 (a) specific consent for retention is given by the authorized posses-
21 sor;

22 (b) a court order authorizes retention upon a showing of ongoing
23 investigative necessity; or

24 (c) the information relates to child sexual exploitation and is
25 entered into a state- or federally-recognized multi-agency database used
26 solely for such investigations.

27 § 86-g. Suppression, enforcement, and immunity. 1. Any person may move
28 pursuant to section 710.60 of the criminal procedure law to suppress
29 surveillance information obtained in violation of this article.

30 2. The attorney general may bring civil actions to enforce this arti-
31 cle.

32 3. An operator or its employees who act in good faith reliance on a
33 valid warrant, court order, or emergency request shall be immune from
34 liability for disclosure made pursuant to such authorization.

35 § 86-h. Admissibility. Any surveillance information obtained or
36 retained in violation of this article shall be inadmissible in any crim-
37 inal, civil, or administrative proceeding.

38 § 86-i. Severability. If any provision of this article or the applica-
39 tion thereof to any person or circumstance is held invalid, such inva-
40 lidity shall not affect other provisions or applications of this article
41 which can be given effect without the invalid provision or application,
42 and to this end the provisions of this article are declared to be sever-
43 able.

44 § 2. This act shall take effect on the ninetieth day after it shall
45 have become a law.