

119TH CONGRESS
2D SESSION

H. R. 9716

To prohibit Federal law enforcement agencies from using or accessing State or local surveillance equipment or data to circumvent warrant requirements, to establish a Jurisdictional Wall List of covered technologies, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 15, 2026

Mr. SELF (for himself, Mr. CRANE, and Mr. CLYDE) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Oversight and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To prohibit Federal law enforcement agencies from using or accessing State or local surveillance equipment or data to circumvent warrant requirements, to establish a Jurisdictional Wall List of covered technologies, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Protecting Rights in
3 Video and Equipment Acquired Discovery Act” or the
4 “PRIVACY Act”.

5 **SEC. 2. USE OF STATE OR LOCAL SURVEILLANCE DEVICES**
6 **AND DATA BY FEDERAL LAW ENFORCEMENT**
7 **AGENCIES.**

8 (a) JURISDICTIONAL WALL LIST.—

9 (1) ESTABLISHMENT.—The Attorney General
10 shall create and maintain a list of surveillance de-
11 vices and technologies operated by State or local law
12 enforcement agencies that collect surveillance data to
13 be known as the “Jurisdictional Wall List”.

14 (2) CONTENTS.—The list shall include, at a
15 minimum—

16 (A) automated license plate readers;

17 (B) cameras that capture images of a vehi-
18 cle’s occupants;

19 (C) cameras that provide continuous cov-
20 erage of a particular location;

21 (D) long-range microphones;

22 (E) electronic fingerprint detection tech-
23 nology;

24 (F) field chemical scanners; and

1 (G) any substantially similar technology
2 determined appropriate by the Attorney Gen-
3 eral.

4 (3) PERIODIC REVIEW.—At least every 90 days,
5 the Attorney General shall review the list and deter-
6 mine whether to add, remove, or redesignate any de-
7 vices or technologies.

8 (4) NOTICE OF ADDITIONS.—The Attorney
9 General shall publish in the Federal Register any
10 addition to the list under paragraph (3), not less
11 than 30 days prior to the effective date of such addi-
12 tion, including a description sufficient to identify the
13 device or technology and its primary collection capa-
14 bilities.

15 (b) WARRANT REQUIREMENT.—Except as provided
16 in subsection (e), the head of a Federal law enforcement
17 agency may not access, receive, query, direct, task, or oth-
18 erwise obtain covered surveillance data without a warrant
19 issued by a Federal judge.

20 (c) RETENTION; USE AS EVIDENCE.—

21 (1) RETENTION LIMITATION.—The head of a
22 Federal law enforcement agency may not retain cov-
23 ered surveillance data obtained pursuant to sub-
24 section (b) for more than 30 days unless—

1 (A) the issuing court authorizes extended
2 retention for good cause shown, not to exceed
3 an additional 90 days; or

4 (B) the data constitutes evidence in an on-
5 going prosecution for which charges have been
6 filed, in which case the retention of such data
7 shall be limited to the needs of the prosecution
8 and subject to protective orders.

9 (2) SUPPRESSION AND INADMISSIBILITY.—

10 (A) IN GENERAL.—If the head of a Fed-
11 eral law enforcement agency obtains covered
12 surveillance data without a warrant in violation
13 of subsection (b), or retains covered surveillance
14 data lawfully obtained longer than permitted
15 under paragraph (1), such data may not be ad-
16 mitted by the prosecution as evidence in any
17 trial, hearing, or other proceeding in Federal
18 court.

19 (B) NOT EXCLUDED FROM DISCLOSURE.—
20 The Government may not exclude data de-
21 scribed in subparagraph (A) from any disclo-
22 sure obligation in a proceeding in Federal Court
23 solely on the basis of the manner in which such
24 data was obtained.

1 (C) APPLICATION OF RULE 16.—Data de-
2 scribed in subparagraph (A) that is within the
3 possession, custody, or control of the Govern-
4 ment shall be subject to the disclosure require-
5 ments of Rule 16 of the Federal Rules of
6 Criminal Procedure, including the requirement
7 that the Government permit inspection, copy-
8 ing, or photographing of such materials when
9 material to preparing the defense, intended for
10 use in the Government’s case in chief, or ob-
11 tained from or belonging to the defendant.

12 (D) BRADY OBLIGATIONS.—Notwith-
13 standing any other provision of law, the Gov-
14 ernment shall disclose to the defendant any in-
15 formation described in paragraph (A) that is fa-
16 vorable to the accused and material to guilt or
17 punishment, including exculpatory or impeach-
18 ment evidence, consistent with any applicable
19 constitutional requirements.

20 (E) NO WAIVER OF OTHER REMEDIES.—
21 Nothing in this section shall be construed to
22 limit a defendant’s ability to seek suppression
23 of evidence obtained by impermissible means or
24 to pursue any other remedy available under the
25 Constitution or laws of the United States.

1 (3) INCIDENTAL COLLECTION.—If the head of a
2 Federal law enforcement agency obtains covered sur-
3 veillance data pursuant to subsection (b), and in the
4 course of doing so, obtains covered surveillance data
5 that exceeds the scope of the warrant, they shall
6 minimize and dispose of such data, and may not use
7 such data for any investigative or evidentiary pur-
8 pose, except as otherwise required by law to prevent
9 an imminent threat to life where no less intrusive al-
10 ternative exists.

11 (d) RECORD KEEPING.—If the head of a Federal law
12 enforcement agency obtains covered surveillance data pur-
13 suant to subsection (b), they shall maintain contempora-
14 neous records of each access, query, acquisition, direction,
15 or tasking, including the warrant number, issuing court,
16 date ranges, devices or technologies involved, and any re-
17 tention extensions, and shall make such records available
18 for review by the Attorney General.

19 (e) EXCEPTIONS; DEFINED RIGHTS.—

20 (1) EMERGENCY EXCEPTION.—

21 (A) IN GENERAL.—The requirements
22 under this section shall not apply if the head of
23 a Federal law enforcement agency reasonably
24 believes that an emergency involving imminent
25 danger of death or serious physical injury re-

1 quires the immediate acquisition of covered sur-
2 veillance data and that obtaining a warrant is
3 impracticable.

4 (B) MINIMUM DATA NECESSARY.—Any
5 covered surveillance data acquired under this
6 paragraph shall be limited to the minimum
7 amount of data necessary to prevent death or
8 serious physical injury.

9 (C) DISPOSAL OF DATA.—The head of a
10 Federal law enforcement agency that acquires
11 covered surveillance data under this paragraph
12 shall document such acquisition not later than
13 24 hours after acquiring the data, and dispose
14 of such data not later than 30 days after ac-
15 quiring the data, unless the head of the agency
16 obtains a warrant for such data in accordance
17 with this section.

18 (2) CONSENT.—The requirements under this
19 section shall not apply if the person to whom the
20 covered surveillance data pertains provides vol-
21 untary, informed, written consent to the head of the
22 agency to access the data.

1 **SEC. 3. LIMITATIONS ON FEDERAL FUNDING FOR SURVEIL-**
2 **LANCE DEVICES.**

3 (a) PROHIBITION.—No Federal funds may be used
4 to purchase, acquire, or install a surveillance device or
5 technology listed on the Jurisdictional Wall List.

6 (b) EXCEPTIONS.—Subsection (a) shall not apply to
7 the use of grant funds for—

8 (1) systems used solely as part of a federally
9 funded highway for the collection of tolls;

10 (2) school violence prevention programs, with
11 respect to which the device or technology is limited
12 in scope, operated with parental and community
13 oversight, and subject to minimization and retention
14 limits that are consistent with this Act;

15 (3) grants under section 1701 of the Omnibus
16 Crime Control and Safe Streets Act of 1968 (34
17 U.S.C. 10381), if the use of the device or technology
18 is subject to minimization and retention limits that
19 are consistent with this Act; or

20 (4) portable systems operated for specific, case-
21 bounded law enforcement purposes pursuant to a
22 duly issued warrant, and subject to minimization
23 and retention limits consistent with this Act.

24 (c) BYRNE JAG AMENDMENT.—Section 501(a) of the
25 Omnibus Crime Control and Safe Streets Act of 1968 (34

1 U.S.C. 10152(a)) is amended by adding at the end the
2 following:

3 “(3) LIMITATION ON USE OF GRANT.—A grant
4 under this part may not be used to purchase, ac-
5 quire, or install a surveillance device or technology
6 on Jurisdictional Wall List established under section
7 2 of the Protecting Rights in Video and Equipment
8 Acquired Discovery Act.”.

9 **SEC. 4. REPORTING TO CONGRESSIONAL COMMITTEES.**

10 (a) SEMIANNUAL REPORTS.—Beginning 180 days
11 after the effective date of this Act, and every 180 days
12 thereafter, the Attorney General shall submit to the Com-
13 mittees on the Judiciary of the House of Representatives
14 and of the Senate a report detailing for the previous 180-
15 day period—

16 (1) the number of incidents in which Federal
17 law enforcement agencies accessed, received, queried,
18 directed, tasked, or otherwise obtained covered sur-
19 veillance data;

20 (2) the number and nature of warrants ob-
21 tained for the acquisition of such data, including the
22 courts that issued such warrants, and the general
23 categories of offenses for which the data was sought;

1 (3) the number of emergency exception uses
2 under section 2(e)(1), including justifications and
3 outcomes; and

4 (4) any instances in which a Federal law en-
5 forcement agency obtained covered surveillance data
6 without a warrant in violation of subsection (b), or
7 retained covered surveillance data lawfully obtained
8 longer than permitted under paragraph (1), and any
9 corrective actions taken by the agency.

10 (b) AGENCY REPORTING.—The head of each Federal
11 law enforcement agency that obtains covered surveillance
12 data shall provide such information as is necessary to the
13 Attorney General for purposes of the reports under sub-
14 section (a).

15 (c) PUBLIC SUMMARY.—The Attorney General shall
16 make an unclassified summary of each report publicly
17 available.

18 **SEC. 5. MINIMIZATION STANDARDS.**

19 The Attorney General shall promulgate regulations—

20 (1) establishing minimization procedures appli-
21 cable to the acquisition of covered surveillance data
22 under this Act including—

23 (A) prompt deletion of non-pertinent data;

1 (B) strict segregation of data to prevent
2 the use of such data outside the scope of the
3 warrant; and

4 (C) a prohibition on using covered surveil-
5 lance data to identify individuals engaged in
6 protected First Amendment activity absent
7 probable cause and a warrant;

8 (2) providing for the auditing of Federal law
9 enforcement agencies to ensure compliance with the
10 requirements under this Act; and

11 (3) providing for training for employees of Fed-
12 eral law enforcement agencies to ensure compliance
13 with the requirements under this Act.

14 **SEC. 6. NO RETALIATORY USE.**

15 The head of a Federal law enforcement agency may
16 not use covered surveillance data to monitor, track, or lo-
17 cate an individual based solely on the exercise of rights
18 secured by the First Amendment to the Constitution.

19 **SEC. 7. RULES OF CONSTRUCTION.**

20 Nothing in this Act may be construed to—

21 (1) authorize any collection of surveillance data
22 not otherwise permitted by law;

23 (2) diminish State or local obligations to comply
24 with the laws of the State or locality; or

1 (3) limit any greater privacy protections af-
2 fording by other Federal or State law.

3 **SEC. 8. ENFORCEMENT.**

4 (a) CIVIL ACTION.—Any person with respect to whom
5 the head of a Federal law enforcement agency obtains cov-
6 ered surveillance data in violation of this Act may bring
7 a civil action in an appropriate United States district court
8 against the United States, any Federal law enforcement
9 agency, or officer or employee thereof acting in an official
10 capacity, for declaratory and injunctive relief, actual dam-
11 ages, and reasonable attorney’s fees and costs. Sovereign
12 immunity is waived to the extent necessary to provide such
13 relief.

14 (b) ADMINISTRATIVE SANCTIONS.—An employee of a
15 Federal law enforcement agency who knowingly or reck-
16 lessly violates this Act shall be subject to appropriate ad-
17 ministrative sanctions, including suspension, termination,
18 and referral to the Office of Professional Responsibility
19 of the applicable Federal law enforcement agency.

20 (c) INSPECTOR GENERAL OVERSIGHT.—The Inspec-
21 tor General of each Federal law enforcement agency shall
22 conduct periodic audits of the compliance of the relevant
23 Federal law enforcement agency with this Act and shall
24 report their findings and recommendations to the Attorney

1 General and to the Committees on the Judiciary of the
2 House of Representatives and of the Senate.

3 **SEC. 9. SEVERABILITY; CONSTITUTIONAL VALIDITY.**

4 (a) SEVERABILITY.—If any provision of this Act, or
5 the application of such provision to any person or cir-
6 cumstance, is held to be invalid, the remainder of this Act,
7 and the application of the remaining provisions to any per-
8 son or circumstance, shall not be affected.

9 (b) CONSTITUTIONAL VALIDITY.—Nothing in this
10 Act shall be construed to limit, diminish, or expand the
11 validity of the Constitution of the United States, including
12 rights secured by the Fourth Amendment.

13 (c) OTHER LAW.—This Act does not limit require-
14 ments under chapters 119 and 121 of title 18, United
15 States Code (commonly referred to as the “Electronic
16 Communications Privacy Act”), section 552a of title 5,
17 United States Code.

18 **SEC. 10. DEFINITIONS.**

19 In this Act:

20 (1) SURVEILLANCE DATA.—The term “surveil-
21 lance data” means any image, video, audio, signal,
22 location information, metadata, or derivative analyt-
23 ical output collected, generated, or stored by a sur-
24 veillance device or technology.

1 (2) COVERED SURVEILLANCE DATA.—The term
2 “covered surveillance data” means surveillance data
3 that is collected by a State or local law enforcement
4 agency using any device or technology that is on the
5 Jurisdictional Wall List as of the date of the collec-
6 tion of such data.

7 (3) FEDERAL LAW ENFORCEMENT AGENCY.—
8 The term “Federal law enforcement agency” has the
9 meaning given such term in section 2 of the En-
10 hanced Border Security and Visa Entry Reform Act
11 of 2002 (8 U.S.C. 1701).

12 **SEC. 11. EFFECTIVE DATE.**

13 This Act and the amendments made by this Act shall
14 take effect on the date that is 180 days after the date of
15 enactment of this Act.

○