

.....
(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

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

Mr. SELF introduced the following bill; which was referred to the Committee
on _____

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,*

3 **SECTION 1. SHORT TITLE.**

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

1 **SEC. 2. USE OF STATE OR LOCAL SURVEILLANCE DEVICES**
2 **AND DATA BY FEDERAL LAW ENFORCEMENT**
3 **AGENCIES.**

4 (a) JURISDICTIONAL WALL LIST.—

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

10 (2) CONTENTS.—The list shall include, at a
11 minimum—

12 (A) automated license plate readers;

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

15 (C) cameras that provide continuous cov-
16 erage of a particular location;

17 (D) long-range microphones;

18 (E) electronic fingerprint detection tech-
19 nology;

20 (F) field chemical scanners; and

21 (G) any substantially similar technology
22 determined appropriate by the Attorney Gen-
23 eral.

24 (3) PERIODIC REVIEW.—At least every 90 days,
25 the Attorney General shall review the list and deter-

1 mine whether to add, remove, or redesignate any de-
2 vices or technologies.

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

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

15 (c) RETENTION; USE AS EVIDENCE.—

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

20 (A) the issuing court authorizes extended
21 retention for good cause shown, not to exceed
22 an additional 90 days; or

23 (B) the data constitutes evidence in an on-
24 going prosecution for which charges have been
25 filed, in which case the retention of such data

1 shall be limited to the needs of the prosecution
2 and subject to protective orders.

3 (2) SUPPRESSION AND INADMISSIBILITY.—

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

13 (B) NOT EXCLUDED FROM DISCLOSURE.—
14 The Government may not exclude data de-
15 scribed in subparagraph (A) from any disclo-
16 sure obligation in a proceeding in Federal Court
17 solely on the basis of the manner in which such
18 data was obtained.

19 (C) APPLICATION OF RULE 16.— Data de-
20 scribed in subparagraph (A) that is within the
21 possession, custody, or control of the Govern-
22 ment shall be subject to the disclosure require-
23 ments of Rule 16 of the Federal Rules of
24 Criminal Procedure, including the requirement
25 that the Government permit inspection, copy-

1 ing, or photographing of such materials when
2 material to preparing the defense, intended for
3 use in the Government's case in chief, or ob-
4 tained from or belonging to the defendant.

5 (D) BRADY OBLIGATIONS.—Notwith-
6 standing any other provision of law, the Gov-
7 ernment shall disclose to the defendant any in-
8 formation described in paragraph (A) that is fa-
9 vorable to the accused and material to guilt or
10 punishment, including exculpatory or impeach-
11 ment evidence, consistent with any applicable
12 constitutional requirements.

13 (E) NO WAIVER OF OTHER REMEDIES.—
14 Nothing in this section shall be construed to
15 limit a defendant's ability to seek suppression
16 of evidence obtained by impermissible means or
17 to pursue any other remedy available under the
18 Constitution or laws of the United States.

19 (3) INCIDENTAL COLLECTION.—If the head of a
20 Federal law enforcement agency obtains covered sur-
21 veillance data pursuant to subsection (b), and in the
22 course of doing so, obtains covered surveillance data
23 that exceeds the scope of the warrant, they shall
24 minimize and dispose of such data, and may not use
25 such data for any investigative or evidentiary pur-

1 pose, except as otherwise required by law to prevent
2 an imminent threat to life where no less intrusive al-
3 ternative exists.

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

12 (e) EXCEPTIONS; DEFINED RIGHTS.—

13 (1) EMERGENCY EXCEPTION.—

14 (A) IN GENERAL.—The requirements
15 under this section shall not apply if the head of
16 a Federal law enforcement agency reasonably
17 believes that an emergency involving imminent
18 danger of death or serious physical injury re-
19 quires the immediate acquisition of covered sur-
20 veillance data and that obtaining a warrant is
21 impracticable.

22 (B) MINIMUM DATA NECESSARY.—Any
23 covered surveillance data acquired under this
24 paragraph shall be limited to the minimum

1 amount of data necessary to prevent death or
2 serious physical injury.

3 (C) DISPOSAL OF DATA.—The head of a
4 Federal law enforcement agency that acquires
5 covered surveillance data under this paragraph
6 shall document such acquisition not later than
7 24 hours after acquiring the data, and dispose
8 of such data not later than 30 days after ac-
9 quiring the data, unless the head of the agency
10 obtains a warrant for such data in accordance
11 with this section.

12 (2) CONSENT.—The requirements under this
13 section shall not apply if the person to whom the
14 covered surveillance data pertains provides vol-
15 untary, informed, written consent to the head of the
16 agency to access the data.

17 **SEC. 3. LIMITATIONS ON FEDERAL FUNDING FOR SURVEIL-**
18 **LANCE DEVICES.**

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

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

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

1 (2) school violence prevention programs, with
2 respect to which the device or technology is limited
3 in scope, operated with parental and community
4 oversight, and subject to minimization and retention
5 limits that are consistent with this Act;

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

11 (4) portable systems operated for specific, case-
12 bounded law enforcement purposes pursuant to a
13 duly issued warrant, and subject to minimization
14 and retention limits consistent with this Act.

15 (c) BYRNE JAG AMENDMENT.—Section 501(a) of the
16 Omnibus Crime Control and Safe Streets Act of 1968 (34
17 U.S.C. 10152(a)) is amended by adding at the end the
18 following:

19 “(3) LIMITATION ON USE OF GRANT.—A grant
20 under this part may not be used to purchase, ac-
21 quire, or install a surveillance device or technology
22 on Jurisdictional Wall List established under section
23 2 of the Protecting Rights in Video and Equipment
24 Acquired Discovery Act.”.

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

2 (a) SEMIANNUAL REPORTS.—Beginning 180 days
3 after the effective date of this Act, and every 180 days
4 thereafter, the Attorney General shall submit to the Com-
5 mittees on the Judiciary of the House of Representatives
6 and of the Senate a report detailing for the previous 180-
7 day period—

8 (1) the number of incidents in which Federal
9 law enforcement agencies accessed, received, queried,
10 directed, tasked, or otherwise obtained covered sur-
11 veillance data;

12 (2) the number and nature of warrants ob-
13 tained for the acquisition of such data, including the
14 courts that issued such warrants, and the general
15 categories of offenses for which the data was sought;

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

19 (4) any instances in which a Federal law en-
20 forcement agency obtained covered surveillance data
21 without a warrant in violation of subsection (b), or
22 retained covered surveillance data lawfully obtained
23 longer than permitted under paragraph (1), and any
24 corrective actions taken by the agency.

25 (b) AGENCY REPORTING.—The head of each Federal
26 law enforcement agency that obtains covered surveillance

1 data shall provide such information as is necessary to the
2 Attorney General for purposes of the reports under sub-
3 section (a).

4 (c) PUBLIC SUMMARY.—The Attorney General shall
5 make an unclassified summary of each report publicly
6 available.

7 **SEC. 5. MINIMIZATION STANDARDS.**

8 The Attorney General shall promulgate regulations—

9 (1) establishing minimization procedures appli-
10 cable to the acquisition of covered surveillance data
11 under this Act including—

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

13 (B) strict segregation of data to prevent
14 the use of such data outside the scope of the
15 warrant;

16 (C) a prohibition on using covered surveil-
17 lance data to identify individuals engaged in
18 protected First Amendment activity absent
19 probable cause and a warrant; and

20 (2) providing for the auditing of Federal law
21 enforcement agencies to ensure compliance with the
22 requirements under this Act; and

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

1 **SEC. 6. NO RETALIATORY USE.**

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

6 **SEC. 7. RULES OF CONSTRUCTION.**

7 Nothing in this Act may be construed to—

8 (1) authorize any collection of surveillance data
9 not otherwise permitted by law;

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

12 (3) limit any greater privacy protections af-
13 forded by other Federal or State law.

14 **SEC. 8. ENFORCEMENT.**

15 (a) CIVIL ACTION.—Any person with respect to whom
16 the head of a Federal law enforcement agency obtains cov-
17 ered surveillance data in violation of this Act may bring
18 a civil action in an appropriate United States district court
19 against the United States, any Federal law enforcement
20 agency, or officer or employee thereof acting in an official
21 capacity, for declaratory and injunctive relief, actual dam-
22 ages, and reasonable attorney’s fees and costs. Sovereign
23 immunity is waived to the extent necessary to provide such
24 relief.

25 (b) ADMINISTRATIVE SANCTIONS.—An employee of a
26 Federal law enforcement agency who knowingly or reck-

1 lessly violates this Act shall be subject to appropriate ad-
2 ministrative sanctions, including suspension, termination,
3 and referral to the Office of Professional Responsibility
4 of the applicable Federal law enforcement agency.

5 (c) INSPECTOR GENERAL OVERSIGHT.—The Inspec-
6 tor General of each Federal law enforcement agency shall
7 conduct periodic audits of the compliance of the relevant
8 Federal law enforcement agency with this Act and shall
9 report their findings and recommendations to the Attorney
10 General and to the Committees on the Judiciary of the
11 House of Representatives and of the Senate.

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

13 (a) SEVERABILITY.—If any provision of this Act, or
14 the application of such provision to any person or cir-
15 cumstance, is held to be invalid, the remainder of this Act,
16 and the application of the remaining provisions to any per-
17 son or circumstance, shall not be affected.

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

22 (c) OTHER LAW.—This Act does not limit require-
23 ments under chapters 119 and 121 of title 18, United
24 States Code (commonly referred to as the “Electronic

1 Communications Privacy Act”), section 552a of title 5,
2 United States Code.

3 **SEC. 10. DEFINITIONS.**

4 In this Act:

5 (1) **SURVEILLANCE DATA.**—The term “surveil-
6 lance data” means any image, video, audio, signal,
7 location information, metadata, or derivative analyt-
8 ical output collected, generated, or stored by a sur-
9 veillance device or technology.

10 (2) **COVERED SURVEILLANCE DATA.**—The term
11 “covered surveillance data” means surveillance data
12 that is collected by a State or local law enforcement
13 agency using any device or technology that is on the
14 Jurisdictional Wall List as of the date of the collec-
15 tion of such data.

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

21 **SEC. 11. EFFECTIVE DATE.**

22 This Act and the amendments made by this Act shall
23 take effect on the date that is 180 days after the date of
24 enactment of this Act.