

.....
(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R.

To amend title 18, United States Code, to ensure that all searches that significantly impinge on the privacy or security of a person require a warrant based on probable cause, to provide a right of action for violations of Fourth Amendment rights, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

To amend title 18, United States Code, to ensure that all searches that significantly impinge on the privacy or security of a person require a warrant based on probable cause, to provide a right of action for violations of Fourth Amendment rights, 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 “Surveillance Account-
5 ability Act”.

1 **SEC. 2. WARRANT REQUIREMENT FOR SEARCHES.**

2 (a) IN GENERAL.—Chapter 205 of title 18, United
3 States Code, is amended by adding at the end the fol-
4 lowing new section:

5 **“§ 3119. Searches to accord with the Fourth Amend-**
6 **ment**

7 “(a) WARRANT REQUIREMENT.—

8 “(1) IN GENERAL.—Except as provided in sub-
9 section (b), no search may be conducted without a
10 warrant issued by a neutral and detached magistrate
11 upon probable cause, supported by oath or affirma-
12 tion, and particularly describing the place to be
13 searched and the persons or things to be seized.

14 “(2) THIRD-PARTY DATA.—

15 “(A) PRESUMPTION OF PRIVACY.—The
16 government shall not access any data,
17 metadata, or personal information held by a
18 third party, including financial services pro-
19 viders, telecommunication service providers,
20 internet service providers, cloud storage compa-
21 nies, or data brokers, without a valid warrant,
22 regardless of whether the third party consents
23 or cooperates.

24 “(B) EXCEPTION INVALIDATED.—No con-
25 tractual agreement between a user and a third
26 party may be interpreted as waiving the govern-

1 ment’s warrant requirement for access to the
2 data of that user, unless such waiver is know-
3 ing, voluntary, and explicit.

4 “(b) EXCEPTIONS.—The following may be conducted
5 without a warrant:

6 “(1) Plain-view searches.

7 “(2) The verification of government-issued pri-
8 mary photo identification documents during a stop
9 of a motor vehicle, travel, or other interactions with
10 law enforcement, including the verification of—

11 “(A) a State identification card;

12 “(B) a driver’s license;

13 “(C) a passport;

14 “(D) a passport card;

15 “(E) a military identification; or

16 “(F) a permanent resident card.

17 “(3) The collection or analysis of information
18 that is lawfully published or voluntarily made avail-
19 able by a person or entity to a public audience, and
20 which requires no circumvention of privacy settings,
21 encryption, or other access controls.

22 “(4) The use of lawful investigative techniques
23 to collect data from publicly available sources such
24 as new outlets, official government publications, pub-
25 lic records, or user-posted content that is clearly ac-

1 cessible to the general public without special access
2 or tools.

3 “(5) Searches conducted with consent.

4 “(6) Searched conducted under exigent cir-
5 cumstances.

6 “(c) LIMITATIONS.—The exceptions described in sub-
7 section (b) shall not be construed to permit the
8 warrantless collection, retention, querying, or analysis of
9 data exposed to public view or accessible to a third party
10 if the person associated with the collected identifiers did
11 not express informed and voluntary consent to such collec-
12 tion with respect to data gathered by entering a public
13 place, operating a motor vehicle on a public roadway, or
14 patronizing a private establishment open to the public, in-
15 cluding—

16 “(1) biometric data, including facial images,
17 faceprints, gait, voice recognition, or other unique
18 physical identifiers, obtained through facial recogni-
19 tion systems or comparable surveillance technologies;
20 or

21 “(2) license plate images, vehicle metadata, or
22 vehicle movement patterns obtained through auto-
23 mated license plate readers or similar systems.

24 “(d) DEFINITONS.—In this section:

1 “(1) SEARCH.—The term ‘search’ means any
2 government-initiated act that intrudes upon an indi-
3 vidual’s reasonable expectation of privacy, including
4 the following:

5 “(A) INVESTIGATORY ACTS.—Any inves-
6 tigatory act purposefully directed at a specific
7 person or entity, or the property of a specific
8 person or entity, with the intent of obtaining in-
9 formation not otherwise available to the public.

10 “(B) GOVERNMENT SURVEILLANCE AND
11 MONITORING.—Any non-consensual surveil-
12 lance, monitoring, or inquiry conducted by a
13 government entity or its agents, whether
14 through human, digital, or automated means,
15 that collects information on a specific individual
16 or entity, including information on that indi-
17 vidual or entity’s—

18 “(i) communications;

19 “(ii) associations;

20 “(iii) employment;

21 “(iv) social media usage;

22 “(v) internet usage;

23 “(vi) financial transactions; or

24 “(vii) travel.

1 “(C) COLLECTION OF PERSONAL DATA.—

2 The acquisition and analysis of any data,
3 metadata, or information pertaining to a per-
4 son’s digital or physical life, including—

5 “(i) geolocation;

6 “(ii) communication records;

7 “(iii) personal device activity;

8 “(iv) assets;

9 “(v) liabilities;

10 “(vi) biometric identifiers;

11 “(vii) behavioral signals data; or

12 “(viii) financial transactions.

13 “(2) PLAIN-VIEW SEARCHES DEFINED.—In this
14 section, the term ‘plain-view searches’ means the ob-
15 servation or seizure of evidence by a law enforce-
16 ment officer who is lawfully present at a location,
17 where the incriminating nature of the evidence is im-
18 mediately apparent, and where such observation is
19 incidental to the officer’s lawful presence and does
20 not involve the use of enhanced surveillance tech-
21 nology or systematic monitoring.

22 “(e) RULE OF CONSTRUCTION.—Nothing in this sec-
23 tion shall be construed to—

1 States or any person within the jurisdiction thereof to the
2 deprivation of any rights, privileges, or immunities secured
3 by the Fourth Amendment, shall be liable to the party
4 injured in an action at law, suit in equity, or other proper
5 proceeding for redress.

6 “(b) ATTORNEY’S FEES.—In any action, suit, or pro-
7 ceeding to enforce this Act, the court, in its discretion,
8 may allow the prevailing party, other than the United
9 States, a reasonable attorney’s fee as part of the costs.

10 “(c) FEDERAL EMPLOYEE DEFINED.—In this sec-
11 tion, the term ‘Federal employee’ means an individual
12 other than the President or the Vice President, who occu-
13 pies a position in any agency or instrumentality of the ex-
14 ecutive branch (including any independent agency).

15 “(d) RULE OF CONSTRUCTION.—Nothing in this sec-
16 tion shall be construed to authorize a Federal employee
17 to bring a suit against their Federal employer or the Fed-
18 eral Government for conduct that is within the scope of
19 the employment relationship.”.

20 (b) SEVERABILITY.—If any provision of this Act or
21 the application of such provision to any person or cir-
22 cumstance is held to be unconstitutional, the remainder
23 of this Act, and the application of this Act, to any other
24 person or circumstance, shall not be affected thereby.