

118TH CONGRESS
2D SESSION

H. R. 4639

IN THE SENATE OF THE UNITED STATES

APRIL 18, 2024

Received

AN ACT

To amend section 2702 of title 18, United States Code, to prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value, to address communications and records in the possession of intermediary internet service providers, 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 “Fourth Amendment
3 Is Not For Sale Act”.

4 **SEC. 2. PROTECTION OF RECORDS HELD BY DATA BRO-**
5 **KERS.**

6 Section 2702 of title 18, United States Code, is
7 amended by adding at the end the following:

8 “(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR
9 ANYTHING OF VALUE CERTAIN RECORDS AND INFORMA-
10 TION BY LAW ENFORCEMENT AND INTELLIGENCE AGEN-
11 CIES.—

12 “(1) DEFINITIONS.—In this subsection—

13 “(A) the term ‘covered customer or sub-
14 scriber record’ means a covered record that is—

15 “(i) disclosed to a third party by—

16 “(I) a provider of an electronic
17 communication service to the public or
18 a provider of a remote computing
19 service of which the covered person
20 with respect to the covered record is a
21 subscriber or customer; or

22 “(II) an intermediary service pro-
23 vider that delivers, stores, or proc-
24 esses communications of such covered
25 person;

1 “(ii) collected by a third party from
2 an online account of a covered person; or

3 “(iii) collected by a third party from
4 or about an electronic device of a covered
5 person;

6 “(B) the term ‘covered person’ means—

7 “(i) a person who is located inside the
8 United States; or

9 “(ii) a person—

10 “(I) who is located outside the
11 United States or whose location can-
12 not be determined; and

13 “(II) who is a United States per-
14 son, as defined in section 101 of the
15 Foreign Intelligence Surveillance Act
16 of 1978 (50 U.S.C. 1801);

17 “(C) the term ‘covered record’—

18 “(i) means a record or other informa-
19 tion that—

20 “(I) pertains to a covered person;

21 and

22 “(II) is—

23 “(aa) a record or other in-
24 formation described in the matter

1 preceding paragraph (1) of sub-
2 section (c);

3 “(bb) the contents of a com-
4 munication; or

5 “(cc) location information;
6 and

7 “(ii) does not include a record or
8 other information that—

9 “(I) has been voluntarily made
10 available to the general public by a
11 covered person on a social media plat-
12 form or similar service;

13 “(II) is lawfully available to the
14 public as a Federal, State, or local
15 government record or through other
16 widely distributed media;

17 “(III) is obtained by a law en-
18 forcement agency of a governmental
19 entity or an element of the intelligence
20 community for the purpose of con-
21 ducting a background check of a cov-
22 ered person—

23 “(aa) with the written con-
24 sent of such person;

1 “(bb) for access or use by
2 such agency or element for the
3 purpose of such background
4 check; and

5 “(cc) that is destroyed after
6 the date on which it is no longer
7 needed for such background
8 check; or

9 “(IV) is data generated by a pub-
10 lic or private ALPR system;

11 “(D) the term ‘electronic device’ has the
12 meaning given the term ‘computer’ in section
13 1030(e);

14 “(E) the term ‘illegitimately obtained in-
15 formation’ means a covered record that—

16 “(i) was obtained—

17 “(I) from a provider of an elec-
18 tronic communication service to the
19 public or a provider of a remote com-
20 puting service in a manner that—

21 “(aa) violates the service
22 agreement between the provider
23 and customers or subscribers of
24 the provider; or

1 “(bb) is inconsistent with
2 the privacy policy of the provider;

3 “(II) by deceiving the covered
4 person whose covered record was ob-
5 tained; or

6 “(III) through the unauthorized
7 accessing of an electronic device or
8 online account; or

9 “(ii) was—

10 “(I) obtained from a provider of
11 an electronic communication service to
12 the public, a provider of a remote
13 computing service, or an intermediary
14 service provider; and

15 “(II) collected, processed, or
16 shared in violation of a contract relat-
17 ing to the covered record;

18 “(F) the term ‘intelligence community’ has
19 the meaning given that term in section 3 of the
20 National Security Act of 1947 (50 U.S.C.
21 3003);

22 “(G) the term ‘location information’ means
23 information derived or otherwise calculated
24 from the transmission or reception of a radio
25 signal that reveals the approximate or actual

1 geographic location of a customer, subscriber,
2 or device;

3 “(H) the term ‘obtain in exchange for any-
4 thing of value’ means to obtain by purchasing,
5 to receive in connection with services being pro-
6 vided for consideration, or to otherwise obtain
7 in exchange for consideration, including an ac-
8 cess fee, service fee, maintenance fee, or licens-
9 ing fee;

10 “(I) the term ‘online account’ means an
11 online account with an electronic communica-
12 tion service to the public or remote computing
13 service;

14 “(J) the term ‘pertain’, with respect to a
15 person, means—

16 “(i) information that is linked to the
17 identity of a person; or

18 “(ii) information—

19 “(I) that has been anonymized to
20 remove links to the identity of a per-
21 son; and

22 “(II) that, if combined with other
23 information, could be used to identify
24 a person;

1 “(K) the term ‘third party’ means a person
2 who—

3 “(i) is not a governmental entity; and

4 “(ii) in connection with the collection,
5 disclosure, obtaining, processing, or shar-
6 ing of the covered record at issue, was not
7 acting as—

8 “(I) a provider of an electronic
9 communication service to the public;
10 or

11 “(II) a provider of a remote com-
12 puting service; and

13 “(L) the term ‘automated license plate rec-
14 ognition system’ or ‘ALPR system’ means a
15 system of one or more mobile or fixed high-
16 speed cameras combined with computer algo-
17 rithms to convert images of license plates into
18 computer-readable data.

19 “(2) LIMITATION.—

20 “(A) IN GENERAL.—A law enforcement
21 agency of a governmental entity and an element
22 of the intelligence community may not obtain
23 from a third party in exchange for anything of
24 value a covered customer or subscriber record
25 or any illegitimately obtained information.

1 “(B) INDIRECTLY ACQUIRED RECORDS
2 AND INFORMATION.—The limitation under sub-
3 paragraph (A) shall apply without regard to
4 whether the third party possessing the covered
5 customer or subscriber record or illegitimately
6 obtained information is the third party that ini-
7 tially obtained or collected, or is the third party
8 that initially received the disclosure of, the cov-
9 ered customer or subscriber record or illegit-
10 imately obtained information.

11 “(3) LIMIT ON SHARING BETWEEN AGEN-
12 CIES.—An agency of a governmental entity that is
13 not a law enforcement agency or an element of the
14 intelligence community may not provide to a law en-
15 forcement agency of a governmental entity or an ele-
16 ment of the intelligence community a covered cus-
17 tomer or subscriber record or illegitimately obtained
18 information that was obtained from a third party in
19 exchange for anything of value.

20 “(4) PROHIBITION ON USE AS EVIDENCE.—A
21 covered customer or subscriber record or illegit-
22 imately obtained information obtained by or pro-
23 vided to a law enforcement agency of a governmental
24 entity or an element of the intelligence community in
25 violation of paragraph (2) or (3), and any evidence

1 derived therefrom, may not be received in evidence
2 in any trial, hearing, or other proceeding in or be-
3 fore any court, grand jury, department, officer,
4 agency, regulatory body, legislative committee, or
5 other authority of the United States, a State, or a
6 political subdivision thereof.

7 “(5) MINIMIZATION PROCEDURES.—

8 “(A) IN GENERAL.—The Attorney General
9 shall adopt specific procedures that are reason-
10 ably designed to minimize the acquisition and
11 retention, and prohibit the dissemination, of in-
12 formation pertaining to a covered person that is
13 acquired in violation of paragraph (2) or (3).

14 “(B) USE BY AGENCIES.—If a law enforce-
15 ment agency of a governmental entity or ele-
16 ment of the intelligence community acquires in-
17 formation pertaining to a covered person in vio-
18 lation of paragraph (2) or (3), the law enforce-
19 ment agency of a governmental entity or ele-
20 ment of the intelligence community shall mini-
21 mize the acquisition and retention, and prohibit
22 the dissemination, of the information in accord-
23 ance with the procedures adopted under sub-
24 paragraph (A).”.

1 **SEC. 3. REQUIRED DISCLOSURE.**

2 Section 2703 of title 18, United States Code, is
3 amended by adding at the end the following:

4 “(i) COVERED CUSTOMER OR SUBSCRIBER RECORDS
5 AND ILLEGITIMATELY OBTAINED INFORMATION.—

6 “(1) DEFINITIONS.—In this subsection, the
7 terms ‘covered customer or subscriber record’, ‘illegi-
8 timately obtained information’, and ‘third party’
9 have the meanings given such terms in section
10 2702(e).

11 “(2) LIMITATION.—Unless a governmental enti-
12 ty obtains an order in accordance with paragraph
13 (3), the governmental entity may not require a third
14 party to disclose a covered customer or subscriber
15 record or any illegitimately obtained information if a
16 court order would be required for the governmental
17 entity to require a provider of remote computing
18 service or a provider of electronic communication
19 service to the public to disclose such a covered cus-
20 tomer or subscriber record or illegitimately obtained
21 information that is a record of a customer or sub-
22 scriber of the provider.

23 “(3) ORDERS.—

24 “(A) IN GENERAL.—A court may only
25 issue an order requiring a third party to dis-
26 close a covered customer or subscriber record or

1 any illegitimately obtained information on the
2 same basis and subject to the same limitations
3 as would apply to a court order to require dis-
4 closure by a provider of remote computing serv-
5 ice or a provider of electronic communication
6 service to the public of a record of a customer
7 or subscriber of the provider.

8 “(B) STANDARD.—For purposes of sub-
9 paragraph (A), a court shall apply the most
10 stringent standard under Federal statute or the
11 Constitution of the United States that would be
12 applicable to a request for a court order to re-
13 quire a comparable disclosure by a provider of
14 remote computing service or a provider of elec-
15 tronic communication service to the public of a
16 record of a customer or subscriber of the pro-
17 vider.”.

18 **SEC. 4. INTERMEDIARY SERVICE PROVIDERS.**

19 (a) DEFINITION.—Section 2711 of title 18, United
20 States Code, is amended—

- 21 (1) in paragraph (3), by striking “and” at the
22 end;
23 (2) in paragraph (4), by striking the period at
24 the end and inserting “; and”; and
25 (3) by adding at the end the following:

1 “(5) the term ‘intermediary service provider’
2 means an entity or facilities owner or operator that
3 directly or indirectly delivers, stores, or processes
4 communications for or on behalf of a provider of
5 electronic communication service to the public or a
6 provider of remote computing service.”.

7 (b) PROHIBITION.—Section 2702(a) of title 18,
8 United States Code, is amended—

9 (1) in paragraph (1), by striking “and” at the
10 end;

11 (2) in paragraph (2), by striking “and” at the
12 end;

13 (3) in paragraph (3), by striking the period at
14 the end and inserting “; and”; and

15 (4) by adding at the end the following:

16 “(4) an intermediary service provider shall not
17 knowingly divulge—

18 “(A) to any person or entity the contents
19 of a communication while in electronic storage
20 by that provider; or

21 “(B) to any governmental entity a record
22 or other information pertaining to a subscriber
23 to or customer of, a recipient of a communica-
24 tion from a subscriber to or customer of, or the
25 sender of a communication to a subscriber to or

1 customer of, the provider of electronic commu-
 2 nication service to the public or the provider of
 3 remote computing service for, or on behalf of,
 4 which the intermediary service provider directly
 5 or indirectly delivers, transmits, stores, or proc-
 6 esses communications.”.

7 **SEC. 5. LIMITS ON SURVEILLANCE CONDUCTED FOR FOR-**
 8 **EIGN INTELLIGENCE PURPOSES OTHER**
 9 **THAN UNDER THE FOREIGN INTELLIGENCE**
 10 **SURVEILLANCE ACT OF 1978.**

11 (a) IN GENERAL.—Section 2511(2)(f) of title 18,
 12 United States Code, is amended to read as follows:

13 “(f)(i)(A) Nothing contained in this chapter, chapter
 14 121 or 206 of this title, or section 705 of the Communica-
 15 tions Act of 1934 (47 U.S.C. 151 et seq.) shall be deemed
 16 to affect an acquisition or activity described in clause (B)
 17 that is carried out utilizing a means other than electronic
 18 surveillance, as defined in section 101 of the Foreign In-
 19 telligence Surveillance Act of 1978 (50 U.S.C. 1801).

20 “(B) An acquisition or activity described in this
 21 clause is—

22 “(I) an acquisition by the United States Gov-
 23 ernment of foreign intelligence information from
 24 international or foreign communications that—

1 “(aa) is acquired pursuant to express stat-
2 utory authority; or

3 “(bb) only includes information of persons
4 who are not United States persons and are lo-
5 cated outside the United States; or

6 “(II) a foreign intelligence activity involving a
7 foreign electronic communications system that—

8 “(aa) is conducted pursuant to express
9 statutory authority; or

10 “(bb) only involves the acquisition by the
11 United States Government of information of
12 persons who are not United States persons and
13 are located outside the United States.

14 “(ii) The procedures in this chapter, chapter 121,
15 and the Foreign Intelligence Surveillance Act of 1978 (50
16 U.S.C. 1801 et seq.) shall be the exclusive means by which
17 electronic surveillance, as defined in section 101 of such
18 Act, and the interception of domestic wire, oral, and elec-
19 tronic communications may be conducted.”.

20 (b) EXCLUSIVE MEANS RELATED TO COMMUNICA-
21 TIONS RECORDS.—The Foreign Intelligence Surveillance
22 Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive
23 means by which electronic communications transactions
24 records, call detail records, or other information from com-
25 munications of United States persons or persons inside the

1 United States are acquired for foreign intelligence pur-
2 poses inside the United States or from a person or entity
3 located in the United States that provides telecommuni-
4 cations, electronic communication, or remote computing
5 services.

6 (c) EXCLUSIVE MEANS RELATED TO LOCATION IN-
7 FORMATION, WEB BROWSING HISTORY, AND INTERNET
8 SEARCH HISTORY.—

9 (1) DEFINITION.—In this subsection, the term
10 “location information” has the meaning given that
11 term in subsection (e) of section 2702 of title 18,
12 United States Code, as added by section 2 of this
13 Act.

14 (2) EXCLUSIVE MEANS.—Title I and sections
15 303, 304, 702, 703, 704, and 705 of the Foreign In-
16 telligence Surveillance Act of 1978 (50 U.S.C. 1801
17 et seq., 1823, 1824, 1881a, 1881b, 1881c, 1881d)
18 shall be the exclusive means by which location infor-
19 mation, web browsing history, and internet search
20 history of United States persons or persons inside
21 the United States are acquired for foreign intel-
22 ligence purposes inside the United States or from a
23 person or entity located in the United States.

24 (d) EXCLUSIVE MEANS RELATED TO FOURTH
25 AMENDMENT-PROTECTED INFORMATION.—Title I and

1 sections 303, 304, 702, 703, 704, and 705 of the Foreign
2 Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et
3 seq., 1823, 1824, 1881a, 1881b, 1881c, 1881d) shall be
4 the exclusive means by which any information, records,
5 data, or tangible things are acquired for foreign intel-
6 ligence purposes from a person or entity located in the
7 United States if the compelled production of such informa-
8 tion, records, data, or tangible things would require a war-
9 rant for law enforcement purposes.

10 (e) DEFINITION.—In this section, the term “United
11 States person” has the meaning given that term in section
12 101 of the Foreign Intelligence Surveillance Act of 1978
13 (50 U.S.C. 1801).

14 **SEC. 6. LIMIT ON CIVIL IMMUNITY FOR PROVIDING INFOR-**
15 **MATION, FACILITIES, OR TECHNICAL ASSIST-**
16 **ANCE TO THE GOVERNMENT ABSENT A**
17 **COURT ORDER.**

18 Section 2511(2)(a) of title 18, United States Code,
19 is amended—

20 (1) in subparagraph (ii), by striking clause (B)
21 and inserting the following:

22 “(B) a certification in writing—

23 “(I) by a person specified in section
24 2518(7) or the Attorney General of the United
25 States;

7 (2) by striking subparagraph (iii) and inserting
8 the following:

Passed the House of Representatives April 17, 2024.

HR 4639 RDS