

APRIL 12, 2024

RULES COMMITTEE PRINT 118–28
TEXT OF H.R. 4639, FOURTH AMENDMENT IS
NOT FOR SALE ACT

[Showing the text of H.R. 4639, as ordered reported by the
Committee on the Judiciary]

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

1 service of which the covered person
2 with respect to the covered record is a
3 subscriber or customer; or

4 “(II) an intermediary service pro-
5 vider that delivers, stores, or proc-
6 esses communications of such covered
7 person;

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

10 “(iii) collected by a third party from
11 or about an electronic device of a covered
12 person;

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

14 “(i) a person who is located inside the
15 United States; or

16 “(ii) a person—

17 “(I) who is located outside the
18 United States or whose location can-
19 not be determined; and

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

24 “(C) the term ‘covered record’ means a
25 record or other information that—

1 “(i) pertains to a covered person; and

2 “(ii) is—

3 “(I) a record or other informa-
4 tion described in the matter preceding
5 paragraph (1) of subsection (c);

6 “(II) the contents of a commu-
7 nication; or

8 “(III) location information;

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

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

14 “(i) was obtained—

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

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

23 “(bb) is inconsistent with
24 the privacy policy of the provider;

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

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

7 “(ii) was—

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

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

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

20 “(G) the term ‘location information’ means
21 information derived or otherwise calculated
22 from the transmission or reception of a radio
23 signal that reveals the approximate or actual
24 geographic location of a customer, subscriber,
25 or device;

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

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

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

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

16 “(ii) information—

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

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

23 “(K) the term ‘third party’ means a person
24 who—

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

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

5 “(I) a provider of an electronic
6 communication service to the public;
7 or

8 “(II) a provider of a remote com-
9 puting service.

10 “(2) LIMITATION.—

11 “(A) IN GENERAL.—A law enforcement
12 agency of a governmental entity and an element
13 of the intelligence community may not obtain
14 from a third party in exchange for anything of
15 value a covered customer or subscriber record
16 or any illegitimately obtained information.

17 “(B) INDIRECTLY ACQUIRED RECORDS
18 AND INFORMATION.—The limitation under sub-
19 paragraph (A) shall apply without regard to
20 whether the third party possessing the covered
21 customer or subscriber record or illegitimately
22 obtained information is the third party that ini-
23 tially obtained or collected, or is the third party
24 that initially received the disclosure of, the cov-

1 ered customer or subscriber record or illegit-
2 imately obtained information.

3 “(3) LIMIT ON SHARING BETWEEN AGEN-
4 CIES.—An agency of a governmental entity that is
5 not a law enforcement agency or an element of the
6 intelligence community may not provide to a law en-
7 forcement agency of a governmental entity or an ele-
8 ment of the intelligence community a covered cus-
9 tomer or subscriber record or illegitimately obtained
10 information that was obtained from a third party in
11 exchange for anything of value.

12 “(4) PROHIBITION ON USE AS EVIDENCE.—A
13 covered customer or subscriber record or illegit-
14 imately obtained information obtained by or pro-
15 vided to a law enforcement agency of a governmental
16 entity or an element of the intelligence community in
17 violation of paragraph (2) or (3), and any evidence
18 derived therefrom, may not be received in evidence
19 in any trial, hearing, or other proceeding in or be-
20 fore any court, grand jury, department, officer,
21 agency, regulatory body, legislative committee, or
22 other authority of the United States, a State, or a
23 political subdivision thereof.

24 “(5) MINIMIZATION PROCEDURES.—

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

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

18 **SEC. 3. REQUIRED DISCLOSURE.**

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

21 “(i) COVERED CUSTOMER OR SUBSCRIBER RECORDS
22 AND ILLEGITIMATELY OBTAINED INFORMATION.—

23 “(1) DEFINITIONS.—In this subsection, the
24 terms ‘covered customer or subscriber record’, ‘ille-
25 gitimately obtained information’, and ‘third party’

1 have the meanings given such terms in section
2 2702(e).

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

15 “(3) ORDERS.—

16 “(A) IN GENERAL.—A court may only
17 issue an order requiring a third party to dis-
18 close a covered customer or subscriber record or
19 any illegitimately obtained information on the
20 same basis and subject to the same limitations
21 as would apply to a court order to require dis-
22 closure by a provider of remote computing serv-
23 ice or a provider of electronic communication
24 service to the public of a record of a customer
25 or subscriber of the provider.

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

11 **SEC. 4. INTERMEDIARY SERVICE PROVIDERS.**

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

14 (1) in paragraph (3), by striking “and” at the
15 end;

16 (2) in paragraph (4), by striking the period at
17 the end and inserting “; and”; and

18 (3) by adding at the end the following:

19 “(5) the term ‘intermediary service provider’
20 means an entity or facilities owner or operator that
21 directly or indirectly delivers, stores, or processes
22 communications for or on behalf of a provider of
23 electronic communication service to the public or a
24 provider of remote computing service.”.

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

3 (1) in paragraph (1), by striking “and” at the
4 end;

5 (2) in paragraph (2), by striking “and” at the
6 end;

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

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

10 “(4) an intermediary service provider shall not
11 knowingly divulge—

12 “(A) to any person or entity the contents
13 of a communication while in electronic storage
14 by that provider; or

15 “(B) to any governmental entity a record
16 or other information pertaining to a subscriber
17 to or customer of, a recipient of a communica-
18 tion from a subscriber to or customer of, or the
19 sender of a communication to a subscriber to or
20 customer of, the provider of electronic commu-
21 nication service to the public or the provider of
22 remote computing service for, or on behalf of,
23 which the intermediary service provider directly
24 or indirectly delivers, transmits, stores, or proc-
25 esses communications.”.

1 **SEC. 5. LIMITS ON SURVEILLANCE CONDUCTED FOR FOR-**
2 **EIGN INTELLIGENCE PURPOSES OTHER**
3 **THAN UNDER THE FOREIGN INTELLIGENCE**
4 **SURVEILLANCE ACT OF 1978.**

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

7 “(f)(i)(A) Nothing contained in this chapter, chapter
8 121 or 206 of this title, or section 705 of the Communica-
9 tions Act of 1934 (47 U.S.C. 151 et seq.) shall be deemed
10 to affect an acquisition or activity described in clause (B)
11 that is carried out utilizing a means other than electronic
12 surveillance, as defined in section 101 of the Foreign In-
13 telligence Surveillance Act of 1978 (50 U.S.C. 1801).

14 “(B) An acquisition or activity described in this
15 clause is—

16 “(I) an acquisition by the United States Gov-
17 ernment of foreign intelligence information from
18 international or foreign communications that—

19 “(aa) is acquired pursuant to express stat-
20 utory authority; or

21 “(bb) only includes information of persons
22 who are not United States persons and are lo-
23 cated outside the United States; or

24 “(II) a foreign intelligence activity involving a
25 foreign electronic communications system that—

1 “(aa) is conducted pursuant to express
2 statutory authority; or

3 “(bb) only involves the acquisition by the
4 United States Government of information of
5 persons who are not United States persons and
6 are located outside the United States.

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

13 (b) EXCLUSIVE MEANS RELATED TO COMMUNICA-
14 TIONS RECORDS.—The Foreign Intelligence Surveillance
15 Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive
16 means by which electronic communications transactions
17 records, call detail records, or other information from com-
18 munications of United States persons or persons inside the
19 United States are acquired for foreign intelligence pur-
20 poses inside the United States or from a person or entity
21 located in the United States that provides telecommuni-
22 cations, electronic communication, or remote computing
23 services.

1 (c) EXCLUSIVE MEANS RELATED TO LOCATION IN-
2 FORMATION, WEB BROWSING HISTORY, AND INTERNET
3 SEARCH HISTORY.—

4 (1) DEFINITION.—In this subsection, the term
5 “location information” has the meaning given that
6 term in subsection (e) of section 2702 of title 18,
7 United States Code, as added by section 2 of this
8 Act.

9 (2) EXCLUSIVE MEANS.—Title I and sections
10 303, 304, 703, 704, and 705 of the Foreign Intel-
11 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et
12 seq., 1823, 1824, 1881b, 1881c, 1881d) shall be the
13 exclusive means by which location information, web
14 browsing history, and internet search history of
15 United States persons or persons inside the United
16 States are acquired for foreign intelligence purposes
17 inside the United States or from a person or entity
18 located in the United States.

19 (d) EXCLUSIVE MEANS RELATED TO FOURTH
20 AMENDMENT-PROTECTED INFORMATION.—Title I and
21 sections 303, 304, 703, 704, and 705 of the Foreign Intel-
22 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.,
23 1823, 1824, 1881b, 1881c, 1881d) shall be the exclusive
24 means by which any information, records, data, or tangible
25 things are acquired for foreign intelligence purposes from

1 a person or entity located in the United States if the com-
2 pelled production of such information, records, data, or
3 tangible things would require a warrant for law enforce-
4 ment purposes.

5 (e) DEFINITION.—In this section, the term “United
6 States person” has the meaning given that term in section
7 101 of the Foreign Intelligence Surveillance Act of 1978
8 (50 U.S.C. 1801).

9 **SEC. 6. LIMIT ON CIVIL IMMUNITY FOR PROVIDING INFOR-**
10 **MATION, FACILITIES, OR TECHNICAL ASSIST-**
11 **ANCE TO THE GOVERNMENT ABSENT A**
12 **COURT ORDER.**

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

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

17 “(B) a certification in writing—

18 “(I) by a person specified in section
19 2518(7) or the Attorney General of the United
20 States;

21 “(II) that the requirements for an emer-
22 gency authorization to intercept a wire, oral, or
23 electronic communication under section 2518(7)
24 have been met; and

1 “(III) that the specified assistance is re-
2 quired,”; and

3 (2) by striking subparagraph (iii) and inserting
4 the following:

5 “(iii) For assistance provided pursuant to a certifi-
6 cation under subparagraph (ii)(B), the limitation on
7 causes of action under the last sentence of the matter fol-
8 lowing subparagraph (ii)(B) shall only apply to the extent
9 that the assistance ceased at the earliest of the time the
10 application for a court order was denied, the time the com-
11 munication sought was obtained, or 48 hours after the
12 interception began.”.

