

116TH CONGRESS
1ST SESSION

S. _____

To ensure the digital contents of electronic equipment and online accounts belonging to or in the possession of United States persons entering or exiting the United States are adequately protected at the border, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN (for himself, Mr. PAUL, Mr. MARKEY, and Mr. MERKLEY) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To ensure the digital contents of electronic equipment and online accounts belonging to or in the possession of United States persons entering or exiting the United States are adequately protected at the border, 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 Data at
5 the Border Act”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

1 (1) United States persons have a reasonable ex-
2 pectation of privacy in the digital contents of their
3 electronic equipment, the digital contents of their
4 online accounts, and the nature of their online pres-
5 ence.

6 (2) The Supreme Court of the United States
7 recognized in *Riley v. California*, 134 S. Ct. 2473
8 (2014) the extraordinary privacy interests in elec-
9 tronic equipment like cell phones.

10 (3) The privacy interest of United States per-
11 sons in the digital contents of their electronic equip-
12 ment, the digital contents of their online accounts,
13 and the nature of their online presence differs in
14 both degree and kind from their privacy interest in
15 closed containers.

16 (4) Accessing the digital contents of electronic
17 equipment, accessing the digital contents of an on-
18 line account, or obtaining information regarding the
19 nature of the online presence of a United States per-
20 son entering or exiting the United States, without a
21 lawful warrant based on probable cause, is unreason-
22 able under the Fourth Amendment to the Constitu-
23 tion of the United States.

24 **SEC. 3. DEFINITIONS.**

25 As used in this Act—

1 (1) the term “access credential” includes a
2 username, password, PIN number, fingerprint, or bi-
3 ometric indicator;

4 (2) the term “border” means the international
5 border of the United States and the functional
6 equivalent of such border;

7 (3) the term “digital contents” means any
8 signs, signals, writing, images, sounds, data, or in-
9 telligence of any nature transmitted in whole or in
10 part by electronic equipment, or stored in electronic
11 equipment or an online account;

12 (4) the term “electronic communication service”
13 has the meaning given that term in section 2510 of
14 title 18, United States Code;

15 (5) the term “electronic equipment” has the
16 meaning given the term “computer” in section
17 1030(e) of title 18, United States Code;

18 (6) the term “Governmental entity” means a
19 department or agency of the United States (includ-
20 ing any officer, employee, or contractor or other
21 agent thereof);

22 (7) the term “online account” means an online
23 account with an electronic communication service or
24 remote computing service;

1 (8) the term “online account information”
2 means the screen name or other identifier or infor-
3 mation that would allow a Governmental entity to
4 identify the online presence of an individual;

5 (9) the term “remote computing service” has
6 the meaning given that term in section 2711 of title
7 18, United States Code; and

8 (10) the term “United States person” means an
9 individual who is a United States person, as defined
10 in section 101 of the Foreign Intelligence Surveil-
11 lance Act of 1978 (50 U.S.C. 1801).

12 **SEC. 4. PROCEDURES FOR LAWFUL ACCESS TO DIGITAL**
13 **DATA AT THE BORDER.**

14 (a) STANDARD.—Subject to subsection (b), a Govern-
15 mental entity may not—

16 (1) access the digital contents of any electronic
17 equipment belonging to or in the possession of a
18 United States person at the border without a valid
19 warrant supported by probable cause issued using
20 the procedures described in the Federal Rules of
21 Criminal Procedure by a court of competent jurisdic-
22 tion;

23 (2) deny entry into or exit from the United
24 States by a United States person based on a refusal
25 by the United States person to—

1 (A) disclose an access credential that
2 would enable access to the digital contents of
3 electronic equipment or the digital contents of
4 an online account;

5 (B) provide access to the digital contents
6 of electronic equipment or the digital contents
7 of an online account; or

8 (C) provide online account information; or

9 (3) delay entry into or exit from the United
10 States by a United States person for longer than the
11 period of time, which may not exceed 4 hours, nec-
12 essary to determine whether the United States per-
13 son will, in a manner in accordance with subsection
14 (c), consensually provide an access credential, ac-
15 cess, or online account information, as described in
16 subparagraphs (A), (B), and (C) of paragraph (2).

17 (b) EMERGENCY EXCEPTIONS.—

18 (1) EMERGENCY SITUATIONS GENERALLY.—

19 (A) IN GENERAL.—An investigative or law
20 enforcement officer of a Governmental entity
21 who is designated by the Secretary of Home-
22 land Security for purposes of this paragraph
23 may access the digital contents of electronic
24 equipment belonging to or in possession of a
25 United States person at the border without a

1 warrant described in subsection (a)(1) if the in-
2 vestigative or law enforcement officer—

3 (i) reasonably determines that—

4 (I) an emergency situation exists
5 that involves—

6 (aa) immediate danger of
7 death or serious physical injury
8 to any person;

9 (bb) conspiratorial activities
10 threatening the national security
11 interest of the United States; or

12 (cc) conspiratorial activities
13 characteristic of organized crime;

14 (II) the emergency situation de-
15 scribed in subclause (I) requires ac-
16 cess to the digital contents of the elec-
17 tronic equipment before a warrant de-
18 scribed in subsection (a)(1) author-
19 izing such access can, with due dili-
20 gence, be obtained; and

21 (III) there are grounds upon
22 which a warrant described in sub-
23 section (a)(1) could be issued author-
24 izing such access; and

1 (ii) makes an application in accord-
2 ance with this section for a warrant de-
3 scribed in subsection (a)(1) as soon as
4 practicable, but not later than 7 days after
5 the investigative or law enforcement officer
6 accesses the digital contents under the au-
7 thority under this subparagraph.

8 (B) WARRANT NOT OBTAINED.—If an ap-
9 plication for a warrant described in subpara-
10 graph (A)(ii) is denied, or in any other case in
11 which an investigative or law enforcement offi-
12 cer accesses the digital contents of electronic
13 equipment belonging to or in possession of a
14 United States person at the border without a
15 warrant under the emergency authority under
16 subparagraph (A) and a warrant authorizing
17 the access is not obtained—

18 (i) any copy of the digital contents in
19 the custody or control of a Governmental
20 entity shall immediately be destroyed;

21 (ii) the digital contents, and any in-
22 formation derived from the digital con-
23 tents, may not be disclosed to any Govern-
24 mental entity or a State or local govern-
25 ment; and

1 (iii) the Governmental entity employ-
2 ing the investigative or law enforcement of-
3 ficer that accessed the digital contents
4 shall notify the United States person that
5 any copy of the digital contents has been
6 destroyed.

7 (2) PROTECTION OF PUBLIC SAFETY AND
8 HEALTH.—A Governmental entity may access the
9 digital contents of electronic equipment belonging to
10 or in possession of a United States person at the
11 border without a warrant described in subsection
12 (a)(1) if the access is—

13 (A) necessary for the provision of fire,
14 medical, public safety, or other emergency serv-
15 ices; and

16 (B) unrelated to the investigation of a pos-
17 sible crime or other violation of the law.

18 (c) INFORMED CONSENT IN WRITING.—

19 (1) NOTICE.—

20 (A) IN GENERAL.—A Governmental entity
21 shall provide the notice described in subpara-
22 graph (B) before requesting that a United
23 States person at the border—

24 (i) provide consent to access the dig-
25 ital contents of any electronic equipment

1 belonging to or in the possession of or the
2 digital contents of an online account of the
3 United States person;

4 (ii) disclose an access credential that
5 would enable access to the digital contents
6 of electronic equipment or the digital con-
7 tents of an online account of the United
8 States person;

9 (iii) provide access to the digital con-
10 tents of electronic equipment or the digital
11 contents of an online account of the United
12 States person; or

13 (iv) provide online account informa-
14 tion of the United States person.

15 (B) CONTENTS.—The notice described in
16 this subparagraph is written notice in a lan-
17 guage understood by the United States person
18 that the Governmental entity—

19 (i) may not—

20 (I) compel access to the digital
21 contents of electronic equipment be-
22 longing to or in the possession of, the
23 digital contents of an online account
24 of, or the online account information

1 of a United States person without a
2 valid warrant;

3 (II) deny entry into or exit from
4 the United States by the United
5 States person based on a refusal by
6 the United States person to—

7 (aa) disclose an access cre-
8 dential that would enable access
9 to the digital contents of elec-
10 tronic equipment or the digital
11 contents of an online account;

12 (bb) provide access to the
13 digital contents of electronic
14 equipment or the digital contents
15 of an online account; or

16 (cc) provide online account
17 information; or

18 (III) delay entry into or exit from
19 the United States by the United
20 States person for longer than the pe-
21 riod of time, which may not exceed 4
22 hours, necessary to determine whether
23 the United States person will consen-
24 sually provide an access credential, ac-
25 cess, or online account information, as

1 described in items (aa), (bb), and (cc)
2 of subclause (II); and

3 (ii) if the Governmental entity has
4 probable cause that the electronic equip-
5 ment contains information that is relevant
6 to an allegation that the United States
7 person has committed a felony, may seize
8 electronic equipment belonging to or in the
9 possession of the United States person for
10 a period of time if the United States per-
11 son refuses to consensually provide access
12 to the digital contents of the electronic
13 equipment.

14 (2) CONSENT.—

15 (A) IN GENERAL.—A Governmental entity
16 shall obtain written consent described in sub-
17 paragraph (B) before—

18 (i) accessing, pursuant to the consent
19 of a United States person at the border
20 the digital contents of electronic equipment
21 belonging to or in the possession of or the
22 digital contents of an online account of the
23 United States person;

24 (ii) obtaining, pursuant to the consent
25 of a United States person at the border, an

1 access credential of the United States per-
2 son that would enable access to the digital
3 contents of electronic equipment or the
4 digital contents of an online account; or

5 (iii) obtaining, pursuant to the con-
6 sent of a United States person at the bor-
7 der, online account information for an on-
8 line account of the United States person.

9 (B) CONTENTS OF WRITTEN CONSENT.—

10 Written consent described in this subparagraph
11 is written consent that—

12 (i) indicates the United States person
13 understands the protections and limitations
14 described in paragraph (1)(B);

15 (ii) states the United States person
16 is—

17 (I) providing consent to the Gov-
18 ernmental entity to access certain dig-
19 ital contents or consensually disclosing
20 an access credential; or

21 (II) consensually providing online
22 account information; and

23 (iii) specifies the digital contents, ac-
24 cess credential, or online account informa-

1 tion with respect to which the United
2 States person is providing consent.

3 (d) RETENTION OF DIGITAL CONTENTS.—

4 (1) LAWFUL ACCESS.—A Governmental entity
5 that obtains access to the digital contents of elec-
6 tronic equipment, the digital contents of an online
7 account, or online account information in accordance
8 with this section may not make or retain a copy of
9 the digital contents or online account information, or
10 any information directly or indirectly derived from
11 the digital contents or online account information,
12 unless there is probable cause to believe the digital
13 contents or online account information contains evi-
14 dence of, or constitutes the fruits of, a crime.

15 (2) UNLAWFUL ACCESS.—If a Governmental
16 entity obtains access to the digital contents of elec-
17 tronic equipment, digital contents of an online ac-
18 count, or online account information in a manner
19 that is not in accordance with this section, the Gov-
20 ernmental entity—

21 (A) shall immediately destroy any copy of
22 the digital contents or online account informa-
23 tion, and any information directly or indirectly
24 derived from the digital contents or online ac-

1 count information, in the custody or control of
2 the Governmental entity;

3 (B) may not disclose the digital contents
4 or online account information, or any informa-
5 tion directly or indirectly derived from the dig-
6 ital contents or online account information, to
7 any other Governmental entity or a State or
8 local government; and

9 (C) shall notify the United States person
10 that any copy of the digital contents or online
11 account information, and any information di-
12 rectly or indirectly derived from the digital con-
13 tents or online account information, has been
14 destroyed.

15 (e) RECORDKEEPING.—A Governmental entity shall
16 keep a record of each instance in which the Governmental
17 entity obtains access to the digital contents of electronic
18 equipment belonging to or in the possession of an indi-
19 vidual at the border, the digital contents of an online ac-
20 count of an individual who is at the border, or online ac-
21 count information of an individual who is at the border,
22 which shall include—

23 (1) the reason for the access;

24 (2) the nationality, immigration status, and ad-
25 mission category of the individual;

1 (3) the nature and extent of the access;

2 (4) if the access was consensual, how and to
3 what the individual consented, and what the indi-
4 vidual provided by consent;

5 (5) whether electronic equipment of the indi-
6 vidual was seized;

7 (6) whether the Governmental entity made a
8 copy of all or a portion of the digital contents or on-
9 line account information, or any information directly
10 or indirectly derived from the digital contents or on-
11 line account information; and

12 (7) whether the digital contents or online ac-
13 count information, or any information directly or in-
14 directly derived from the digital contents or online
15 account information, was shared with another Gov-
16 ernmental entity or a State or local government.

17 **SEC. 5. LIMITS ON USE OF DIGITAL CONTENTS AS EVI-**
18 **DENCE.**

19 (a) IN GENERAL.—Whenever any digital contents or
20 online account information have been obtained in violation
21 of this Act, no part of the digital contents or online ac-
22 count information and no evidence derived therefrom may
23 be received in evidence in any trial, hearing, or other pro-
24 ceeding (including any proceeding relating to the immigra-
25 tion laws, as defined in section 101(a) of the Immigration

1 and Nationality Act (8 U.S.C. 1101(a)) in or before any
2 court, grand jury, department, officer, agency, regulatory
3 body, legislative committee, or other authority of the
4 United States, a State, or a political subdivision thereof.

5 (b) APPLICATION.—To the maximum extent prac-
6 ticable, the limitations under subsection (a) shall be ap-
7 plied in the same manner as the limitations under section
8 2515 of title 18, United States Code.

9 **SEC. 6. LIMITS ON SEIZURE OF ELECTRONIC EQUIPMENT.**

10 A Governmental entity may not seize any electronic
11 equipment belonging to or in the possession of a United
12 States person at the border unless there is probable cause
13 to believe that the electronic equipment contains informa-
14 tion that is relevant to an allegation that the United
15 States person has committed a felony.

16 **SEC. 7. AUDIT AND REPORTING REQUIREMENTS.**

17 In March of each year, the Secretary of Homeland
18 Security shall submit to Congress and make publicly avail-
19 able on the Web site of the Department of Homeland Se-
20 curity a report that includes the following:

21 (1) The number of times during the previous
22 year that an officer or employee of the Department
23 of Homeland Security did each of the following:

24 (A) Accessed the digital contents of any
25 electronic equipment belonging to or in the pos-

1 session of or the digital contents of an online
2 account of a United States person at the border
3 pursuant to a warrant supported by probable
4 cause issued using the procedures described in
5 the Federal Rules of Criminal Procedure by a
6 court of competent jurisdiction.

7 (B) Accessed the digital contents of any
8 electronic equipment belonging to or in the pos-
9 session of a United States person at the border
10 pursuant to the emergency authority under sec-
11 tion 5(b).

12 (C) Requested consent to access the digital
13 contents of any electronic equipment belonging
14 to or in the possession of, the digital contents
15 of an online account of, or online account infor-
16 mation of a United States person at the border.

17 (D) Accessed the digital contents of any
18 electronic equipment belonging to or in the pos-
19 session of, the digital contents of an online ac-
20 count of, or online account information of a
21 United States person at the border pursuant to
22 written consent provided in accordance with
23 section 5(c).

24 (E) Requested a United States person at
25 the border consensually disclose an access cre-

1 dential that would enable access to the digital
2 contents of electronic equipment or the digital
3 contents of an online account of the United
4 States person.

5 (F) Accessed the digital contents of elec-
6 tronic equipment or the digital contents of an
7 online account of a United States person at the
8 border using an access credential pursuant to
9 written consent provided in accordance with
10 section 5(c).

11 (G) Accessed the digital contents of any
12 electronic equipment belonging to or in the pos-
13 session of, the digital contents of an online ac-
14 count of, or online account information of a
15 United States person at the border in a manner
16 that was not in accordance with section 5.

17 (H) Accessed the digital contents of any
18 electronic equipment belonging to or in the pos-
19 session of, the digital contents of an online ac-
20 count of, or online account information of an
21 individual who is not a United States person at
22 the border.

23 (I) Accessed the digital contents of any
24 electronic equipment belonging to or in the pos-
25 session of an individual at the border, the dig-

1 ital contents of an online account of an indi-
2 vidual at the border, or online account informa-
3 tion of an individual at the border (regardless
4 of whether the individual is a United States
5 person) at the request of a Governmental entity
6 (including another component of the Depart-
7 ment of Homeland Security) that is not the
8 Governmental entity employing the individual
9 accessing the digital contents or online account
10 information.

11 (2) Aggregate data on—

12 (A) the number of United States persons
13 for which a Governmental entity obtains access
14 to—

15 (i) the digital contents of electronic
16 equipment belonging to or in the posses-
17 sion of the United States person at the
18 border;

19 (ii) the digital contents of an online
20 account of the United States person while
21 at the border; or

22 (iii) online account information of the
23 United States person while at the border;

24 (B) the country from which United States
25 persons departed most recently before arriving

1 in the United States for the United States per-
2 sons for which a Governmental entity obtains
3 access to—

4 (i) the digital contents of electronic
5 equipment belonging to or in the posses-
6 sion of the United States person at the
7 border;

8 (ii) the digital contents of an online
9 account of the United States person while
10 at the border; or

11 (iii) online account information of the
12 United States person while at the border;

13 (C) the number and nationality of individ-
14 uals who are not United States persons for
15 which a Governmental entity obtains access
16 to—

17 (i) the digital contents of electronic
18 equipment belonging to or in the posses-
19 sion of the individuals at the border;

20 (ii) the digital contents of an online
21 account of the individuals while at the bor-
22 der; or

23 (iii) online account information of the
24 individuals while at the border; and

1 (D) the country from which individuals
2 who are not United States persons departed
3 most recently before arriving in the United
4 States for the individuals for which a Govern-
5 mental entity obtains access to—

6 (i) the digital contents of electronic
7 equipment belonging to or in the posses-
8 sion of the individuals at the border;

9 (ii) the digital contents of an online
10 account of the individuals while at the bor-
11 der; or

12 (iii) online account information of the
13 individuals while at the border.

14 (3) Aggregate data regarding the perceived race
15 and ethnicity of individuals for whom a Govern-
16 mental entity obtains access to—

17 (A) the digital contents of electronic equip-
18 ment belonging to or in the possession of the
19 individuals at the border;

20 (B) the digital contents of an online ac-
21 count of the individuals while at the border; or

22 (C) online account information of the indi-
23 viduals while at the border.

24 **SEC. 8. SAVINGS PROVISIONS.**

25 Nothing in this Act shall be construed to—

1 (1) prohibit a Governmental entity from con-
2 ducting an inspection of the external physical com-
3 ponents of the electronic equipment to determine the
4 presence or absence of weapons or contraband with-
5 out a warrant, including activating or attempting to
6 activate an object that appears to be electronic
7 equipment to verify that the object is electronic
8 equipment; or

9 (2) limit the authority of a Governmental entity
10 under the Foreign Intelligence Surveillance Act of
11 1978 (50 U.S.C. 1801 et seq.).