

115TH CONGRESS
1ST SESSION

S. 823

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

APRIL 4, 2017

Mr. WYDEN (for himself and Mr. PAUL) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

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. SCOPE.**

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.).

12 **SEC. 4. DEFINITIONS.**

13 As used in this Act—

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

17 (2) the term “border” means the international
18 border of the United States and the functional
19 equivalent of such border;

20 (3) the term “digital contents” means any
21 signs, signals, writing, images, sounds, data, or in-
22 telligence of any nature transmitted in whole or in
23 part by electronic equipment, or stored in electronic
24 equipment or an online account;

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

4 (5) the term “electronic equipment” has the
5 meaning given the term “computer” in section
6 1030(e) of title 18, United States Code;

7 (6) the term “Governmental entity” means a
8 department or agency of the United States (includ-
9 ing any officer, employee, or contractor or other
10 agent thereof);

11 (7) the term “online account” means an online
12 account with an electronic communication service or
13 remote computing service;

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

18 (9) the term “remote computing service” has
19 the meaning given that term in section 2711 of title
20 18, United States Code; and

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

1 **SEC. 5. PROCEDURES FOR LAWFUL ACCESS TO DIGITAL**
2 **DATA AT THE BORDER.**

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

5 (1) access the digital contents of any electronic
6 equipment belonging to or in the possession of a
7 United States person at the border without a valid
8 warrant supported by probable cause issued using
9 the procedures described in the Federal Rules of
10 Criminal Procedure by a court of competent jurisdic-
11 tion;

12 (2) deny entry into or exit from the United
13 States by a United States person based on a refusal
14 by the United States person to—

15 (A) disclose an access credential that
16 would enable access to the digital contents of
17 electronic equipment or the digital contents of
18 an online account;

19 (B) provide access to the digital contents
20 of electronic equipment or the digital contents
21 of an online account; or

22 (C) provide online account information; or

23 (3) delay entry into or exit from the United
24 States by a United States person for longer than the
25 period of time, which may not exceed 4 hours, nec-
26 essary to determine whether the United States per-

1 son will, in a manner in accordance with subsection
2 (c), consensually provide an access credential, ac-
3 cess, or online account information, as described in
4 subparagraphs (A), (B), and (C) of paragraph (2).

5 (b) EMERGENCY EXCEPTIONS.—

6 (1) EMERGENCY SITUATIONS GENERALLY.—

7 (A) IN GENERAL.—An investigative or law
8 enforcement officer of a Governmental entity
9 who is designated by the Secretary of Home-
10 land Security for purposes of this paragraph
11 may access the digital contents of electronic
12 equipment belonging to or in possession of a
13 United States person at the border without a
14 warrant described in subsection (a)(1) if the in-
15 vestigative or law enforcement officer—

16 (i) reasonably determines that—

17 (I) an emergency situation exists
18 that involves—

19 (aa) immediate danger of
20 death or serious physical injury
21 to any person;

22 (bb) conspiratorial activities
23 threatening the national security
24 interest of the United States; or

1 (cc) conspiratorial activities
2 characteristic of organized crime;

3 (II) the emergency situation de-
4 scribed in subclause (I) requires ac-
5 cess to the digital contents of the elec-
6 tronic equipment before a warrant de-
7 scribed in subsection (a)(1) author-
8 izing such access can, with due dili-
9 gence, be obtained; and

10 (III) there are grounds upon
11 which a warrant described in sub-
12 section (a)(1) could be issued author-
13 izing such access; and

14 (ii) makes an application in accord-
15 ance with this section for a warrant de-
16 scribed in subsection (a)(1) as soon as
17 practicable, but not later than 7 days after
18 the investigative or law enforcement officer
19 accesses the digital contents under the au-
20 thority under this subparagraph.

21 (B) WARRANT NOT OBTAINED.—If an ap-
22 plication for a warrant described in subpara-
23 graph (A)(ii) is denied, or in any other case in
24 which an investigative or law enforcement offi-
25 cer accesses the digital contents of electronic

1 equipment belonging to or in possession of a
2 United States person at the border without a
3 warrant under the emergency authority under
4 subparagraph (A) and a warrant authorizing
5 the access is not obtained—

6 (i) any copy of the digital contents in
7 the custody or control of a Governmental
8 entity shall immediately be destroyed;

9 (ii) the digital contents, and any in-
10 formation derived from the digital con-
11 tents, may not be disclosed to any Govern-
12 mental entity or a State or local govern-
13 ment; and

14 (iii) the Governmental entity employ-
15 ing the investigative or law enforcement of-
16 ficer that accessed the digital contents
17 shall notify the United States person that
18 any copy of the digital contents has been
19 destroyed.

20 (2) PROTECTION OF PUBLIC SAFETY AND
21 HEALTH.—A Governmental entity may access the
22 digital contents of electronic equipment belonging to
23 or in possession of a United States person at the
24 border without a warrant described in subsection
25 (a)(1) if the access is—

1 (A) necessary for the provision of fire,
2 medical, public safety, or other emergency serv-
3 ices; and

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

6 (c) INFORMED CONSENT IN WRITING.—

7 (1) NOTICE.—

8 (A) IN GENERAL.—A Governmental entity
9 shall provide the notice described in subpara-
10 graph (B) before requesting that a United
11 States person at the border—

12 (i) provide consent to access the dig-
13 ital contents of any electronic equipment
14 belonging to or in the possession of or the
15 digital contents of an online account of the
16 United States person;

17 (ii) disclose an access credential that
18 would enable access to the digital contents
19 of electronic equipment or the digital con-
20 tents of an online account of the United
21 States person;

22 (iii) provide access to the digital con-
23 tents of electronic equipment or the digital
24 contents of an online account of the United
25 States person; or

1 (iv) provide online account informa-
2 tion of the United States person.

3 (B) CONTENTS.—The notice described in
4 this subparagraph is written notice in a lan-
5 guage understood by the United States person
6 that the Governmental entity—

7 (i) may not—

8 (I) compel access to the digital
9 contents of electronic equipment be-
10 longing to or in the possession of, the
11 digital contents of an online account
12 of, or the online account information
13 of a United States person without a
14 valid warrant;

15 (II) deny entry into or exit from
16 the United States by the United
17 States person based on a refusal by
18 the United States person to—

19 (aa) disclose an access cre-
20 dential that would enable access
21 to the digital contents of elec-
22 tronic equipment or the digital
23 contents of an online account;

24 (bb) provide access to the
25 digital contents of electronic

1 equipment or the digital contents
2 of an online account; or
3 (cc) provide online account
4 information; or
5 (III) delay entry into or exit from
6 the United States by the United
7 States person for longer than the pe-
8 riod of time, which may not exceed 4
9 hours, necessary to determine whether
10 the United States person will consen-
11 sually provide an access credential, ac-
12 cess, or online account information, as
13 described in items (aa), (bb), and (cc)
14 of subclause (II); and
15 (ii) if the Governmental entity has
16 probable cause that the electronic equip-
17 ment contains information that is relevant
18 to an allegation that the United States
19 person has committed a felony, may seize
20 electronic equipment belonging to or in the
21 possession of the United States person for
22 a period of time if the United States per-
23 son refuses to consensually provide access
24 to the digital contents of the electronic
25 equipment.

1 (2) CONSENT.—

2 (A) IN GENERAL.—A Governmental entity
3 shall obtain written consent described in sub-
4 paragraph (B) before—

5 (i) accessing, pursuant to the consent
6 of a United States person at the border
7 the digital contents of electronic equipment
8 belonging to or in the possession of or the
9 digital contents of an online account of the
10 United States person;

11 (ii) obtaining, pursuant to the consent
12 of a United States person at the border, an
13 access credential of the United States per-
14 son that would enable access to the digital
15 contents of electronic equipment or the
16 digital contents of an online account; or

17 (iii) obtaining, pursuant to the con-
18 sent of a United States person at the bor-
19 der, online account information for an on-
20 line account of the United States person.

21 (B) CONTENTS OF WRITTEN CONSENT.—

22 Written consent described in this subparagraph
23 is written consent that—

1 (i) indicates the United States person
2 understands the protections and limitations
3 described in paragraph (1)(B);

4 (ii) states the United States person
5 is—

6 (I) providing consent to the Gov-
7 ernmental entity to access certain dig-
8 ital contents or consensually disclosing
9 an access credential; or

10 (II) consensually providing online
11 account information; and

12 (iii) specifies the digital contents, ac-
13 cess credential, or online account informa-
14 tion with respect to which the United
15 States person is providing consent.

16 (d) RETENTION OF DIGITAL CONTENTS.—

17 (1) LAWFUL ACCESS.—A Governmental entity
18 that obtains access to the digital contents of elec-
19 tronic equipment, the digital contents of an online
20 account, or online account information in accordance
21 with this section may not make or retain a copy of
22 the digital contents or online account information, or
23 any information directly or indirectly derived from
24 the digital contents or online account information,
25 unless there is probable cause to believe the digital

1 contents or online account information contains evi-
2 dence of, or constitutes the fruits of, a crime.

3 (2) UNLAWFUL ACCESS.—If a Governmental
4 entity obtains access to the digital contents of elec-
5 tronic equipment, digital contents of an online ac-
6 count, or online account information in a manner
7 that is not in accordance with this section, the Gov-
8 ernmental entity—

9 (A) shall immediately destroy any copy of
10 the digital contents or online account informa-
11 tion, and any information directly or indirectly
12 derived from the digital contents or online ac-
13 count information, in the custody or control of
14 the Governmental entity;

15 (B) may not disclose the digital contents
16 or online account information, or any informa-
17 tion directly or indirectly derived from the dig-
18 ital contents or online account information, to
19 any other Governmental entity or a State or
20 local government; and

21 (C) shall notify the United States person
22 that any copy of the digital contents or online
23 account information, and any information di-
24 rectly or indirectly derived from the digital con-

1 tents or online account information, has been
2 destroyed.

3 (e) RECORDKEEPING.—A Governmental entity shall
4 keep a record of each instance in which the Governmental
5 entity obtains access to the digital contents of electronic
6 equipment belonging to or in the possession of an indi-
7 vidual at the border, the digital contents of an online ac-
8 count of an individual who is at the border, or online ac-
9 count information of an individual who is at the border,
10 which shall include—

11 (1) the reason for the access;

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

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

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

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

20 (6) whether the Governmental entity made a
21 copy of all or a portion of the digital contents or on-
22 line account information, or any information directly
23 or indirectly derived from the digital contents or on-
24 line account information; and

1 (7) whether the digital contents or online ac-
2 count information, or any information directly or in-
3 directly derived from the digital contents or online
4 account information, was shared with another Gov-
5 ernmental entity or a State or local government.

6 **SEC. 6. LIMITS ON USE OF DIGITAL CONTENTS AS EVI-**
7 **DENCE.**

8 (a) **IN GENERAL.**—Whenever any digital contents or
9 online account information have been obtained in violation
10 of this Act, no part of the digital contents or online ac-
11 count information and no evidence derived therefrom may
12 be received in evidence in any trial, hearing, or other pro-
13 ceeding (including any proceeding relating to the immigra-
14 tion laws, as defined in section 101(a) of the Immigration
15 and Nationality Act (8 U.S.C. 1101(a))) in or before any
16 court, grand jury, department, officer, agency, regulatory
17 body, legislative committee, or other authority of the
18 United States, a State, or a political subdivision thereof.

19 (b) **APPLICATION.**—To the maximum extent prac-
20 ticable, the limitations under subsection (a) shall be ap-
21 plied in the same manner as the limitations under section
22 2515 of title 18, United States Code.

23 **SEC. 7. LIMITS ON SEIZURE OF ELECTRONIC EQUIPMENT.**

24 A Governmental entity may not seize any electronic
25 equipment belonging to or in the possession of a United

1 States person at the border unless there is probable cause
2 to believe that the electronic equipment contains informa-
3 tion that is relevant to an allegation that the United
4 States person has committed a felony.

5 **SEC. 8. AUDIT AND REPORTING REQUIREMENTS.**

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

10 (1) The number of times during the previous
11 year that an officer or employee of the Department
12 of Homeland Security did each of the following:

13 (A) Accessed the digital contents of any
14 electronic equipment belonging to or in the pos-
15 session of or the digital contents of an online
16 account of a United States person at the border
17 pursuant to a warrant supported by probable
18 cause issued using the procedures described in
19 the Federal Rules of Criminal Procedure by a
20 court of competent jurisdiction.

21 (B) Accessed the digital contents of any
22 electronic equipment belonging to or in the pos-
23 session of a United States person at the border
24 pursuant to the emergency authority under sec-
25 tion 5(b).

1 (C) Requested consent to access the digital
2 contents of any electronic equipment belonging
3 to or in the possession of, the digital contents
4 of an online account of, or online account infor-
5 mation of a United States person at the border.

6 (D) Accessed the digital contents of any
7 electronic equipment belonging to or in the pos-
8 session of, the digital contents of an online ac-
9 count of, or online account information of a
10 United States person at the border pursuant to
11 written consent provided in accordance with
12 section 5(c).

13 (E) Requested a United States person at
14 the border consensually disclose an access cre-
15 dential that would enable access to the digital
16 contents of electronic equipment or the digital
17 contents of an online account of the United
18 States person.

19 (F) Accessed the digital contents of elec-
20 tronic equipment or the digital contents of an
21 online account of a United States person at the
22 border using an access credential pursuant to
23 written consent provided in accordance with
24 section 5(c).

1 (G) Accessed the digital contents of any
2 electronic equipment belonging to or in the pos-
3 session of, the digital contents of an online ac-
4 count of, or online account information of a
5 United States person at the border in a manner
6 that was not in accordance with section 5.

7 (H) Accessed the digital contents of any
8 electronic equipment belonging to or in the pos-
9 session of, the digital contents of an online ac-
10 count of, or online account information of an
11 individual who is not a United States person at
12 the border.

13 (I) Accessed the digital contents of any
14 electronic equipment belonging to or in the pos-
15 session of an individual at the border, the dig-
16 ital contents of an online account of an indi-
17 vidual at the border, or online account informa-
18 tion of an individual at the border (regardless
19 of whether the individual is a United States
20 person) at the request of a Governmental entity
21 (including another component of the Depart-
22 ment of Homeland Security) that is not the
23 Governmental entity employing the individual
24 accessing the digital contents or online account
25 information.

1 (2) Aggregate data on—

2 (A) the number of United States persons
3 for which a Governmental entity obtains access
4 to—

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

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

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

14 (B) the country from which United States
15 persons departed most recently before arriving
16 in the United States for the United States per-
17 sons for which a Governmental entity obtains
18 access to—

19 (i) the digital contents of electronic
20 equipment belonging to or in the posses-
21 sion of the United States person at the
22 border;

23 (ii) the digital contents of an online
24 account of the United States person while
25 at the border; or

1 (iii) online account information of the
2 United States person while at the border;

3 (C) the number and nationality of individ-
4 uals who are not United States persons for
5 which a Governmental entity obtains access
6 to—

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

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

13 (iii) online account information of the
14 individuals while at the border; and

15 (D) the country from which individuals
16 who are not United States persons departed
17 most recently before arriving in the United
18 States for the individuals for which a Govern-
19 mental entity obtains access to—

20 (i) the digital contents of electronic
21 equipment belonging to or in the posses-
22 sion of the individuals at the border;

23 (ii) the digital contents of an online
24 account of the individuals while at the bor-
25 der; or

1 (iii) online account information of the
2 individuals while at the border.

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

6 (A) the digital contents of electronic equip-
7 ment belonging to or in the possession of the
8 individuals at the border;

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

11 (C) online account information of the indi-
12 viduals while at the border.

○