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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Protecting Data at the Border Act''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) United States persons have a reasonable expectation of privacy in the digital contents of their electronic equipment, the digital contents of their online accounts, and the nature of their online presence.

(2) The Supreme Court of the United States recognized in Riley v. California, 134 S. Ct. 2473 (2014) the extraordinary privacy interests in electronic equipment like cell phones.

(3) The privacy interest of United States persons in the digital contents of their electronic equipment, the digital contents of their online accounts, and the nature of their online presence differs in both degree and kind from their privacy interest in closed containers.

(4) Accessing the digital contents of electronic equipment, accessing the digital contents of an online account, or obtaining information regarding the nature of the online presence of a United States person entering or exiting the United States, without a lawful warrant based on probable cause, is unreasonable under the Fourth Amendment to the Constitution of the United States.

SEC. 3. SCOPE.

Nothing in this Act shall be construed to—

(1) prohibit a Governmental entity from conducting an inspection of the external physical components of the electronic equipment to determine the presence or absence of weapons or contraband without a warrant, including activating or attempting to activate an object that appears to be electronic equipment to verify that the object is electronic equipment; or

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

SEC. 4. DEFINITIONS.

As used in this Act—

(1) the term ''access credential'' includes a username, password, PIN number, fingerprint, or biometric indicator;

(2) the term ''border'' means the international border of the United States and the functional equivalent of such border;

(3) the term ''digital contents'' means any signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by electronic equipment, or stored in electronic equipment or an online account;

(4) the term ''electronic communication service'' has the meaning given that term in section 2510 of title 18, United States Code;

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

(6) the term ''Governmental entity'' means a department or agency of the United States (including any officer, employee, or contractor or other agent thereof);

(7) the term ''online account'' means an online account with an electronic communication service or remote computing service;

(8) the term ''online account information'' means the screen name or other identifier or information that would allow a Governmental entity to identify the online presence of an individual;

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

(10) the term ''United States person'' means an individual who is a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

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

(a) STANDARD.—Subject to subsection (b), a Governmental entity may not—

(1) access the digital contents of any electronic equipment belonging to or in the possession of a United States person at the border without a valid warrant supported by probable cause issued using the procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction;

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

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

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

(C) provide online account information; or

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

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

(b) EMERGENCY EXCEPTIONS.—

(1) EMERGENCY SITUATIONS GENERALLY.—

(A) IN GENERAL.—An investigative or law enforcement officer of a Governmental entity who is designated by the Secretary of Homeland Security for purposes of this paragraph may access the digital contents of electronic equipment belonging to or in possession of a United States person at the border without a warrant described in subsection (a)(1) if the investigative or law enforcement officer—

(i) reasonably determines that—

(I) an emergency situation exists that involves—

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

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

(cc) conspiratorial activities characteristic of organized crime;

(II) the emergency situation described in subclause (I) requires access to the digital contents of the electronic equipment before a warrant described in subsection (a)(1) authorizing such access can, with due diligence, be obtained; and

(III) there are grounds upon which a warrant described in subsection (a)(1) could be issued authorizing such access; and

(ii) makes an application in accordance with this section for a warrant described in subsection (a)(1) as soon as practicable, but not later than 7 days after the investigative or law enforcement officer accesses the digital contents under the authority under this subparagraph.

(B) WARRANT NOT OBTAINED.—If an application for a warrant described in subparagraph (A)(ii) is denied, or in any other case in which an investigative or law enforcement officer accesses the digital contents of electronic

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

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

(ii) the digital contents, and any information derived from the digital contents, may not be disclosed to any Governmental entity or a State or local government; and

(iii) the Governmental entity employing the investigative or law enforcement officer that accessed the digital contents shall notify the United States person that any copy of the digital contents has been destroyed.

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

(A) necessary for the provision of fire, medical, public safety, or other emergency services; and

(B) unrelated to the investigation of a possible crime or other violation of the law.

(c) INFORMED CONSENT IN WRITING.—

(1) NOTICE.—

(A) IN GENERAL.—A Governmental entity shall provide the notice described in subparagraph (B) before requesting that a United States person at the border—

(i) provide consent to access the digital contents of any electronic equipment belonging to or in the possession of or the digital contents of an online account of the United States person;

(ii) disclose an access credential that would enable access to the digital contents of electronic equipment or the digital contents of an online account of the United States person;

(iii) provide access to the digital contents of electronic equipment or the digital contents of an online account of the United States person; or

(iv) provide online account information of the United States person.

(B) CONTENTS.—The notice described in this subparagraph is written notice in a language understood by the United States person that the Governmental entity—

(i) may not—

(I) compel access to the digital contents of electronic equipment belonging to or in the possession of, the digital contents of an online account of, or the online account information of a United States person without a valid warrant;

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

(aa) disclose an access credential that would enable access to the digital contents of electronic equipment or the digital contents of an online account;

(bb) provide access to the digital contents of electronic

equipment or the digital contents of an online account; or

(cc) provide online account information; or

(III) delay entry into or exit from the United States by the United States person for longer than the period of time, which may not exceed 4 hours, necessary to determine whether the United States person will consensually provide an access credential, access, or online account information, as described in items (aa), (bb), and (cc) of subclause (II); and

(ii) if the Governmental entity has probable cause that the electronic equipment contains information that is relevant to an allegation that the United States person has committed a felony, may seize electronic equipment belonging to or in the possession of the United States person for a period of time if the United States person refuses to consensually provide access to the digital contents of the electronic equipment.

(2) CONSENT.—

(A) IN GENERAL.—A Governmental entity shall obtain written consent described in subparagraph (B) before—

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

(ii) obtaining, pursuant to the consent of a United States person at the border, an access credential of the United States person that would enable access to the digital contents of electronic equipment or the digital contents of an online account; or

(iii) obtaining, pursuant to the consent of a United States person at the border, online account information for an online account of the United States person.

(B) CONTENTS OF WRITTEN CONSENT.—Written consent described in this subparagraph is written consent that—

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

(ii) states the United States person is—

(I) providing consent to the Governmental entity to access certain digital contents or consensually disclosing an access credential; or

(II) consensually providing online account information; and

(iii) specifies the digital contents, access credential, or online account information with respect to which the United States person is providing consent.

(d) RETENTION OF DIGITAL CONTENTS.—

(1) LAWFUL ACCESS.—A Governmental entity that obtains access to the digital contents of electronic equipment, the digital contents of an online account, or online account information in accordance with this section may not make or retain a copy of the digital contents or online account information, or any information directly or indirectly derived from the digital contents or online account information, unless there is probable cause to believe the digital

contents or online account information contains evidence of, or constitutes the fruits of, a crime.

(2) UNLAWFUL ACCESS.—If a Governmental entity obtains access to the digital contents of electronic equipment, digital contents of an online account, or online account information in a manner that is not in accordance with this section, the Governmental entity—

(A) shall immediately destroy any copy of the digital contents or online account information, and any information directly or indirectly derived from the digital contents or online account information, in the custody or control of the Governmental entity;

(B) may not disclose the digital contents or online account information, or any information directly or indirectly derived from the digital contents or online account information, to any other Governmental entity or a State or local government; and

(C) shall notify the United States person that any copy of the digital contents or online account information, and any information directly or indirectly derived from the digital con-

tents or online account information, has been destroyed.

(e) RECORDKEEPING.—A Governmental entity shall keep a record of each instance in which the Governmental entity obtains access to the digital contents of electronic equipment belonging to or in the possession of an individual at the border, the digital contents of an online account of an individual who is at the border, or online account information of an individual who is at the border, which shall include—

(1) the reason for the access;

(2) the nationality, immigration status, and admission category of the individual;

(3) the nature and extent of the access;

(4) if the access was consensual, how and to what the individual consented, and what the individual provided by consent;

(5) whether electronic equipment of the individual was seized;

(6) whether the Governmental entity made a copy of all or a portion of the digital contents or online account information, or any information directly or indirectly derived from the digital contents or online account information; and

(7) whether the digital contents or online account information, or any information directly or indirectly derived from the digital contents or online account information, was shared with another Governmental entity or a State or local government.

SEC. 6. LIMITS ON USE OF DIGITAL CONTENTS AS EVIDENCE.

(a) IN GENERAL.—Whenever any digital contents or online account information have been obtained in violation of this Act, no part of the digital contents or online account information and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding (including any proceeding relating to the immigration laws, as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))) in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

(b) APPLICATION.—To the maximum extent practicable, the limitations under subsection (a) shall be applied in the same manner as the limitations under section 2515 of title 18, United States Code.

SEC. 7. LIMITS ON SEIZURE OF ELECTRONIC EQUIPMENT.

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

States person at the border unless there is probable cause to believe that the electronic equipment contains information that is relevant to an allegation that the United States person has committed a felony.

SEC. 8. AUDIT AND REPORTING REQUIREMENTS.

In March of each year, the Secretary of Homeland Security shall submit to Congress and make publicly available on the Web site of the Department of Homeland Security a report that includes the following:

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

(A) Accessed the digital contents of any electronic equipment belonging to or in the possession of or the digital contents of an online account of a United States person at the border pursuant to a warrant supported by probable cause issued using the procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction.

(B) Accessed the digital contents of any electronic equipment belonging to or in the possession of a United States person at the border pursuant to the emergency authority under section 5(b).

(C) Requested consent to access the digital contents of any electronic equipment belonging to or in the possession of, the digital contents of an online account of, or online account information of a United States person at the border.

(D) Accessed the digital contents of any electronic equipment belonging to or in the possession of, the digital contents of an online account of, or online account information of a United States person at the border pursuant to written consent provided in accordance with section 5(c).

(E) Requested a United States person at the border consensually disclose an access credential that would enable access to the digital contents of electronic equipment or the digital contents of an online account of the United States person.

(F) Accessed the digital contents of electronic equipment or the digital contents of an online account of a United States person at the border using an access credential pursuant to written consent provided in accordance with section 5(c).

(G) Accessed the digital contents of any electronic equipment belonging to or in the possession of, the digital contents of an online account of, or online account information of a United States person at the border in a manner that was not in accordance with section 5.

(H) Accessed the digital contents of any electronic equipment belonging to or in the possession of, the digital contents of an online account of, or online account information of an individual who is not a United States person at the border.

(I) Accessed the digital contents of any electronic equipment belonging to or in the possession of an individual at the border, the digital contents of an online account of an individual at the border, or online account information of an individual at the border (regardless of whether the individual is a United States person) at the request of a Governmental entity (including another component of the Department of Homeland Security) that is not the Governmental entity employing the individual accessing the digital contents or online account information.

(2) Aggregate data on—

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

(i) the digital contents of electronic equipment belonging to or in the possession of the United States person at the border;

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

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

(B) the country from which United States persons departed most recently before arriving in the United States for the United States persons for which a Governmental entity obtains access to—

(i) the digital contents of electronic equipment belonging to or in the possession of the United States person at the border;

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

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

(C) the number and nationality of individuals who are not United States persons for which a Governmental entity obtains access to—

(i) the digital contents of electronic equipment belonging to or in the possession of the individuals at the border;

(ii) the digital contents of an online account of the individuals while at the border; or

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

(D) the country from which individuals who are not United States persons departed most recently before arriving in the United States for the individuals for which a Governmental entity obtains access to—

(i) the digital contents of electronic equipment belonging to or in the possession of the individuals at the border;

(ii) the digital contents of an online account of the individuals while at the border; or

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

(3) Aggregate data regarding the perceived race and ethnicity of individuals for whom a Governmental entity obtains access to—

(A) the digital contents of electronic equipment belonging to or in the possession of the individuals at the border;

(B) the digital contents of an online account of the individuals while at the border; or

(C) online account information of the individuals while at the border.

○