S 823

Protecting Data at the Border Act

Congress: 115 (2017–2019, Ended)
Chamber: Senate
Policy Area: Immigration
Introduced: Apr 4, 2017
Current Status: Committee on Homeland Security and Governmental Affairs Subcommittee on Federal Spending Oversight a
Latest Action: Committee on Homeland Security and Governmental Affairs Subcommittee on Federal Spending Oversight and Emergency Management. Hearings held. With printed Hearing: S.Hrg. 115-365. (Jul 11, 2018)
Official Text: https://www.congress.gov/bill/115th-congress/senate-bill/823

Sponsor

Name: Sen. Wyden, Ron [D-OR]
Party: Democratic • **State:** OR • **Chamber:** Senate

Cosponsors (3 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Paul, Rand [R-KY]	R · KY		Apr 4, 2017
Sen. Markey, Edward J. [D-MA]	D · MA		Apr 5, 2017
Sen. Merkley, Jeff [D-OR]	D · OR		Jun 21, 2017

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Hearings By (subcommittee)	Jul 11, 2018
Homeland Security Committee	House	Bills of Interest - Exchange of Letters	Feb 23, 2018

Subjects & Policy Tags

Policy Area:

Immigration

Related Bills

Bill	Relationship	Last Action
115 HR 1899	Identical bill	**Apr 26, 2017:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.

Summary (as of Apr 4, 2017)

Protecting Data at the Border Act

This bill prohibits a governmental entity from: (1) accessing the digital contents of electronic equipment belonging to, or in the possession of, a U.S. person (person) at the border without a valid warrant; or (2) denying a person's U.S. entry or exit based on the person's refusal to disclose an access credential or in order to determine whether such person will consensually provide an access credential, access, or online account information.

A border officer may access the digital contents of electronic equipment without a warrant if the officer determines that an emergency situation exists. The officer must subsequently apply for a warrant within seven days, and if such warrant is not granted: (1) digital content copies must be destroyed, (2) digital contents or information may not be disclosed, and (3) the person shall be notified of such destruction.

A governmental entity may not make or retain a copy of the digital contents of electronic equipment, an online account, or online account information without probable cause to believe that such information contains evidence of, or constitutes the fruits of, a crime.

Unlawfully accessed information: (1) must be destroyed and the person notified of its destruction; (2) may not be disclosed; and (3) may not be received in evidence in any trial, hearing, or other proceeding.

A governmental entity shall keep a record of each instance in which it obtains access to an individual's digital information.

A governmental entity may not seize electronic equipment belonging to, or in the possession of, a person at the border without probable cause to believe that such equipment contains information relevant to a felony.

Actions Timeline

- **Jul 11, 2018:** Committee on Homeland Security and Governmental Affairs Subcommittee on Federal Spending Oversight and Emergency Management. Hearings held. With printed Hearing: S.Hrg. 115-365.
- **Apr 4, 2017:** Introduced in Senate
- **Apr 4, 2017:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.