A BILL

To place restrictions on searches and seizures of electronic devices at the border.

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

SECTION 1. DEFINITIONS.

In this Act:

(1) FORENSIC SEARCH.—The term “forensic search” means any examination of an electronic de-
vice that—

(A) is conducted for longer than 4 hours;

(B) is conducted with the assistance of any

other electronic device, electronic equipment, or
software, including software enabling the searching, scanning, or indexing of the contents of the device;

(C) involves the copying or documentation of data stored on the device; or

(D) is conducted in any other manner that would not fall within the definition of a manual search or a search described in section 4(1).

(2) MANUAL SEARCH.—The term “manual search” means the examination of an electronic device that is conducted manually without—

(A) the assistance of any other electronic device, electronic equipment, or software, including the use of special search programs; or

(B) the entry of any password, passcode, fingerprint, account information, or other biometric identifier that permits access to data otherwise protected by technological means.

SEC. 2. SEARCHES AND SEIZURES OF ELECTRONIC DEVICES AT THE BORDER.

(a) In General.—Except as otherwise provided in this section, an official of the Department of Homeland Security may not search or seize an electronic device transported by a United States person at the international border.
(b) MANUAL SEARCHES.—An electronic device transported by an individual at the border may be subject to a manual search by an official of the Department of Homeland Security, in accordance with the procedures described in subsection (f) if the official has a reasonable suspicion that—

(1) the individual transporting the device—

(A) is carrying contraband or is otherwise transporting goods or persons in violation of the laws enforced by the Department of Homeland Security; or

(B) is inadmissible or otherwise not entitled to enter the United States under such laws; and

(2) the device contains information or evidence relevant to a violation referred to in paragraph (1).

(c) SEIZURES.—An electronic device transported by an individual at the border may be seized by an official of the Department of Homeland Security, in accordance with the procedures described in subsection (f) if the official has probable cause to believe that—

(1) the individual—

(A) is carrying contraband or is otherwise transporting goods or persons in violation of the
laws enforced by the Department of Homeland
Security;

(B) is inadmissible or otherwise not enti-
tled to enter the United States under such laws;

or

(C) is in violation of any Federal or State
law punishable by more than 1 year; and

(2) the electronic device contains information or
evidence relevant to a violation referred to in para-
graph (1).

(d) FORENSIC SEARCHES.—An electronic device
transported by an individual at the border may be subject
to forensic search only pursuant to a warrant issued using
the procedures described in the Federal Rules of Criminal
Procedure (or, in the case of a State court, issued using
State warrant procedures) by a court of competent juris-
diction.

(e) ADMISSIBILITY OF EVIDENCE.—Information ob-
tained or derived pursuant to a violation of this section—

(1) may not be used as the basis for dem-
onstrating the inadmissibility or removability of an
individual; and

(2) may not be received in evidence or disclosed
in any trial, hearing, or other proceeding in or be-
fore any court, grand jury, department, officer,
agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(f) PROCEDURES FOR SEARCHES AND SEIZURES OF ELECTRONIC DEVICES AT THE BORDER.—

(1) INITIATING A SEARCH OR SEIZURE.—Prior to initiating any search or seizure of an electronic device transported by an individual at the border pursuant to the authority under this section, the official of the Department of Homeland Security initiating the search or seizure shall—

(A) obtain supervisory approval to engage in the search or seizure; and

(B) record—

(i) the nature of the reasonable suspicion or probable cause and the specific facts or bases for that determination; and

(ii) the age, sex, country of origin, citizenship or immigration status, ethnicity, and race of the individual transporting the electronic device.

(2) CONDITIONS FOR A MANUAL SEARCH.—

(A) PRESENCE OF THE INDIVIDUAL.—The individual transporting the electronic device subject to a manual search shall be permitted
to remain present during the search of the elec-
tronic device.

(B) Scope of Manual Search.—A manual
search—

(i) shall be conducted by an official of
the Department of Homeland Security
manually, without the assistance of any
electronic device or electronic equipment;

(ii) shall be tailored to the reasonable
suspicion recorded by the official of the
Department of Homeland Security before
the manual search began;

(iii) shall be confined to documents,
files, or other electronic information stored
on the electronic device that could reason-
ably contain information or evidence rel-
evant to a violation described in paragraph
(3) and are accessible without the entry of
any password, passcode, fingerprint, or
other biometric identifier; and

(iv) may not exceed a total of 4 hours.

(C) Destruction of Inadvertently
Collected Information.—Unless an official
of the Department of Homeland Security deter-
mines, not later than 5 days after a manual
search, that information obtained from the electronic device is evidence of a violation described in paragraph (3), an official of the Department shall delete any information collected from or about the device from Department records not later than 10 days after the date on which the search was conducted.

(3) CONDITIONS FOR A SEIZURE OF AN ELECTRONIC DEVICE.—

(A) REQUIREMENT FOR WARRANT OR COURT ORDER APPROVING SEIZURE.—

(i) IN GENERAL.—Not later than 48 hours after an official of the Department of Homeland Security seizes an electronic device pursuant to the authority under this section, an official of the Department shall seek a warrant or order approving the seizure under the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures).

(ii) NO WARRANT OR ORDER.—If a warrant or order is denied or fails to be issued after the seizure, an official of the Department of Homeland Security shall
immediately return the electronic device to
the individual from whom it was seized.

(B) Suspension and Prohibition of
Search.—An electronic device seized at the
border pursuant to the authority under this sec-
tion may not be accessed or searched by any
governmental entity before the issuance of a
warrant or court order authorizing the access-
ing or search of the device.

SEC. 3. REPORTING.

The Secretary of Homeland Security shall submit an
annual report to the Committee on the Judiciary of the
Senate, the Committee on the Judiciary of the House of
Representatives, the Committee on Homeland Security
and Governmental Affairs of the Senate, and the Com-
mittee on Homeland Security of the House of Representa-
tives that details—

(1) the number of electronic devices subject to
a manual search pursuant to the authority under
section 2;

(2) the number of electronic devices subject to
a forensic search pursuant to the authority under
section 2;

(3) the number of electronic devices seized pur-
suant to the authority under section 2;
(4) statistics regarding the age, sex, country of origin, citizenship or immigration status, ethnicity, and race of the individuals transporting electronic devices that were subject to a manual search, a forensic search, or seizure; and

(5) the number of individuals whose electronic devices were searched or seized pursuant to the authority under section 2 and were later charged with a criminal offense based on information obtained from such search or seizure.

SEC. 4. SAVINGS PROVISIONS.

Nothing in this Act may be construed—

(1) to affect the authority of any law enforcement official to conduct any other lawful search predicated on an established exception, other than the exception for border searches, to the warrant requirement of the Fourth Amendment to the Constitution of the United States; or

(2) to require the individual subject to a search of his or her electronic device to provide any password, passcode, fingerprint, faceprint, or other biometric identifier without his or her consent, in violation of the Fifth Amendment to the Constitution of the United States.