AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

112TH CONGRESS
1ST SESSION

S. 1011

To improve the provisions relating to the privacy of electronic communications.

IN THE SENATE OF THE UNITED STATES

MAY 17, 2011

Mr. LEAHY introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To improve the provisions relating to the privacy of electronic communications.

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 ''Electronic Communications Privacy Act Amendments Act of 2011''.

SEC. 2. PROHIBITION ON DISCLOSURE OF CONTENT.

Section 2702(a)(3) of title 18, United States Code, is amended to read as follows:

''(3) a provider of electronic communication service, remote computing service, or geolocation information service to the public shall not knowingly

divulge to any governmental entity the contents of any communication described in section 2703(a), or any record or other information pertaining to a subscriber or customer of such provider or service.''.

SEC. 3. ELIMINATION OF 180-DAY RULE AND SEARCH WARRANT REQUIREMENT; REQUIRED DISCLOSURE OF CUSTOMER RECORDS.

(a) IN GENERAL.—Section 2703 of title 18, United States Code, is amended—

(1) by striking subsections (a), (b), and (c) and inserting the following:

''(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—

''(1) IN GENERAL.—A governmental entity may require the disclosure by a provider of electronic communication service, remote computing service, or geolocation information service of the contents of a wire or electronic communication that is in electronic storage with or otherwise held or maintained by the provider if the governmental entity obtains a warrant issued and executed in accordance with the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure.

"(2) NOTICE.—Except as provided in section 2705, not later than 3 days after a governmental entity receives the contents of a wire or electronic communication of a subscriber or customer from a provider of electronic communication service, remote computing service, or geolocation information service under paragraph (1), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

"(A) a copy of the warrant; and

"(B) a notice that includes the information referred to in section 2705(a)(5)(B)(i).

"(b) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE, REMOTE COMPUTING SERVICE, OR GEOLOCATION INFORMATION SERVICE.—

"(1) IN GENERAL.—Subject to paragraph (2) and subsection (g), a governmental entity may require a provider of electronic communication service, remote computing service, or geolocation information service to disclose a record or other information pertaining to a subscriber or customer of the provider or service (not including the contents of communications), only if the governmental entity—

"(A) obtains a warrant issued and executed in accordance with the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure;

"(B) obtains a court order directing the disclosure under subsection (c);

"(C) has the consent of the subscriber or customer to the disclosure; or

"(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of the provider or service that is engaged in telemarketing (as defined in section 2325).

"(2) SUBPOENAS.—

"(A) IN GENERAL.—A governmental entity may require a provider of electronic communication service, remote computing service, or geolocation information service to disclose information described in subparagraph (B) if the governmental entity obtains—

"(i) an administrative subpoena under a Federal or State statute; or

"(ii) a Federal or State grand jury subpoena or trial subpoena.

"(B) REQUIREMENTS.—The information described in this subparagraph is—

"(i) the name of the subscriber or customer;

"(ii) the address of the subscriber or customer;

"(iii) the local and long distance telephone connection records, or records of session times and durations, of the subscriber or customer;

"(iv) length of service (including start date) and types of service utilized by the subscriber or customer;

"(v) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, of the subscriber or customer; and

"(vi) means and source of payment for such service (including any credit card or bank account number) of the subscriber or customer.

"(3) NOTICE NOT REQUIRED.—A governmental entity that receives records or information under this subsection is not required to provide notice to a subscriber or customer."; and

(2) by redesignating subsections (d) through (g) as subsections (c) through (f), respectively.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) SECTION 2258A.—Section 2258A(h)(1) of title 18, United States Code, is amended by striking "section 2703(f)" and inserting "section 2703(e)".

(2) SECTION 2703.—Section 2703(c) of title 18, United States Code, as redesignated by subsection (a), is amended—

(A) by striking "A court order for disclosure under subsection (b) or (c)" and inserting "A court order for disclosure under subsection (b)(1)(B) or (g)(3)(A)(ii)"; and

(B) by striking "the contents of a wire or electronic communication, or the records or other information sought," and inserting "the records, other information, or historical geolocation information sought".

(3) SECTION 2707.—Section 2707(a) of title 18, United States Code, is amended by striking "section 2703(e)" and inserting "section 2703(d)".

(4) SECTION 3486.—Section 3486(a)(1)(C)(i) of title 18, United States Code, is amended by striking "section 2703(c)(2)" and inserting "section 2703(b)(2)(B)".

SEC. 4. DELAYED NOTICE.

Section 2705 of title 18, United States Code, is amended to read as follows:

"§ 2705. Delayed notice

"(a) DELAY OF NOTIFICATION.—

"(1) IN GENERAL.—A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order delaying the notification required under section 2703(a) for a period of not more than 90 days.

"(2) DETERMINATION.—A court shall grant a request for delayed notification made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant may result in—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses;

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial; or

"(F) endangering national security.

"(3) EXTENSION.—Upon request by a governmental entity, a court may grant 1 or more extensions of the delay of notification granted under paragraph (2) of not more than 90 days.

"(4) EXPIRATION OF THE DELAY OF NOTIFICATION.—Upon expiration of the period of delay of notification under paragraph (2) or (3), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail or other means reasonably calculated to be effective as specified by the court approving the search warrant, the customer or subscriber—

"(A) a copy of the warrant; and

"(B) notice that informs the customer or subscriber—

"(i) that information maintained for the customer or subscriber by the provider of electronic communication service, remote computing service, or geolocation information service named in the process or re-

quest was supplied to, or requested by, the governmental entity;

"(ii) of the date on which the request to the provider for information was made by the governmental entity and the date on which the information was provided by the provider to the governmental entity;

"(iii) that notification of the customer or subscriber was delayed;

"(iv) the identity of the court authorizing the delay; and

"(v) of the provision of this chapter under which the delay was authorized.

"(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—

"(1) IN GENERAL.—A governmental entity that is obtaining the contents of a communication or information or records under section 2703 or geolocation information under section 2713 may apply to a court for an order directing a provider of electronic communication service, remote computing service, or geolocation information service to which a warrant, order, subpoena, or other directive under section 2703 or 2713 is directed not to notify any other person of the existence of the warrant, order,

subpoena, or other directive for a period of not more than 90 days.

"(2) DETERMINATION.—A court shall grant a request for an order made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant, order, subpoena, or other directive may result in—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses;

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial; or

"(F) endangering national security.

"(3) EXTENSION.—Upon request by a governmental entity, a court may grant 1 or more extensions of an order granted under paragraph (2) of not more than 90 days.".

SEC. 5. LOCATION INFORMATION PRIVACY.

(a) IN GENERAL.—Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

"§ 2713. Location tracking of electronic communications device

"(a) PROHIBITION.—Except as provided in subsection (b), (c), or (d), no governmental entity may access or use an electronic communications device to acquire geolocation information.

"(b) ACQUISITION PURSUANT TO A WARRANT OR COURT ORDER.—A governmental entity may access or use an electronic communications device to acquire geolocation information if the governmental entity obtains—

"(1) a warrant issued and executed in accordance with the Federal Rules of Criminal Procedure relating to tracking devices (or, in the case of a State court, issued using State warrant procedures), issued by a court of competent jurisdiction authorizing the accessing or use of an electronic communications device to acquire geolocation information; or

"(2) a court order under title I or title VII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq. and 1881 et seq.) authorizing the accessing or use of an electronic communications device to acquire geolocation information.

"(c) PERMITTED ACQUISITIONS WITHOUT COURT ORDER.—A governmental entity may access or use an

electronic communications device to acquire geolocation information—

"(1) as permitted under section 222(d)(4) of the Communications Act of 1934 (47 U.S.C. 222(d)(4)) in order to respond to a call for emergency services by a user of an electronic communications device; or

"(2) with the express consent of the owner or user of the electronic communications device concerned.

"(d) EMERGENCY ACQUISITION OF GEOLOCATION INFORMATION.—

"(1) IN GENERAL.—Subject to paragraph (2), an investigative or law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, any United States attorney, any acting United States attorney, or the principal prosecuting attorney of any State or political subdivision thereof acting pursuant to a statute of that State may access or use an electronic communications device to acquire geolocation information if the investigative or law enforcement officer reasonably determines that—

"(A) an emergency situation exists that—

"(i) involves—

"(I) immediate danger of death or serious bodily injury to any person;

"(II) conspiratorial activities characteristic of organized crime; or

"(III) an immediate threat to national security; and

"(ii) requires the accessing or use of an electronic communications device to acquire geolocation information before an order authorizing the acquisition may, with due diligence, be obtained; and

"(B) there are grounds upon which an order could be entered under this section to authorize the accessing or use of an electronic communications device to acquire geolocation information.

"(2) ORDER AND TERMINATION.—If an investigative or law enforcement officer accesses or uses an electronic communications device to acquire geolocation information under paragraph (1)—

"(A) not later than 48 hours after the activity to acquire the geolocation information has occurred, or begins to occur, the investigative or

law enforcement officer shall seek a warrant or order described in subsection (b) approving the acquisition; and

"(B) unless a warrant or order described in subsection (b) is issued approving the acquisition, the activity to acquire the geolocation information shall terminate immediately at the earlier of the time—

"(i) the information sought is obtained;

"(ii) the application for the warrant or order is denied; or

"(iii) at which 48 hours have elapsed since the activity to acquire the geolocation information began to occur.

"(3) VIOLATION AND SUPPRESSION OF EVIDENCE.—

"(A) IN GENERAL.—In a circumstance described in subparagraph (B), a court may determine that—

"(i) no information obtained, or evidence derived from, geolocation information acquired as part of the accessing or use of an electronic communications device to acquire geolocation information may be

received into evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof; and

"(ii) no information concerning any person acquired from the geolocation information may be used or disclosed in any other manner, without the consent of the person.

"(B) CIRCUMSTANCES.—A circumstance described in this subparagraph is any instance in which—

"(i) an investigative or law enforcement officer does not—

"(I) obtain a warrant or order described in subsection (b) within 48 hours of commencing the accessing or use of the electronic communications device; or

"(II) terminate the activity to acquire geolocation information in accordance with paragraph (2)(B); or

"(ii) a court denies the application for a warrant or order approving the accessing or use of an electronic communications device to acquire geolocation information.

"(e) ASSISTANCE AND COMPENSATION.—

"(1) IN GENERAL.—A warrant described in subsection (b)(1) authorizing the accessing or use of an electronic communications device to acquire geolocation information shall, upon request of the applicant, direct that a provider of electronic communication service, remote computing service, or geolocation information service shall provide to the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with the services that the provider is providing to or through the electronic communications device in question.

"(2) COMPENSATION.—Any provider of electronic communication service, remote computing service, or geolocation information service providing information, facilities, or technical assistance under a directive under paragraph (1) shall be compensated by the applicant for reasonable expenses

incurred in providing the information, facilities, or assistance.

"(f) NO CAUSE OF ACTION AGAINST A PROVIDER.—No cause of action shall lie in any court against any provider of electronic communication service, remote computing service, or geolocation information service, or an officer, employee, or agent of the provider or other specified person for providing information, facilities, or assistance necessary to accomplish an acquisition of geolocation information authorized under this section.".

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Title 18 of the United States Code is amended—

(1) in the table of sections for chapter 121, by adding at the end the following:

"2713. Location tracking of electronic communications device.";

(2) in section 2703—

(A) in subsection (d), as redesignated by section 3, by inserting "geolocation information service, or remote computing service," after "electronic communication service,";

(B) in subsection (e)(1), as redesignated by section 3, by striking "electronic communication services or a" and inserting "electronic communication service, geolocation information service, or"; and

(C) in subsection (f), as redesignated by section 3—

(i) by inserting ", geolocation information service," after "electronic communication service"; and

(ii) by inserting ", geolocation information," after "contents of communications";

(3) in section 2711—

(A) in paragraph (3), by striking "and" at the end;

(B) in paragraph (4), by striking the period at the end and inserting a semicolon; and

(C) by adding at the end the following:

"(5) the term 'electronic communications device' means any device that enables access to or use of an electronic communications system, electronic communication service, remote computing service, or geolocation information service;

"(6) the term 'geolocation information'—

"(A) means any information concerning the location of an electronic communications device that is in whole or in part generated by or derived from the operation or use of the electronic communications device;

"(B) does not include—

"(i) information described in section 2703(b)(2)(B); or

"(ii) the contents of a communication;

"(7) the term 'geolocation information service' means the provision of a global positioning service or other mapping, locational, or directional information service;

"(8) the term 'electronic communication identifiable information' means the—

"(A) name of a person or entity;

"(B) address of a person or entity;

"(C) records of session times and durations of a person or entity;

"(D) length of service and types of service used by a person or entity;

"(E) telephone or instrument number or other subscriber number or identity (including any temporarily assigned network address) of a person or entity; and

"(F) dialing, routing, addressing, and signaling information associated with each communication to or from the subscriber account of a person or entity (including the date, time, and

duration of the communications, without geographical limit);

''(9) the term 'toll billing records' means the—

''(A) name of a person or entity;

''(B) address of a person or entity;

''(C) length of service of a person or entity; and

''(D) local and long distance billing records of a person or entity; and

''(10) the term 'customer' means any person, or authorized representative of that person, who used or is using any service provided by an electronic communication service, remote computing service, or geolocation information service, regardless of whether the service was, or is, being provided for a monetary fee.''; and

(4) in section 3127—

(A) in paragraph (1), by striking ''and 'contents' have'' and inserting '''contents', and 'geolocation information' have'';

(B) in paragraph (3), by inserting '' or geolocation information,'' after ''contents of any communication''; and

(C) in paragraph (4), by inserting ''or geolocation information'' after ''contents of any communication''.

SEC. 6. REQUIRED DISCLOSURE OF LOCATION INFORMATION AND WARRANT REQUIREMENT.

Section 2703 of title 18, United States Code, as amended by section 3, is amended by adding at the end the following:

''(g) LOCATION INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), a governmental entity may not require a provider of electronic communication service, remote computing service, or geolocation information service to disclose geolocation information contemporaneously or prospectively.

''(2) EXCEPTIONS.—

''(A) WARRANTS.—A governmental entity may require a provider of electronic communication service, remote computing service, or geolocation information service to disclose geolocation information contemporaneously or prospectively pursuant to a warrant issued and executed in accordance with the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant proce-

dures), issued by a court of competent jurisdiction.

"(B) CALL FOR EMERGENCY SERVICES.—A provider of electronic communication service, remote computing service, or geolocation information service may provide geolocation information contemporaneously or prospectively to a governmental entity as permitted under section 222(d)(4) of the Communications Act of 1934 (47 U.S.C. 222(d)(4)) in order to respond to a call for emergency services by a user of an electronic communications device.

"(3) HISTORICAL LOCATION INFORMATION.—

"(A) IN GENERAL.—A governmental entity may require a provider of electronic communication service, remote computing service, or geolocation information service to disclose historical geolocation information pertaining to a subscriber or customer of the provider only if the governmental entity —

"(i) obtains a warrant issued and executed in accordance with the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of

competent jurisdiction directing the disclosure;

"(ii) obtains a court order directing the disclosure under subsection (c); or

"(iii) has the consent of the subscriber or customer to the disclosure.

"(B) NOTICE NOT REQUIRED.—A governmental entity that receives historical geolocation information under subparagraph (A) is not required to provide notice to a subscriber or customer.".

SEC. 7. VOLUNTARY DISCLOSURES TO PROTECT CYBERSECURITY.

Section 2702 of title 18, United States Code is amended—

(1) in subsection (b)(5), by inserting ", cybersecurity," after "rights";

(2) in subsection (c)(3), by inserting ", cybersecurity," after "rights"; and

(3) by adding at the end the following:

"(e) REPORTING OF CYBERSECURITY DISCLOSURES.—On an annual basis, the Attorney General of the United States shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

"(1) the number of accounts from which the Federal Government has received voluntary disclosures under subsection (b)(5) that pertain to the protection of cybersecurity; and

"(2) a summary of the basis for disclosure in each instance where—

"(A) a voluntary disclosure under subsection (b)(5) that pertains to the protection of cybersecurity was made to the Department of Justice; and

"(B) the investigation pertaining to the disclosure was closed without the filing of criminal charges.".

SEC. 8. ELECTRONIC COMMUNICATION IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Section 2709(a) of title 18, United States Code, is amended by striking "electronic communication transactional records" and inserting "electronic communication identifiable information".

(b) REQUIRED CERTIFICATION.—Section 2709(b) of title 18, United States Code, is amended to read as follows:

"(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation, or a designee in a position not lower than Deputy Assistant Director at Bu-

reau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may request the toll billing records and electronic communication identifiable information of a person or entity if the Director (or designee) certifies in writing to the wire or electronic communication service provider or geolocation information service provider to which the request is made that the toll billing records and electronic communication identifiable information sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.''.

○