SECTION 1. SHORT TITLE. This Act may be referred to as the Always-On Device Data Privacy Protection Act of 2017.

SECTION 2. DEFINITIONS. For the purposes of this section,

(1) "Always-on device" means a commercial device that continuously collects audio, video, or image data or data that can be directly used to measure biometric information, including heart rate, breathing, human movement, or human location. "Always-on device" does not include a device that collects such data only when purposely triggered by the contemporaneous action of a consumer.

(2) "Always-on device data" means any information obtained, recorded, or transmitted by an Always-on device, including, but not limited to, raw or transcribed audio, image, or video data, timestamp information, or any personally identifiable information.

(3) "Consumer" means the owner or user of an Always-on device.

(4) "Government entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(5) "Interface" means is any medium that enables consumers to interact with an Always-on device.

(6) "Personally identifiable information" means data captured by an Always-on device that uniquely identifies an individual.

(7) "Service provider" means a person or entity offering services related to Always-on devices, including device manufacturers, or any person or other entity that uses information obtained from Always-on devices for processing and fulfillment, product development, analytics, advertising and marketing, or similar business functions.

SECTION 3. RESTRICTIONS ON COMMERCIAL USE.

(a) Except as provided in this section, a service provider who knowingly discloses, to any person, Always-on device data concerning any consumer shall be liable to the aggrieved person for the relief provided in Section 8.

(b) A service provider may disclose Always-on device data concerning any consumer—

(1) to the consumer when the data pertains to the consumer him or herself;

(2) as may be necessarily incident to the rendition of the service;

(3) when the data pertains to the consumer him or herself, to any person with the consumer's informed, written or oral consent (including through an electronic means using the internet) that—

(A) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;

(B) at the election of the consumer—

(i) is given at the time the disclosure is sought; or

(ii) is given in advance for a set period of time, not to exceed 2 years, or until consent is withdrawn by the consumer, whichever is sooner;

(C) the service provider has provided an opportunity, in a clear and conspicuous manner for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election; and

(D) the service provider has provided a separate clear and conspicuous opportunity to consent to each separate type of disclosure or category of Always-on data recipient;

(E) where the failure to consent to a particular type of disclosure would

seriously undermine the advertised function of the Always-on device, the service provider has provided the consumer with clear and conspicuous notice prior to purchase of the Always-on device; and

(F) if the consent is provided orally, it is recorded and made available to the consumer pursuant to Section 6;

(4) to a government entity, if the service provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(A) A government entity that receives Always-on device data pursuant to this paragraph must comply with the requirements of Section 4(b)(3);

(5) to a government entity pursuant to Section 4.

(c) A service provider may not alter the price of an Always-on device based on whether or not the consumer consents to disclosure of Always-on device data.

SECTION 4. PRODUCTION OF OR ACCESS TO ALWAYS-ON DEVICE DATA.

(a) Except as provided in this section, a government entity shall not do any of the following:

(1) Compel the production of or access to Always-on device data from a service provider;

(2) Compel the production of or access to Always-on device data from any person or entity other than the consumer; or

(3) Access Always-on device data by means of physical interaction or electronic communication with the Always-on device.

(b) A government entity may compel the production of or access to Always-on device data from a service provider, or compel the production of or access to Always-on device data from any person or entity other than the consumer only under the following circumstances:

(1) With the specific consent of the consumer when the data pertains to the consumer him or herself;

(2) Pursuant to a warrant issued under the procedures described in the Federal Rules of Criminal Procedure, or, in the case of a State court, issued under State warrant procedures, by a court of competent jurisdiction;

(3) If the government entity believes that an emergency involving immediate danger of death or serious physical injury to any person requires obtaining without delay Always-on device data relating to the emergency and the request is narrowly tailored to address the emergency, subject to the following limitations:

(A) the request shall document the factual basis for believing that an emergency involving immediate danger of death or serious physical injury to a person requires obtaining without delay of the information relating to the emergency; and

(B) not later than 48 hours after the date on which a government entity thereof obtains access to records under paragraph (3), the governmental entity shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the government entity setting forth the grounds for the emergency access.

(4) A government entity specially designated by the Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of the State, may acquire Always-on device data before obtaining a warrant if:

(A) The government entity cannot, with due diligence, obtain a warrant to address an emergency situation that involves:

(i) immediate danger of death or serious bodily injury, or

(ii) immediate threat to the national security interest; and

(B) When the government entity acquires Always-on device data, there are grounds upon which a warrant could be entered under this chapter to authorize the acquisition.

(5) A government entity that acquires Always-on device data before obtaining a warrant authorizing the acquisition must, within forty-eight hours after the acquisition occurs or begins to occur, obtain a warrant approving acquisition in accordance with paragraph (2).

(6) In the absence of a warrant, such acquisition shall immediately terminate when the data sought is obtained or when the application for a warrant is denied, whichever is earlier.

(7) In the event such application for a warrant is denied, or in any other case where the interception is terminated without a warrant having been issued, the Always-on device data acquired shall be treated as having been obtained in violation of this chapter, and notice shall be served to all consumers about whom Always-on device data was acquired according to Section 5 of this chapter.

(c) No Always-on device data and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or state authority, or a political subdivision thereof, if the disclosure of that information would be in violation of this chapter.

SECTION 5. NOTICE.

(a) Unless delayed notice is ordered under subsection (b), not later than three days after a government entity receives Always-on device data under Section 4, the government

entity shall serve upon, or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the warrant to the consumer(s)—

(1) a copy of the warrant; and

(2) notice that informs such consumer(s)—

(A) of the nature of the law enforcement inquiry with reasonable specificity;

(B) that Always-on device data maintained for such consumer(s) was supplied to or requested by that government entity and the date on which the supplying or request took place;

(C) an inventory of the Always-on device data supplied, including, at a minimum, the data and time of each Always-on device datum supplied;

(D) if such Always-on device data was obtained from a service provider or other third party, the identity of the third party from which the information was obtained;

(E) whether notification of such consumer(s) was delayed pursuant to subsection (b);

(F) what court made the certification or determination pursuant to which that delay was made, if applicable; and

(G) if applicable, which provision of this chapter allowed such delay.

(b) Delay of Notification— A government entity acting under Section 4 may include in the application a request for an order delaying the notification required under section 5(a) for

a period not to exceed 90 days, and the court shall issue the order if the court determines that there is reason to believe that notification of the existence of the warrant result in—

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

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(c) Upon expiration of the period of delay granted under subsection (b), the government entity shall provide the consumer(s) a copy of warrant together with notice required under, and by the means described in, subsection (a).

(d) Preclusion of Notice to Subject of Governmental Access— A government entity acting under Section 4 may include in the application a request for an order directing a service provider to which a warrant is directed not to notify any other person of the existence of the warrant for a period of not more than 90 days, and the court shall issue the order if the court determines that there is reason to believe that notification of the existence of the warrant may result in—

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

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

SECTION 6. DATA RETENTION AND USER CONTROL.

(a) A service provider shall establish and maintain a consumer interface that permits any

consumer to view, permanently delete, or permanently save any Always-on device data pertaining to that consumer.

(b) A service provider shall permanently delete a customer's Always-on device data as soon as practicable, but no later than two years from the date the information is no longer necessary for the purpose for which it was collected.

(c) Notwithstanding subsections (a) and (b), the service provider must retain—

(1) any recording of oral consent required by Section 3(b) until the consumer withdraws his or her consent or terminates his or her relationship with the service provider;

(2) any Always-on device data the consumer has requested to permanently save under subsection (a); and

(3) any Always-on device data that is the subject of a warrant issued under Section 4(b)(2) or a preservation request issued under subsection (e).

(d) A service provider shall ensure that, to the extent reasonably possible, its Always-on devices distinguish between the consumer's personally identifiable information and the personally identifiable information of individuals other than the consumer and shall permanently delete any personally identifiable information collected that pertains to individuals other than the customer immediately.

(1) This subsection shall not apply to Always-on devices

(A) that aid the visually impaired or the hard of hearing;

(B) that are used exclusively for protecting, securing, or monitoring a home; or

(C) that monitor infants, the elderly, or the disabled for their protection.

(e) A service provider, upon the request of a government entity, shall take all necessary steps to preserve Always-on device data in its possession for 14 days pending the issuance of a warrant

under Section 4(b)(2).

(1) A requesting government entity must specify in a written sworn statement:

(A) the particular Always-on device(s) for which Always-on device data must be preserved; and

(B) the date or dates and timeframes for which Always-on device data must be preserved.

SECTION 7. DATA SECURITY.

(a) A service provider shall—

(1) store, transmit, and protect from disclosure all Always-on device data using the reasonable standard of care within the service provider's industry; and

(2) store, transmit, and protect from disclosure all Always-on device data in a manner that is the same as or more protective than the manner in which the service provider stores, transmits, and protects other confidential information.

(b) The Federal Trade Commission may develop appropriate security standards for Always-on device data.

(1) This subsection preempts subsection (a) only to the extent that the security standards developed are more protective of Always-on device data than the industry standard of care.

SECTION 8. CIVIL ACTION.

(a) Any person aggrieved by any act of a service provider in violation of this chapter may bring a civil action in the United States district court for the judicial district where the aggrieved person resides.

(b) The court may award—

(1) actual damages but not less than liquidated damages in an amount of $100,000;

(2) punitive damages;

(3) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(4) such other preliminary and equitable relief as the court determines to be appropriate.

SECTION 9. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) Violation of this chapter or any regulation prescribed under this chapter shall be treated as a violation of a rule under Section 18 of the Federal Trade Commission Act (15 U.S.C. 57a) regarding unfair or deceptive acts or practices. The Federal Trade Commission shall enforce this chapter in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this chapter.

(b) Any person who violates this chapter or any regulation prescribed under this chapter shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated in and made part of this chapter.

(c) Nothing in this section shall be construed to limit the authority of the Commission under any other provision of law.

(d) In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates this chapter or any regulation prescribed under this chapter may bring a civil action on behalf of the residents of the State in a district court of the

United States of appropriate jurisdiction to—

(1) enjoin that practice;

(2) enforce compliance with this chapter or any regulation prescribed under this chapter;

(3) obtain damage, restitute, or other compensation on behalf of residents of the State; or

(4) obtain such other relief as the court may consider to be appropriate.

SECTION 10. PREEMPTION. The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.