To improve the ability of law enforcement agencies to access encrypted data, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. GRAHAM (for himself, Mr. COTTON, and Mrs. BLACKBURN) introduced the following bill; which was read twice and referred to the Committee on

A BILL

To improve the ability of law enforcement agencies to access encrypted data, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the “Lawful Access to

Encrypted Data Act”.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Sec. 1. Short title.
Sec. 2. Table of contents.

TITLE I—DATA AT REST

Sec. 101. Data at rest.
TITLE II—DATA IN MOTION

Sec. 201. Assistance.
Sec. 203. CALEA amendment.

TITLE III—ASSISTANCE CAPABILITY DIRECTIVES

Sec. 301. Assistance capability directives.

TITLE IV—PEN REGISTER AND TRAP AND TRACE AMENDMENTS

Sec. 401. Capability requirements.
Sec. 402. Defining technical assistance.

TITLE V—FISA AMENDMENTS

Sec. 501. Electronic surveillance within the United States for foreign intelligence purposes.
Sec. 502. Physical searches within the United States for foreign intelligence purposes.
Sec. 503. Pen register; trap and trace.
Sec. 504. Business records.
Sec. 505. Certain acquisitions inside the United States targeting United States persons outside the United States.

TITLE VI—PRIZE COMPETITION

Sec. 601. Findings.
Sec. 602. Definitions.
Sec. 603. Prize competition.
Sec. 604. Implementation.
Sec. 605. Judges.
Sec. 606. Report to Congress.
Sec. 607. Authorization of appropriations.
Sec. 608. Termination of authority.

TITLE VII—LAWFUL ACCESS TRAINING

Sec. 701. Lawful access training program.

TITLE VIII—EFFECTIVE DATE

Sec. 801. Effective date.

1  TITLE I—DATA AT REST

2 SEC. 101. DATA AT REST.

3 (a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:
§ 3119. Assistance orders to third parties and capability requirements

(a) DEFINITIONS.—In this section—

(1) the term ‘consumer electronic device’ means a device that—

(A) may be purchased by a member of the general public; and

(B) can be configured to store 1 gigabyte of data or more;

(2) the term ‘court of competent jurisdiction’ means—

(A) a district court of the United States (including a magistrate judge of such a court) or a United States court of appeals; and

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants;

(3) the term ‘device manufacturer’ means a person who designs, manufactures, fabricates, or assembles a finished consumer electronic device;

(4) the term ‘governmental entity’ has the meaning given the term in section 2711;

(5) the term ‘operating system provider’ means a person who designs, markets, or sells software that—
“(A) controls the operation of a consumer electronic device; and

“(B) directs the processing of programs on the consumer electronic device (such as by assigning storage space in memory and controlling input and output functions);

“(6) the term ‘remote computing service’ has the meaning given the term in section 2711; and

“(7) the term ‘State’ means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

“(b) COURT ORDER FOR ASSISTANCE.—

“(1) IN GENERAL.—A court of competent jurisdiction, in support of a search warrant based upon probable cause issued by the court that authorizes the search of an electronic device or remotely stored electronic information, shall, upon receiving a motion described in paragraph (3) that states reasonable grounds to believe that the assistance required by the order will aid in the execution of the warrant, order a device manufacturer, an operating system provider, a provider of remote computing service, or another person to furnish all information, facilities, and assistance necessary to access information
stored on an electronic device or to access remotely stored electronic information, as authorized by the search warrant.

“(2) ASSISTANCE.—The information, facilities, and assistance ordered to be furnished under paragraph (1) shall include—

“(A) isolating the information authorized to be searched;

“(B) decrypting or decoding information on the electronic device or remotely stored electronic information that is authorized to be searched, or otherwise providing such information in an intelligible format, unless the independent actions of an unaffiliated entity make it technically impossible to do so; and

“(C) providing technical support as necessary to ensure effective execution of the warrant for the electronic devices particularly described by the warrant.

“(3) MOTION.—An attorney for a governmental entity may move that the court issue an order under this subsection—

“(A) after a search warrant that authorizes the search of an electronic device or re-
motely stored electronic information has been
issued; or

“(B) concurrently with an application for a
search warrant described in subparagraph (A).

“(4) COMPENSATION AND EXEMPTION FROM LI-
ABILITY.—

“(A) IN GENERAL.—Subject to subpara-
graph (B), a device manufacturer, operating
system provider, provider of remote computing
service, or other person furnishing information,
facilities, or assistance pursuant to an order
issued under this subsection—

“(i) shall be compensated for reason-
able expenses directly incurred in com-
plying with the order; and

“(ii) may not be held civilly liable to
any party for any action taken that is rea-
sonably necessary to comply with the
order.

“(B) LIMITATION.—Reasonable expenses
under subparagraph (A) may not exceed $300.

“(c) CAPABILITY TO ASSIST.—

“(1) DEVICE MANUFACTURERS.—A device man-
ufacturer that sold more than 1,000,000 consumer
electronic devices in the United States in 2016 or
any calendar year thereafter, or that has received an assistance capability directive under section 3513, shall ensure that the manufacturer has the ability to provide the assistance described in subsection (b)(2) for any consumer electronic device that the manufacturer—

“(A) designs, manufactures, fabricates, or assembles; and

“(B) intends for sale or distribution in the United States.

“(2) PROVIDERS OF REMOTE COMPUTING SERVICE; OPERATING SYSTEM PROVIDERS.—A provider of remote computing service or operating system provider that provided service to more than 1,000,000 subscribers or users in the United States in 2016 or any calendar year thereafter, or that has received an assistance capability directive under section 3513, shall ensure that the provider has the ability to provide the assistance described in subparagraphs (A) and (B) of subsection (b)(2) for any remotely stored data that the provider processes or stores.

“(3) CONTRACTING AUTHORIZED.—A device manufacturer, provider of remote computing service, or operating system provider may satisfy the obligations under this subsection by contracting with any
other United States person or entity to provide the required assistance.

“(4) Costs.—A device manufacturer, provider of remote computing service, or operating system provider to which this subsection applies shall bear the costs associated with the development of the capability required under this subsection, including any contracting costs incurred by the device manufacturer, provider of remote computing service, or operating system provider under paragraph (3), unless the manufacturer or provider has received an assistance capability directive under section 3513.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—
The table of sections for chapter 205 of title 18, United States Code, is amended by adding at the end the following:

“3119. Assistance orders to third parties and capability requirements.”.

(c) APPLICABILITY.—The obligation under section 3119(c)(1) of title 18, United States Code, as added by subsection (a), shall apply with respect to a consumer electronic device manufactured on or after the effective date in section 801 of this Act.

TITLE II—DATA IN MOTION

SEC. 201. ASSISTANCE.

Section 2518(4) of title 18, United States Code, is amended, in the undesignated matter following paragraph
(e), by striking “with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.” and inserting the following: “in a manner designed to uphold the nondisclosure obligations under section 2511(2)(a)(ii).

Such furnishing of information, facilities, and technical assistance shall include—

“(i) isolating all communications authorized to be intercepted;

“(ii) decrypting, decoding, or otherwise providing in an intelligible format the communications authorized to be intercepted, unless the independent actions of an unaffiliated entity make it technically impossible to do so; and

“(iii) delivering all communications authorized to be intercepted securely, reliably, and concurrently with their transmission.
Any provider of wire or electronic communication service, landlord, custodian, or other person furnishing such information, facilities, or technical assistance shall be compensated therefor by the applicant for reasonable expenses directly incurred in providing such information, facilities, or assistance.”.

SEC. 202. CAPABILITY.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

“§ 2524. Capability requirements

“(a) IN GENERAL.—A provider of wire or electronic communication service that had more than 1,000,000 monthly active users in the United States in January 2016 or any month thereafter, or has received an assistance capability directive under section 3513, shall ensure that the provider has the ability to provide the information, facilities, and technical assistance described in section 2518(4).

“(b) CALCULATION OF MONTHLY ACTIVE USERS.—For purposes of subsection (a), the number of monthly active users of a wire or electronic communication service shall be calculated by taking the average of the number of individual users or subscribers of the service that are active per month in any calendar year.
“(c) COSTS.—A provider of wire or electronic communication service to which subsection (a) applies shall bear any costs associated with the development of the capability required under that subsection, unless the provider has received an assistance capability directive under section 3513.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 119 of title 18, United States Code, is amended by adding at the end the following:

“2524. Capability requirements.”.

SEC. 203. CALEA AMENDMENT.

(a) IN GENERAL.—Section 103(b)(3) of the Communications Assistance for Law Enforcement Act (47 U.S.C. 1002(b)(3)) is amended—

(1) by striking “, or ensuring the government’s ability to decrypt,”;

(2) by striking “the encryption was provided” and inserting “the means of encryption or other encoding was implemented by or facilitated”; and

(3) by striking “and the carrier possesses the information necessary to decrypt the communica-
TITLE III—ASSISTANCE
CAPABILITY DIRECTIVES

SEC. 301. ASSISTANCE CAPABILITY DIRECTIVES.

(a) In general.—Chapter 223 of title 18, United States Code, is amended by adding at the end the following:

“§3513. Assistance capability directives

“(a) Definitions.—The definitions in sections 2510 and 3119 shall apply to this section.

“(b) Contents of Directives and Procedure for Issuing.—

“(1) Authority.—

“(A) In general.—If the Attorney General makes the applicable finding with respect to a person under paragraph (3), the Attorney General may direct the person to create or maintain any of the assistance capabilities described in section 2518, 2524, 3119, 3127, or 3128.

“(B) Written directive.—A directive issued under subparagraph (A) shall be in writing.

“(2) Required reporting.—Not later than 30 days after the date on which a person receives a directive from the Attorney General under para-
graph (1), the person shall report to the Attorney General, or a designee of the Attorney General, on, at a minimum—

“(A) any technical capabilities that the person knows or expects to be necessary to implement and comply with an anticipated court order or other lawful authorization under section 2518, 3119, or 3123; and

“(B) the timeline of the person for developing and deploying the technical capabilities described in subparagraph (A).

“(3) FINDINGS.—The Attorney General may issue a directive to a person under paragraph (1) only if the Attorney General finds—

“(A) in the case of assistance capabilities described in section 2518, 2524, or 3128 that during the preceding calendar year, communications occurring over services the person offers, provides, or has access to were subject to not fewer than 5 court orders issued under—

“(i) chapter 119 of this title; or

“(ii) the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.); or
“(B) in the case of assistance capabilities described in section 3119, that, during the preceding calendar year, data stored in any device, service, or operating system sold or licensed by the person was subject to not fewer than 5 Federal or State search warrants.

“(4) Release from liability.—No civil cause of action shall lie in any court against a person who receives a directive under paragraph (1) for any action or omission reasonably necessary to comply with the directive.

“(5) Effective date and expiration date of directives.—

“(A) in general.—Subject to subparagraph (B), a directive issued under paragraph (1) shall contain—

“(i) a date on which the directive takes effect; and

“(ii) a date when the directive expires.

“(B) limits.—A directive issued under paragraph (1) may not—

“(i) take effect earlier than 180 days after the date on which the directive is issued; or
“(ii) expire later than 2 years after the date on which the directive takes effect.

“(6) REPORTING.—Not later than 30 days after the date on which a directive issued under paragraph (1) takes effect, the Attorney General shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a copy of the directive.

“(7) NO TECHNICAL DEMANDS.—A directive issued to a person under paragraph (1) may not specify technical means by which the person is required to implement the required capabilities.

“(c) CHALLENGES OF DIRECTIVES AND APPEAL.—

“(1) PETITION.—Not later than 30 days after the date on which the Attorney General issues a directive to a person under subsection (b), the person may file a petition to modify or set aside the directive in the United States District Court for the District of Columbia.

“(2) CONSIDERATION OF PETITION.—

“(A) GRANT.—The court may grant a petition filed under paragraph (1) only if—

“(i) the directive does not meet the requirements of this section;
“(ii) the person filing the petition demonstrates, by clear and convincing evidence, that it is technically impossible for the person to make any change to the way the hardware, software, or other property of the person behaves in order to comply with the directive; or

“(iii) the directive is otherwise unlawful.

“(B) DENIAL.—If none of the bases for granting a petition under subparagraph (A) are met, the court shall deny the petition.

“(C) EX PARTE REVIEW.—

“(i) IN GENERAL.—In considering a petition filed under paragraph (1), the court may review any information that the Attorney General, upon filing an affidavit under oath that disclosure of the information would harm the national security of the United States or harm the enforcement of criminal law, chooses to provide to the court solely for ex parte review.

“(ii) NO WAIVER OF PRIVILEGE.—The exercise of the authority under clause (i) does not waive any applicable privilege.
“(3) Initial review.—

“(A) Deadline.—Not later than 30 days after the date on which a petition is filed under paragraph (1), the court shall conduct an initial review of the petition.

“(B) Review.—If the court determines that the petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a non-frivolous argument for extending, modifying, or reversing existing law or for establishing new law, the court shall immediately—

“(i) deny the petition;

“(ii) affirm the directive or any part of the directive that is the subject of the petition; and

“(iii) order the recipient to comply with the directive or part thereof.

“(C) Written statement.—Upon making a determination under subparagraph (B) or promptly thereafter, the court shall provide a written statement for the record of the reasons for the determination.

“(4) Plenary review.—
“(A) DEADLINE.—If the court determines that a petition filed under paragraph (1) re-
quires plenary review—

“(i) not later than 60 days after the petition is filed, the court shall affirm,
modify, or set aside the directive that is the subject of the petition; or

“(ii) if the court does not set aside the directive by the date specified under clause (i), the court shall immediately, or in any event not later than 5 days there-
after—

“(I) affirm or affirm with modi-
fications the directive; and

“(II) order the person who re-
ceived the directive to comply with the directive in its entirety or as modified.

“(B) WRITTEN STATEMENT.—Upon mak-
ing a determination under subparagraph (A) or promptly thereafter, the court shall provide a written statement for the record of the reasons for the determination.

“(5) APPEALS.—

“(A) RIGHT OF APPEAL.—The Attorney General or a person who receives a directive
under subsection (b) may appeal a final order of the district court under this subsection not later than 30 days after entry of the order.

“(B) PROCEDURE.—The United States Court of Appeals for the District of Columbia Circuit shall expedite the consideration of any appeal brought under this paragraph, and the expense or effort required to comply with a directive issued under subsection (b) shall not be a basis for staying a final order of the district court under this subsection pending appeal.

“(d) ENFORCEMENT OF DIRECTIVES.—

“(1) FAILURE TO COMPLY.—If a person fails to comply with a directive issued under subsection (b), the Attorney General may file a petition for an order to compel the person to comply with the directive in the United States District Court for the District of Columbia, which shall have jurisdiction to review the petition.

“(2) EX PARTE REVIEW.—

“(A) IN GENERAL.—In considering a petition filed under paragraph (1), the court may review any information that the Attorney General, upon filing an affidavit under oath that disclosure of the information would harm the
national security of the United States or harm
the enforcement of criminal law, chooses to pro-
vide to the court solely for ex parte review.

“(B) NO WAIVER OF PRIVILEGE.—The ex-
ercise of the authority under subparagraph (A)
does not waive any applicable privilege.

“(3) ORDER TO COMPLY.—

“(A) IN GENERAL.—Not later than 30
days after a petition is filed under paragraph
(1), the court shall issue an order requiring the
person to comply with the directive or any part
of the directive, as issued or as modified, if the
court finds that the directive meets the require-
ments of this section and is otherwise lawful.

“(B) WRITTEN STATEMENT.—Upon mak-
ing a determination under subparagraph (A) or
promptly thereafter, the court shall provide a
written statement for the record of the reasons
for the determination.

“(4) PENALTY.—Failure to obey an order
issued under paragraph (3) shall constitute con-
tempt of court.

“(5) PROCESS.—Any process under this sub-
section may be served in any judicial district in
which the recipient may be found or does business.
“(6) APPEALS.—

“(A) RIGHT OF APPEAL.—The Attorney General or a person who receives a directive under subsection (b) may appeal a final order of the district court under this subsection not later than 30 days after entry of the order.

“(B) PROCEDURE.—The United States Court of Appeals for the District of Columbia Circuit shall expedite the consideration of any appeal brought under this paragraph, and the expense or effort required to comply with a directive issued under subsection (b) shall not be a basis for staying a final order of the district court order under this subsection pending appeal.

“(e) COST REIMBURSEMENT.—

“(1) IN GENERAL.—Subject to paragraph (3), a person who receives a directive under subsection (b) shall be compensated therefor by the United States for reasonable expenses directly incurred in complying with the directive.

“(2) AMOUNT.—The amount of compensation provided under paragraph (1)—
“(A) shall be mutually agreed upon by the Attorney General and the person complying with the directive; or

“(B) in the absence of an agreement under subparagraph (A), shall be determined by the United States District Court for the District of Columbia.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—
The table of sections for chapter 223 of title 18, United States Code, is amended by adding at the end the following:

“3513. Assistance capability directives.”.

TITLE IV—PEN REGISTER AND TRAP AND TRACE AMENDMENTS

SEC. 401. CAPABILITY REQUIREMENTS.

(a) IN GENERAL.—Chapter 206 of title 18, United States Code, is amended by adding at the end the following:

“§ 3128. Capability requirements

“(a) PEN REGISTER CAPABILITY.—

“(1) IN GENERAL.—A wire or electronic communication service provider that had more than 1,000,000 monthly active users in the United States in January 2016 or any month thereafter shall ensure that the provider has the ability to provide the information described in paragraphs (3) and (7) of
section 3127 directly to law enforcement agencies in
an intelligible format unobtrusively and in a manner
designed to uphold the nondisclosure obligations
under section 3123(d)(2).

“(2) Calculation of Monthly Active
Users.—For purposes of paragraph (1), the number
of monthly active users of a wire or electronic com-
munication service shall be calculated by taking the
average of the number of individual users or sub-
scribers of the service that are active per month in
any calendar year.

“(b) Trap and Trace Capability.—

“(1) In general.—A provider of wire or elec-
tronic communication service that had more than
1,000,000 monthly users in the United States in
January 2016 or any month thereafter shall ensure
that the provider has the ability to provide the infor-
mation described in paragraphs (4) and (7) of sec-
tion 3127 directly to law enforcement agencies in an
intelligible format unobtrusively and in a manner de-
signated to uphold the nondisclosure obligations under
section 3123(d)(2).

“(2) Calculation of Monthly Active
Users.—For purposes of paragraph (1), the number
of monthly active users of a wire or electronic com-
munication service shall be calculated by taking the average of the number of individual users or sub-
scribers of the service that are active per month in any calendar year.

“(c) COMPENSATION.—

“(1) IN GENERAL.—Subject to paragraph (2), a provider of wire or electronic communication service that provides the information described in paragraph (3), (4), or (7) of section 3127 directly to a law en-
forcement agency shall be compensated for reason-
able expenses directly incurred in providing the in-
formation.

“(2) LIMITATION.—Reasonable expenses under paragraph (1) may not exceed $150.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—
The table of sections for chapter 206 of title 18, United States Code, is amended by adding at the end the fol-
lowing:

“3128. Capability requirements.”.

SEC. 402. DEFINING TECHNICAL ASSISTANCE.

Section 3127 of title 18, United States Code, is amended—

(1) in paragraph (5), by striking “and” at the end;

(2) in paragraph (6), by striking the period at the end and inserting “; and”; and
(3) by adding at the end the following:

“(7) the term ‘technical assistance’ includes—

“(A) isolating all dialing, routing, addressing, and signaling information authorized to be acquired;

“(B) decrypting, decoding, or otherwise providing in an intelligible format the dialing, routing, addressing, and signaling information authorized to be acquired, unless the independent actions of an unaffiliated entity make it technically impossible to do so; and

“(C) delivering all dialing, routing, addressing, and signaling information authorized to be acquired securely, reliably, and concurrently with its transmission.”.

TITLE V—FISA AMENDMENTS
SEC. 501. ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES.

Title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) in section 101 (50 U.S.C. 1801), by adding at the end the following:

“(q) ‘Technical assistance’ includes—
“(1) isolating all communications or information authorized to be acquired;

“(2) decrypting, decoding, or otherwise providing in an intelligible format the communications or information authorized to be acquired, unless the independent actions of an unaffiliated entity make it technically impossible to do so; and

“(3) delivering all communications or information authorized to be acquired securely, reliably, and concurrently with their transmission.”; and

(2) in section 105(e)(2)(B), by striking “produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance” and inserting “in a manner designed to minimize the possibility of alerting the target whose communications are to be intercepted”.

SEC. 502. PHYSICAL SEARCHES WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES.

Title III of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1821 et seq.) is amended—

(1) in section 301 (50 U.S.C. 1821), by adding at the end the following:

“(6) ‘Assistance’ includes—
“(A) isolating all information, material, or property to be seized, reproduced, or altered;

“(B) decrypting, decoding, or otherwise providing in an intelligible format the information, material, or property to be seized, reproduced, or altered, unless the independent actions of an unaffiliated entity make it technically impossible to do so; and

“(C) providing technical support as necessary to ensure effective execution of an order under this title.”; and

(2) in section 304(c)(2)(B) (50 U.S.C. 1824(c)(2)(B)), by striking “produce a minimum of interference with the services that such landlord, custodian, or other person is providing the target of the physical search” and inserting “in a manner designed to minimize the possibility of alerting the target of the physical search”.

SEC. 503. PEN REGISTER; TRAP AND TRACE.

Section 401 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1841) is amended by adding at the end the following:

“(5) The term ‘technical assistance’ includes—
“(A) isolating all dialing, routing, addressing, and signaling information authorized to be acquired;

“(B) decrypting, decoding, or otherwise providing in an intelligible format the dialing, routing, addressing, and signaling information authorized to be acquired, unless the independent actions of an unaffiliated entity make it technically impossible to do so; and

“(C) delivering all dialing, routing, addressing, and signaling information authorized to be acquired securely, reliably, and concurrently with its transmission.”.

SEC. 504. BUSINESS RECORDS.

Section 501(k) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861(k)) is amended by adding at the end the following:

“(5) TECHNICAL ASSISTANCE.—The term ‘technical assistance’ includes—

“(A) isolating the tangible things (including call detail records) required to be produced;

“(B) decrypting, decoding, or otherwise providing in an intelligible format the tangible things required to be produced, unless the inde-
pendent actions of an unaffiliated entity make it technically impossible to do so; and

“(C) delivering all tangible things required to be produced securely, reliably, and no later than the date on which an order under this title requires their production.”.

SEC. 505. CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

Section 703 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881b) is amended by adding at the end the following:

“(h) ASSISTANCE DEFINED.— For purposes of this section, the term ‘assistance’ includes—

“(1) isolating all communications or information authorized to be acquired;

“(2) decrypting, decoding, or otherwise providing in an intelligible format the communications or information authorized to be acquired, unless the independent actions of an unaffiliated entity make it technically impossible to do so;

“(3) delivering the communications or information authorized to be acquired securely, reliably, and concurrently with their transmission; and
“(4) providing technical support as necessary to ensure effective execution of an order under this section.”

TITLE VI—PRIZE COMPETITION

SEC. 601. FINDINGS.

Congress finds the following:

(1) The rapidly growing use of warrant-proof encryption in everyday devices, platforms, and systems allows illegal actors engaged in dangerous criminal activity—including child sexual abuse, terrorism, and international narcotics trafficking—to use encryption to shield their illicit activities from authorities.

(2) Because of warrant-proof encryption, the government often cannot obtain the electronic evidence and intelligence necessary to investigate and prosecute threats to public safety and national security, even with a warrant or court order. This provides a “lawless space” that criminals, terrorists, and other bad actors can exploit for their nefarious ends.

(3) Many service providers, device manufacturers, and application developers who use encryption fail to implement technology that would allow the government to obtain electronic evidence necessary
to investigate and prosecute threats to public safety
and national security.

(4) The Fourth Amendment to the Constitution
of the United States strikes a balance between the
individual citizen’s reasonable expectation of privacy
on one hand, and on the other, the legitimate need
for the government to gain access to the most inti-
mate spaces in citizens’ lives in order to protect the
public from criminal actors.

(5) The Framers of the Constitution provided
specific barriers to government intrusion into the in-
dividual’s private, intimate space—namely, that the
government must show by probable cause that evi-
dence of a crime exists in that intimate space, and
must have a neutral magistrate, detached from the
law enforcement interest, approve law enforcement’s
request and issue a warrant.

(6) Once the government satisfies the burden of
showing probable cause to a neutral magistrate, the
government is entitled to search and seize evidence
of a crime in an individual’s private space.

(7) That careful balancing of interests estab-
lished by the Framers has continued to be calibrated
throughout the history of the United States as dif-
ferent challenges have arisen, including, most nota-
bly, technological advances in daily life. For example, Congress has imposed additional statutory requirements that the government must meet and that a judge must find satisfied before a court can authorize interception of communications. But the individual’s right to privacy has never been absolute.

(8) If not addressed, criminal anonymity activated by end-to-end encryption technology will continue to pose a serious risk to the public.

(9) Nevertheless, advances in technology continue without due consideration of issues of lawful access.

(10) Moreover, very little, if any, resources from the private sector or from educational and research institutions are devoted to finding technological solutions to providing lawful access within different encrypted technological platforms.

(11) More resources should be devoted to incentivizing the best minds in the United States to research the issues described in this section and decide how to best provide the most secure products and services to customers while also providing law enforcement access to information the government needs to investigate criminals seeking to do the public harm and to protect national security.
SEC. 602. DEFINITIONS.

In this title:

(1) APPLICANT.—The term “applicant” means an individual, group of individuals, organization, nonprofit, or university that applies to participate in the prize competition under this title.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

(3) ATTORNEY GENERAL.—Except as otherwise provided, the term “Attorney General” means the Attorney General, acting through the Director of the National Institute of Justice.

(4) PRIZE.—The term “prize” means a cash prize.

(5) PRIZE COMPETITION.—The term “prize competition” means the prize competition established under section 603.

SEC. 603. PRIZE COMPETITION.

(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall, subject to the availability of funds appropriated under this title, establish in accordance with section 24

(1) to incentivize and encourage research and innovation into solutions providing law enforcement access to encrypted data pursuant to legal process; and

(2) to award 1 or more prizes, not later than 1 year after the establishment of the prize competition, for technological solutions that provide law enforcement access to encrypted data pursuant to legal process.

(b) REQUIREMENTS.—Technological solutions described in subsection (a)(2) shall include—

(1) providing maximum security for the device, platform, or system, consistent with the lawful access solution, to reduce the opportunity for unlawful hacking; and

(2) reducing or eliminating broad surveillance capabilities not targeted at specified facilities or individuals pursuant to a warrant or order within the lawful access solution.

(c) ELIGIBILITY.—

(1) IN GENERAL.—To be eligible to win a prize under the prize competition, an applicant—

(A) shall have complied with—
(i) the requirements of the competition as described in the announcement for the competition; and

(ii) subsections (g), (h), and (i) of section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719) (relating to eligibility);

(B) in the case of a private entity, shall be incorporated in the United States and maintain a primary place of business in the United States; and

(C) in the case of an individual, whether participating singly or in a group, shall be a citizen of, or an alien lawfully admitted for permanent residence in, the United States.

(2) Exclusions.—The following entities and individuals shall not be eligible to win a prize under the prize competition:

(A) A Federal entity.

(B) A Federal employee acting within the scope of employment.

(d) Prioritization.—In selecting the winner or winners of the prize competition, the Attorney General shall give priority to projects that—
(1) incorporate a robust proof of concept model demonstrating the feasibility of the proposed technology achieving the intended goals of the competition as described in paragraph (a); and

(2) include a strategy, submitted with the application or proposal, to move the new technology, hardware, or other processes to market-scale deployment.

SEC. 604. IMPLEMENTATION.

(a) DUTIES.—In implementing the prize competition, the Attorney General shall—

(1) advertise the prize competition;

(2) solicit participants;

(3) use amounts made available under section 607(a)—

(A) to administer the prize competition;

and

(B) to award 1 or more prizes;

(4) develop criteria for the selection of winners;

(5) select judges under section 605 based on criteria developed by the Attorney General;

(6) announce, and award a prize to, 1 or more winners;
(7) protect against unauthorized use or disclosure of any trade secret or confidential business information of a participant; and

(8) promulgate any rules and regulations necessary to carry out this title, including rules and regulations for submitting and reviewing applications.

(b) AWARD.—

(1) RECOMMENDATION BY JUDGES.—After conducting a thorough review of each of the applicant submissions for the prize competition, the judges appointed under section 605 shall—

(A) submit in writing to the Attorney General a recommendation for an award to 1 or more winners of the prize competition; or

(B) if the judges determine that none of the applicant submissions merit an award, submit in writing to the Attorney General a recommendation that no applicant be awarded a prize, including a detailed explanation stating the reasons why no applicant merits an award.

(2) SELECTION BY ATTORNEY GENERAL.—

(A) IN GENERAL.—Not later than 1 year after the date on which the Attorney General establishes the prize competition, and after re-
viewing the recommendation submitted under paragraph (1), the Attorney General shall select 1 or more winners of the prize competition and award a prize to each winner.

(B) Recommendation of no prize.—If the judges recommend under paragraph (1)(B) that no applicant be awarded a prize, the Attorney General may—

(i) select 1 or more award winners, notwithstanding the recommendation of the judges, and award a prize to each winner; or

(ii) award no prize to any applicant.

(C) Notification of no prize.—If the Attorney General determines not to award a prize to any applicant under subparagraph (B)(ii), the Attorney General shall notify the appropriate congressional committees not later than 90 days after that determination.

(c) Assistance from Other Parties.—

(1) Administration by third party organization.—

(A) In general.—The Attorney General may enter into an agreement, including a grant, contract, or cooperative agreement, with a non-
profit or for-profit third party organization, under which the third-party organization administers the prize competition.

(B) Consultation; Division of Authority.—If the Attorney General enters into a contract with a third party organization under subparagraph (A), the third party organization shall consult with the Attorney General on, and the Attorney General shall have the authority to make the final decision with respect to—

(i) the development of criteria for the selection of prize competition winners under subsection (a)(4); and

(ii) the selection of judges under section 605.

(2) Non-Federal Funds.—The Attorney General may solicit and receive non-Federal funds to administer the prize competition and award a prize.

SEC. 605. JUDGES.

(a) Appointment.—The Attorney General shall appoint not fewer than 3 judges who shall, except as provided in section 604(b)(1)(B), recommend 1 or more winners of the prize competition.

(b) Qualifications.—Each judge appointed under subsection (a) shall—
(1) have subject matter expertise in cryptology and encryption-related technology, including relevant devices, platforms, and systems;

(2) have an understanding of—

(A) protections afforded to United States citizens by the Constitution of the United States against unreasonable searches and seizures by the government; and

(B) the legal authorities that permit the government to search and seize the personal effects of United States citizens, particularly with respect to—

(i) the search and seizure of individuals’ data from technological devices, platforms, or systems; and

(ii) the interception of communications over technological devices, platforms, or systems; and

(3) have experience with law enforcement capabilities for lawful access to data and limitations on lawful access to data across various technological devices, platforms, and systems that use encrypted technology.
SEC. 606. REPORT TO CONGRESS.

Not later than 90 days after the date on which the Attorney General awards 1 or more prizes under section 604(b)(2), the Attorney General shall submit to the appropriate congressional committees a report on the prize competition that includes—

(1) a statement by the Attorney General that describes the activities carried out by the Attorney General with respect to the duties described in section 604(a);

(2) if the Attorney General has entered into an agreement with a third party organization under section 604(c)(1), a statement by the Attorney General that describes the activities carried out by the third party organization with respect to the duties described in section 604(c); and

(3) a statement by the Attorney General explaining the basis on which each winner of the prize competition was selected.

SEC. 607. AUTHORIZATION OF APPROPRIATIONS.

(a) Authorization.—

(1) IN GENERAL.—There are authorized to be appropriated such sums as may be necessary, not to exceed $50,000,000, to carry out this title.

(2) MINIMIZATION OF ADMINISTRATIVE EXPENSES.—The Attorney General shall make all rea-
reasonable efforts to control the administrative expenses of the prize competition so that the majority of the amounts made available under paragraph (1) are used for the prize or prizes awarded to the winner or winners of the prize competition under section 603.

(b) Approval of Certain Awards.—The value of a prize awarded to a winner of the prize competition under section 603 may not exceed $1,000,000 without the approval of the Attorney General or the Director of the National Institute of Justice.

(c) Reimbursement of Expenses.—A judge appointed under section 605 shall serve without pay, but may be reimbursed for actual and necessary traveling and subsistence expenses.

SEC. 608. TERMINATION OF AUTHORITY.

The prize competition and all authority provided under this title shall terminate on December 31, 2022.

TITLE VII—LAWFUL ACCESS TRAINING

SEC. 701. LAWFUL ACCESS TRAINING PROGRAM.

(a) Definitions.—In this section:

(1) Cooperative agreement.—The term “cooperative agreement” means a legal instrument of financial assistance between a Federal awarding agen-
cy or pass-through entity and a non-Federal entity, consistent with sections 6302 and 6305 of title 31, United States Code.

(2) PROVIDER.—The term “provider” means—

(A) a device manufacturer, an operating system provider, and a provider of remote computing service, as those terms are defined in section 3119 of title 18, United States Code, as added by title I of this Act; and

(B) a provider of electronic communication service, as defined in section 2510 of title 18, United States Code.

(3) TRAINING PROGRAM.—The term “Training Program” means the lawful access training and assistance program established under subsection (b).

(b) ESTABLISHMENT.—The Attorney General shall establish a lawful access training and real-time assistance program that draws upon the resources of the National Domestic Communications Center (commonly known as the “NDCAC”) and other relevant components of the Department of Justice as appropriate.

(c) ACTIVITIES.—

(1) TRAINING.—

(A) IN GENERAL.—The primary purpose of the Training Program shall be to provide train-
ing and assistance for law enforcement personnel, with a particular emphasis on State and local personnel, on relevant technology and communications platforms, including how to submit appropriately tailored applications for digital evidence, consistent with existing legal requirements and protections for privacy and civil liberties.

(B) CONSULTATION.—The Attorney General may consult with providers regarding the training and assistance under subparagraph (A).

(C) CONTENTS.—Training and assistance under the Training Program shall include—

(i) designing and providing training to distribute knowledge and expertise, including—

(I) consulting with the most qualified experts in law enforcement and the technology industry to assist in the development of all Training Program materials;

(II) identifying current effective law enforcement training programs and tools;
(III) identifying gaps in current law enforcement training programs and tools;

(IV) producing and maintaining training materials and curricula that will be used in classroom training sessions as well as for distribution to law enforcement agencies for reference;

(V) in coordination with providers, delivering information and guidance on accessing digital evidence from specific providers to improve outcomes with regard to particular technology devices, platforms, or systems; and

(VI) establishing and promoting the use of a consistent set of clear standards for securing and minimizing data collected by law enforcement;

(ii) serving as a centralized repository of knowledge and expertise about provider systems and procedures for submitting requests for data;

(iii) coordinating with Federal, State, and international training programs, as
well as any private-sector and nonprofit
initiatives;

(iv) building and maintaining analytic
and forensic tools to assist law enforce-
ment agencies in interpreting data that has
been obtained from service providers and
devices;

(v) hiring and employing technical
specialists that can help develop and main-
tain analytic and forensic tools;

(vi) conducting relevant research and
analysis to identify the greatest challenges
with respect to the ability of law enforce-
ment agencies to access and analyze digital
evidence; and

(vii) providing a call center for law en-
forcement officials to seek advice and ass-
sistance regarding accessing and analyzing
digital evidence.

(2) OTHER FUNCTIONS.—In carrying out the
Training Program, the Attorney General shall de-
velop and coordinate additional functions to improve
lawful access to digital evidence, including the fol-
lowing:
(A) IDENTIFYING AND PROVIDING RESOURCES.—The Attorney General shall—

(i) work with the Office of Justice Programs to identify grants and other grant-making bodies to support law enforcement access to digital evidence; and

(ii) include programs in the training activities that inform law enforcement agencies of the grants described in clause (i) and other resources that support—

(I) training programs;

(II) development and distribution of analytical tools; and

(III) maintenance of crime labs.

(B) DEVELOPMENT OF AUTHENTICATION SYSTEM.—The Attorney General shall work with providers and law enforcement agencies from Federal, State, and local systems to identify options for, and develop, a system for verifying that an individual requesting data from a provider is a law enforcement official entitled to such access pursuant to lawful authority.
48

(C) Coordinating international efforts.—The Attorney General shall coordinate with international partners to—

(i) help set baseline standards and practices to lawfully access digital evidence;

(ii) promote standards to ensure the protection of privacy and civil liberties, and to the extent practical and helpful, harmonize efforts across borders.

(D) Developing master database.—

The Attorney General shall—

(i) develop a master database to track investigations in the United States in which a law enforcement agency secured the legal authority to access digital data but otherwise cannot gain access to that data in an intelligible format due to encryption; and

(ii) through the training activities described in paragraph (1), encourage the robust participation from State and local authorities that is necessary to populate the database described in clause (i) of this subparagraph.
(E) Other Activities.—The Attorney General, in carrying out the Training Program, shall provide any additional activities and services determined appropriate by the Attorney General.

(d) Funding.—

(1) Authorization of Appropriations.—There is authorized to be appropriated to the Attorney General to carry out this section $50,000,000 for fiscal year 2020, which shall remain available until expended.

(2) Limitation.—Not more than 5 percent of the amount appropriated under paragraph (1) may be used to carry out activities under subsection (e)(2).

(e) Cooperative Agreement.—

(1) Assistance.—The Attorney General may enter into a cooperative agreement with providers or other persons to—

(A) provide regular training to law enforcement agencies through the Training Program on information that is potentially available from devices, operating systems, remote computing services, or electronic communication services, and on provider policies, in order to facilitate
tailed and specific applications from law en-
forcement agencies;

(B) maintain up-to-date and comprehen-
sive guidance for law enforcement agencies re-
garding accessing information from providers;

(C) develop or maintain online mechanisms
to—

(i) receive law enforcement requests
for data; and

(ii) provide dated, electronic confirma-
tion of receipt of a request described in
clause (i); and

(D) assist with other tasks as determined
necessary by the NDCAC.

(2) DONATIONS.—

(A) IN GENERAL.—The NDCAC may so-
llicit and accept donations for the Training Pro-
gram from providers or other persons to be
used to carry out this section.

(B) PRIVATE FUNDING REQUIREMENT.—
The NDCAC may not carry out the Training
Program during a fiscal year, including fiscal
year 2020, unless and until the NDCAC has re-
ceived funding for that fiscal year under sub-
paragraph (A) in an amount equal to the
amount authorized to be appropriated for fiscal year 2020 under subsection (d)(1).

(f) Report.—

(1) In general.—Not later than 1 year after the effective date in section 801 of this Act, and once thereafter not later than 2 years after that effective date, the NDCAC shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report on the Training Program.

(2) Contents.— The report submitted under paragraph (1) shall include—

(A) ongoing efforts to identify and respond to gaps in training and distribution of technical tools;

(B) the state of cooperation with providers;

(C) novel uses of legal authorities;

(D) any new policies and best practices being seriously considered or adopted; and

(E) funding contributed by private individuals, organizations, and entities.
TITLE VIII—EFFECTIVE DATE

SEC. 801. EFFECTIVE DATE.

Titles I through V of this Act, and the amendments made by those titles, shall take effect 1 year after the date of enactment of this Act.