

pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) ENFORCEMENT UPON APPLICATION BY ATTORNEY GENERAL.—The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) CIVIL PENALTY.—

(1) IN GENERAL.—A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to \$10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

(2) CONSIDERATIONS.—In determining whether to impose a civil penalty and in determining its amount, the court shall take into account—

(A) the nature, circumstances, and extent of the violation;

(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

(C) such other matters as justice may require.

(d) DEFINITIONS.—As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

(Added Pub. L. 103-414, title II, §201(a), Oct. 25, 1994, 108 Stat. 4289.)

#### Editorial Notes

##### REFERENCES IN TEXT

The Foreign Intelligence Surveillance Act of 1978, referred to in subsec. (a), is Pub. L. 95-511, Oct. 25, 1978, 92 Stat. 1783, as amended, which is classified principally to chapter 36 (§1801 et seq.) of Title 50, War and National Defense. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of Title 50 and Tables.

The Communications Assistance for Law Enforcement Act, referred to in subsections (a) and (b), is title I of Pub. L. 103-414, Oct. 25, 1994, 108 Stat. 4279, which is classified generally to subchapter I (§1001 et seq.) of chapter 9 of Title 47, Telecommunications. Sections 102 and 108 of the Act are classified to sections 1001 and 1007, respectively, of Title 47. For complete classifica-

tion of this Act to the Code, see Short Title note set out under section 1001 of Title 47 and Tables.

#### § 2523. Executive agreements on access to data by foreign governments

(a) DEFINITIONS.—In this section—

(1) the term “lawfully admitted for permanent residence” has the meaning given the term in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)); and

(2) the term “United States person” means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States.

(b) EXECUTIVE AGREEMENT REQUIREMENTS.—For purposes of this chapter, chapter 121, and chapter 206, an executive agreement governing access by a foreign government to data subject to this chapter, chapter 121, or chapter 206 shall be considered to satisfy the requirements of this section if the Attorney General, with the concurrence of the Secretary of State, determines, and submits a written certification of such determination to Congress, including a written certification and explanation of each consideration in paragraphs (1), (2), (3), and (4), that—

(1) the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, if—

(A) such a determination under this section takes into account, as appropriate, credible information and expert input; and

(B) the factors to be met in making such a determination include whether the foreign government—

(i) has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated by being a party to the Convention on Cybercrime, done at Budapest November 23, 2001, and entered into force January 7, 2004, or through domestic laws that are consistent with definitions and the requirements set forth in chapters I and II of that Convention;

(ii) demonstrates respect for the rule of law and principles of nondiscrimination;

(iii) adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights, including—

(I) protection from arbitrary and unlawful interference with privacy;

(II) fair trial rights;

(III) freedom of expression, association, and peaceful assembly;

(IV) prohibitions on arbitrary arrest and detention; and

(V) prohibitions against torture and cruel, inhuman, or degrading treatment or punishment;

(iv) has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities;

(v) has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government; and

(vi) demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet;

(2) the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement;

(3) the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data; and

(4) the agreement requires that, with respect to any order that is subject to the agreement—

(A) the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement;

(B) the foreign government may not target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States;

(C) the foreign government may not issue an order at the request of or to obtain information to provide to the United States Government or a third-party government, nor shall the foreign government be required to share any information produced with the United States Government or a third-party government;

(D) an order issued by the foreign government—

(i) shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

(ii) shall identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order;

(iii) shall be in compliance with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law;

(iv) shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;

(v) shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in

proceedings regarding, enforcement of the order; and

(vi) in the case of an order for the interception of wire or electronic communications, and any extensions thereof, shall require that the interception order—

(I) be for a fixed, limited duration; and

(II) may not last longer than is reasonably necessary to accomplish the approved purposes of the order; and

(III) be issued only if the same information could not reasonably be obtained by another less intrusive method;

(E) an order issued by the foreign government may not be used to infringe freedom of speech;

(F) the foreign government shall promptly review material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those persons trained in applicable procedures;

(G) the foreign government shall, using procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily harm to any person;

(H) the foreign government may not disseminate the content of a communication of a United States person to United States authorities unless the communication may be disseminated pursuant to subparagraph (G) and relates to significant harm, or the threat thereof, to the United States or United States persons, including crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud;

(I) the foreign government shall afford reciprocal rights of data access, to include, where applicable, removing restrictions on communications service providers, including providers subject to United States jurisdiction, and thereby allow them to respond to valid legal process sought by a governmental entity (as defined in section 2711) if foreign law would otherwise prohibit communications-service providers from disclosing the data;

(J) the foreign government shall agree to periodic review of compliance by the foreign government with the terms of the agreement to be conducted by the United States Government; and

(K) the United States Government shall reserve the right to render the agreement inapplicable as to any order for which the United States Government concludes the agreement may not properly be invoked.

(c) LIMITATION ON JUDICIAL REVIEW.—A determination or certification made by the Attorney

General under subsection (b) shall not be subject to judicial or administrative review.

(d) EFFECTIVE DATE OF CERTIFICATION.—

(1) NOTICE.—Not later than 7 days after the date on which the Attorney General certifies an executive agreement under subsection (b), the Attorney General shall provide notice of the determination under subsection (b) and a copy of the executive agreement to Congress, including—

(A) the Committee on the Judiciary and the Committee on Foreign Relations of the Senate; and

(B) the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives.

(2) ENTRY INTO FORCE.—An executive agreement that is determined and certified by the Attorney General to satisfy the requirements of this section shall enter into force not earlier than the date that is 180 days after the date on which notice is provided under paragraph (1), unless Congress enacts a joint resolution of disapproval in accordance with paragraph (4).

(3) REQUESTS FOR INFORMATION.—Upon request by the Chairman or Ranking Member of a congressional committee described in paragraph (1), the head of an agency shall promptly furnish a summary of factors considered in determining that the foreign government satisfies the requirements of this section.

(4) CONGRESSIONAL REVIEW.—

(A) JOINT RESOLUTION DEFINED.—In this paragraph, the term “joint resolution” means only a joint resolution—

(i) introduced during the 180-day period described in paragraph (2);

(ii) which does not have a preamble;

(iii) the title of which is as follows: “Joint resolution disapproving the executive agreement signed by the United States and \_\_\_\_\_”, the blank space being appropriately filled in; and

(iv) the matter after the resolving clause of which is as follows: “That Congress disapproves the executive agreement governing access by \_\_\_\_\_ to certain electronic data as submitted by the Attorney General on \_\_\_\_\_”, the blank spaces being appropriately filled in.

(B) JOINT RESOLUTION ENACTED.—Notwithstanding any other provision of this section, if not later than 180 days after the date on which notice is provided to Congress under paragraph (1), there is enacted into law a joint resolution disapproving of an executive agreement under this section, the executive agreement shall not enter into force.

(C) INTRODUCTION.—During the 180-day period described in subparagraph (B), a joint resolution of disapproval may be introduced—

(i) in the House of Representatives, by the majority leader or the minority leader; and

(ii) in the Senate, by the majority leader (or the majority leader’s designee) or the minority leader (or the minority leader’s designee).

(5) FLOOR CONSIDERATION IN HOUSE OF REPRESENTATIVES.—If a committee of the House of Representatives to which a joint resolution of disapproval has been referred has not reported the joint resolution within 120 days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

(6) CONSIDERATION IN THE SENATE.—

(A) COMMITTEE REFERRAL.—A joint resolution of disapproval introduced in the Senate shall be referred jointly—

(i) to the Committee on the Judiciary; and

(ii) to the Committee on Foreign Relations.

(B) REPORTING AND DISCHARGE.—If a committee to which a joint resolution of disapproval was referred has not reported the joint resolution within 120 days after the date of referral of the joint resolution, that committee shall be discharged from further consideration of the joint resolution and the joint resolution shall be placed on the appropriate calendar.

(C) PROCEEDING TO CONSIDERATION.—It is in order at any time after both the Committee on the Judiciary and the Committee on Foreign Relations report a joint resolution of disapproval to the Senate or have been discharged from consideration of such a joint resolution (even though a previous motion to the same effect has been disagreed to) to move to proceed to the consideration of the joint resolution, and all points of order against the joint resolution (and against consideration of the joint resolution) are waived. The motion is not debatable or subject to a motion to postpone. A motion to reconsider the vote by which the motion is agreed to or disagreed to shall not be in order.

(D) CONSIDERATION IN THE SENATE.—In the Senate, consideration of the joint resolution, and on all debatable motions and appeals in connection therewith, shall be limited to not more than 10 hours, which shall be divided equally between those favoring and those opposing the joint resolution. A motion further to limit debate is in order and not debatable. An amendment to, or a motion to postpone, or a motion to proceed to the consideration of other business, or a motion to recommit the joint resolution is not in order.

(E) CONSIDERATION OF VETO MESSAGES.—Debate in the Senate of any veto message with respect to a joint resolution of disapproval, including all debatable motions and appeals in connection with the joint resolution, shall be limited to 10 hours, to be equally divided between, and controlled by, the majority leader and the minority leader or their designees.

(7) RULES RELATING TO SENATE AND HOUSE OF REPRESENTATIVES.—

(A) TREATMENT OF SENATE JOINT RESOLUTION IN HOUSE.—In the House of Representatives, the following procedures shall apply to a joint resolution of disapproval received

from the Senate (unless the House has already passed a joint resolution relating to the same proposed action):

(i) The joint resolution shall be referred to the appropriate committees.

(ii) If a committee to which a joint resolution has been referred has not reported the joint resolution within 7 days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

(iii) Beginning on the third legislative day after each committee to which a joint resolution has been referred reports the joint resolution to the House or has been discharged from further consideration thereof, it shall be in order to move to proceed to consider the joint resolution in the House. All points of order against the motion are waived. Such a motion shall not be in order after the House has disposed of a motion to proceed on the joint resolution. The previous question shall be considered as ordered on the motion to its adoption without intervening motion. The motion shall not be debatable. A motion to reconsider the vote by which the motion is disposed of shall not be in order.

(iv) The joint resolution shall be considered as read. All points of order against the joint resolution and against its consideration are waived. The previous question shall be considered as ordered on the joint resolution to final passage without intervening motion except 2 hours of debate equally divided and controlled by the sponsor of the joint resolution (or a designee) and an opponent. A motion to reconsider the vote on passage of the joint resolution shall not be in order.

(B) TREATMENT OF HOUSE JOINT RESOLUTION IN SENATE.—

(i) If, before the passage by the Senate of a joint resolution of disapproval, the Senate receives an identical joint resolution from the House of Representatives, the following procedures shall apply:

(I) That joint resolution shall not be referred to a committee.

(II) With respect to that joint resolution—

(aa) the procedure in the Senate shall be the same as if no joint resolution had been received from the House of Representatives; but

(bb) the vote on passage shall be on the joint resolution from the House of Representatives.

(ii) If, following passage of a joint resolution of disapproval in the Senate, the Senate receives an identical joint resolution from the House of Representatives, that joint resolution shall be placed on the appropriate Senate calendar.

(iii) If a joint resolution of disapproval is received from the House, and no companion joint resolution has been introduced in the Senate, the Senate procedures under this subsection shall apply to the House joint resolution.

(C) APPLICATION TO REVENUE MEASURES.—The provisions of this paragraph shall not apply in the House of Representatives to a joint resolution of disapproval that is a revenue measure.

(8) RULES OF HOUSE OF REPRESENTATIVES AND SENATE.—This subsection is enacted by Congress—

(A) as an exercise of the rulemaking power of the Senate and the House of Representatives, respectively, and as such is deemed a part of the rules of each House, respectively, and supersedes other rules only to the extent that it is inconsistent with such rules; and

(B) with full recognition of the constitutional right of either House to change the rules (so far as relating to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House.

(e) RENEWAL OF DETERMINATION.—

(1) IN GENERAL.—The Attorney General, with the concurrence of the Secretary of State, shall review and may renew a determination under subsection (b) every 5 years.

(2) REPORT.—Upon renewing a determination under subsection (b), the Attorney General shall file a report with the Committee on the Judiciary and the Committee on Foreign Relations of the Senate and the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives describing—

(A) the reasons for the renewal;

(B) any substantive changes to the agreement or to the relevant laws or procedures of the foreign government since the original determination or, in the case of a second or subsequent renewal, since the last renewal; and

(C) how the agreement has been implemented and what problems or controversies, if any, have arisen as a result of the agreement or its implementation.

(3) NONRENEWAL.—If a determination is not renewed under paragraph (1), the agreement shall no longer be considered to satisfy the requirements of this section.

(f) REVISIONS TO AGREEMENT.—A revision to an agreement under this section shall be treated as a new agreement for purposes of this section and shall be subject to the certification requirement under subsection (b), and to the procedures under subsection (d), except that for purposes of a revision to an agreement—

(1) the applicable time period under paragraphs (2), (4)(A)(i), (4)(B), and (4)(C) of subsection (d) shall be 90 days after the date notice is provided under subsection (d)(1); and

(2) the applicable time period under paragraphs (5) and (6)(B) of subsection (d) shall be 60 days after the date notice is provided under subsection (d)(1).

(g) PUBLICATION.—Any determination or certification under subsection (b) regarding an executive agreement under this section, including any termination or renewal of such an agreement, shall be published in the Federal Register as soon as is reasonably practicable.

(h) **MINIMIZATION PROCEDURES.**—A United States authority that receives the content of a communication described in subsection (b)(4)(H) from a foreign government in accordance with an executive agreement under this section shall use procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) to appropriately protect nonpublicly available information concerning United States persons.

(Added Pub. L. 115–141, div. V, §105(a), Mar. 23, 2018, 132 Stat. 1217.)

#### Statutory Notes and Related Subsidiaries

##### CONGRESSIONAL FINDINGS

Pub. L. 115–141, div. V, §102, Mar. 23, 2018, 132 Stat. 1213, provided that: “Congress finds the following:

“(1) Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism.

“(2) Such efforts by the United States Government are being impeded by the inability to access data stored outside the United States that is in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States.

“(3) Foreign governments also increasingly seek access to electronic data held by communications-service providers in the United States for the purpose of combating serious crime.

“(4) Communications-service providers face potential conflicting legal obligations when a foreign government orders production of electronic data that United States law may prohibit providers from disclosing.

“(5) Foreign law may create similarly conflicting legal obligations when chapter 121 of title 18, United States Code (commonly known as the ‘Stored Communications Act’), requires disclosure of electronic data that foreign law prohibits communications-service providers from disclosing.

“(6) International agreements provide a mechanism for resolving these potential conflicting legal obligations where the United States and the relevant foreign government share a common commitment to the rule of law and the protection of privacy and civil liberties.”

#### CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec.	
2701.	Unlawful access to stored communications.
2702.	Voluntary disclosure of customer communications or records.
2703.	Required disclosure of customer communications or records.
2704.	Backup preservation.
2705.	Delayed notice.
2706.	Cost reimbursement.
2707.	Civil action.
2708.	Exclusivity of remedies.
2709.	Counterintelligence access to telephone toll and transactional records.
2710.	Wrongful disclosure of video tape rental or sale records.
2711.	Definitions for chapter.
2712.	Civil actions against the United States.
2713.	Required preservation and disclosure of communications and records.

#### Editorial Notes

##### AMENDMENTS

2018—Pub. L. 115–141, div. V, §103(a)(2), Mar. 23, 2018, 132 Stat. 1214, added item 2713.

2002—Pub. L. 107–273, div. B, title IV, §4005(b), Nov. 2, 2002, 116 Stat. 1812, made technical correction to directory language of Pub. L. 107–56, title II, §223(c)(2), Oct. 26, 2001, 115 Stat. 295, effective Oct. 26, 2001. See 2001 Amendment note below.

2001—Pub. L. 107–56, title II, §§223(c)(2), 224, Oct. 26, 2001, 115 Stat. 295, as amended by Pub. L. 107–273, div. B, title IV, §4005(b), Nov. 2, 2002, 116 Stat. 1812, temporarily added item 2712.

Pub. L. 107–56, title II, §§212(a)(2), (b)(2), 224, Oct. 26, 2001, 115 Stat. 285, 295, temporarily substituted “Voluntary disclosure of customer communications or records” for “Disclosure of contents” in item 2702 and “Required disclosure of customer communications or records” for “Requirements for governmental access” in item 2703.

1988—Pub. L. 100–690, title VII, §7067, Nov. 18, 1988, 102 Stat. 4405, which directed amendment of item 2710 by inserting “for chapter” after “Definitions” was executed by making the insertion in item 2711 to reflect the probable intent of Congress and the intervening redesignation of item 2710 as 2711 by Pub. L. 100–618, see below.

Pub. L. 100–618, §2(b), Nov. 5, 1988, 102 Stat. 3197, added item 2710 and redesignated former item 2710 as 2711.

#### § 2701. Unlawful access to stored communications

(a) **OFFENSE.**—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) **PUNISHMENT.**—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case—

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) **EXCEPTIONS.**—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or