order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99–508, set out as a note under section 2510 of this title.

EFFECTIVE DATE OF 1970 AMENDMENT

Amendment by Pub. L. 91–358 effective on first day of seventh calendar month which begins after July 29, 1970, see section 901(a) of Pub. L. 91–358.

RULE OF CONSTRUCTION

Pub. L. 115–141, div. V, §106, Mar. 23, 2018, 132 Stat. 1224, provided that: ''Nothing in this division [see section 101 of Pub. L. 115–141, set out as a Short Title of 2018 Amendment note under section 1 of this title], or the amendments made by this division, shall be construed to preclude any foreign authority from obtaining assistance in a criminal investigation or prosecution pursuant to section 3512 of title 18, United States Code, section 1782 of title 28, United States Code, or as otherwise provided by law.''

§ 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

(Added Pub. L. 99–508, title I, §110(a), Oct. 21, 1986, 100 Stat. 1859.)

Editorial Notes

REFERENCES IN TEXT

The Federal Rules of Civil Procedure, referred to in text, are set out in the Appendix to Title 28, Judiciary and Judicial Procedure.

The Federal Rules of Criminal Procedure, referred to in text, are set out in the Appendix to this title.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99–508, set out as an Effective Date of 1986 Amendment note under section 2510 of this title.

§ 2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) ENFORCEMENT BY COURT ISSUING SURVEILLANCE ORDER.—If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a 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 subsecs. (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