Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

First draft (13 March 2007)

Cybercrime legislation – country profile

United States of America

This profile has been prepared within the framework of the Council of Europe's project on cybercrime in order to permit an assessment of the current state of implementation of the Convention on Cybercrime under national legislation. It serves to share information on cybercrime legislation and to feed into the technical cooperation activities and the work of the Cybercrime Convention Committee of the Council of Europe. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Alexander Seger
Head of Technical Cooperation
Department of Crime Problems
Directorate General of Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**United States of America**
Signature of Convention:	Yes: 23.11.2001
Ratification/accession:	Yes: 29.09.2006
Provisions of the Convention	***Corrresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	18 U.S.C. § 1030(a) (1) – (5)
Article 3 – Illegal interception	18 U.S.C. § 1030; 18 U.S.C. § 2511
Article 4 – Data interference	18 U.S.C. § 1030(a)(5)
Article 5 – System interference	18 U.S.C. § 1030(a)(5)
Article 6 – Misuse of devices	18 U.S.C. § 1029; 18 U.S.C. § 1030; 18 U.S.C. 2512
Article 7 – Computer-related forgery	18 U.S.C. § 1029
Article 8 – Computer-	18 U.S.C. § 1030(a)(4); 18 U.S.C. § 1343

related fraud	
Article 9 – Offences related to child pornography	18 U.S.C. § 2251; 18 U.S.C. § 2252; 18 U.S.C. § 2252A
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	18 U.S.C. § 2319; 17 U.S.C. § 506
Article 11 – Attempt and aiding or abetting	Aiding and Abetting: 18 U.S.C. § 2 Attempt: 18 U.S.C. § 1030(c); 18 U.S.C. § 1029(b); 18 U.S.C. 2251(d); 18 U.S.C. § 2252(b); 18 U.S.C. § 2252A(b)
Article 12 – Corporate liability	Common Law recognizes corporate criminal as well as civil liability. See for example: 18 U.S.C. § 1030(e);
Article 13 – Sanctions and measures	See for example: 18 U.S.C. § 1030 of the US Code
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	
Article 15 – Conditions and safeguards	Common Law has a complex system of safeguards that meet the requirements of the Convention on Cybercrime.
Article 16 – Expedited preservation of stored computer data	18 U.S.C. § 2703 (f)
Article 17 – Expedited preservation and partial disclosure of traffic data	18 U.S.C. § 2703 (f)
Article 18 – Production order	18 U.S.C. § 2703
Article 19 – Search and seizure of stored computer data	18 U.S.C. § 2513
Article 20 – Real-time collection of traffic data	18 U.S.C. § 2704; 18 U.S.C. § 3121 - § 3127
Article 21 – Interception of content data	18 U.S.C. §2511
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	No single clause implementation. In general federal criminal jurisdiction is conferred by an element of interstate or foreign commerce or communication. Even by making use of the possibility to restrict the jurisdiction the federal jurisdiction will not be fully correspond with the requirements of Art. 22 CoC.
Chapter III – International co-operation	
Article 24 – Extradition	
Article 25 – General principles relating to mutual assistance	

Article 26 – Spontaneous information	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	
Article 28 – Confidentiality and limitation on use	
Article 29 – Expedited preservation of stored computer data	
Article 30 – Expedited disclosure of preserved traffic data	
Article 31 – Mutual assistance regarding accessing of stored computer data	
Article 32 – Trans-border access to stored computer data with consent or where publicly available	
Article 33 – Mutual assistance in the real-time collection of traffic data	
Article 34 – Mutual assistance regarding the interception of content data	
Article 35 – 24/7 Network	
Article 42 – Reservations	**Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America declares, pursuant to Articles 2 and 40, that under United States law, the offenses set forth in Article 2 ("Illegal access") includes an additional requirement of intent to obtain computer data. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 2 **Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America declares, pursuant to Articles 6 and 40, that under United States law, the offense set forth in paragraph (1) (b) of Article 6 ("Misuse of devices") includes a requirement that a minimum number of items be possessed. The minimum number shall be the same as that provided for by applicable United States federal law. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 6 **Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America declares, pursuant to Articles 7 and 40, that under United States law, the offense set forth in Article 7 ("Computer-related forgery") includes a requirement of intent to defraud. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 7

Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

The United States of America declares, pursuant to Articles 27 and 40, that requests made to the United States under paragraph 9(e) of Article 27 ("Procedures pertaining to mutual assistance requests in the absence of applicable international agreements") are to be addressed to its central authority for mutual assistance.

Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 27

Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

The United States of America, pursuant to Articles 4 and 42 of the Convention, reserves the right to require that the conduct result in serious harm, which shall be determined in accordance with applicable United States federal law.
Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 4

Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

The United States of America, pursuant to Articles 6 and 42 of the Convention, reserves the right not to apply paragraphs (1) (a) (i) and (1) (b) of Article 6 ("Misuses of devices") with respect to devices designed or adapted primarily for the purpose of committing the offenses established in Article 4 ("Data interference") and Article 5 ("System interference").

Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 6

Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

The United States of America, pursuant to Articles 9 and 42 of the Convention, reserves the right to apply paragraphs (2) (b) and (c) of Article 9 only to the extent consistent with the Constitution of the United States as interpreted by the United States and as provided for under its federal law, which includes, for example, crimes of distribution of material considered to be obscene under applicable United States standards.

Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 9

Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

The United States of America, pursuant to Articles 10 and 42 of the Convention, reserves the right to impose other effective remedies in lieu of criminal liability under paragraphs 1 and 2 of Article 10 ("Offenses related to infringement of copyright and related rights") with respect to infringements of certain rental rights to the extent the criminalisation of such infringements is not required pursuant to the obligations the United States has undertaken under the agreements referenced in paragraphs 1 and 2.

Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 10

Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

The United States of America, pursuant to Articles 22 and 42 of the Convention, reserves the right not to apply in part paragraphs (1) (b), (c) and (d) of Article 22 ("Jurisdiction"). The United States does not provide for plenary jurisdiction over offenses that are committed outside its territory by its citizen or on board ships flying its flag or aircraft registered under its laws. However, United States law does provide for jurisdiction over a number of offenses to be established under the Convention that are committed abroad by United States nationals in circumstances implicating particular federal interests, as well as

over a number of such offenses committed on board United States-flagged ships or aircraft registered under United States law. Accordingly, the United States will implement paragraphs (1) (b), (c) and (d) to the extent provided for under its federal law.

Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 22

Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

The United States of America, pursuant to Articles 41 and 42 of the Convention, reserves the right to assume obligations under Chapter II of the Convention in a manner consistent with its fundamental principles of federalism.

Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 41

Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

Pursuant to Article 24, paragraph 7, of the Convention, the United States of America is not designating an authority responsible for extradition or provisional arrest in the absence of a treaty, as the United States will continue to rely on bilateral extradition treaties, and the authority responsible for making or receiving extradition requests on behalf of the United States is set forth in the applicable bilateral extradition treaties.

Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 24

Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

Pursuant to Article 27, paragraph 2, of the Convention, the Office of International Affairs, United States Department of Justice, Criminal Division, Washington, D.C., 20530, is designated as the central authority of the United States of America for mutual assistance under the Convention.

Period covered: 1/1/2007 -

The preceding statement concerns Article(s) : 27

Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.

Pursuant to Article 35, paragraph 1, of the Convention, the Computer Crime and Intellectual Property Section, United States Department of Justice, Criminal Division, Washington, D.C., 20530, is designated as the point of contact available on a twenty-four hour, seven-day-a-week basis to ensure the provision of immediate assistance under the Convention. Contact Information for the Computer Crime and Intellectual Property Section is given below :24/7 Contact: United States of America

Contact and Telephone Number:
Computer Crime and Intellectual Property Section (CCIPS)
U.S. Department of Justice, Washington, DC
Tel: +1-202-514-1026 / Monday - Friday 0900 - 1800 hrs
Tel: +1-202-353-5216 / Mon - Fri after hours, Saturdays, Sundays, holidays
Tel: +1-202-514-6113 / Always on, but only monitored Monday - Friday 0900 - 1800 hrs

Description of Contact
CCIPS is a section of the Criminal Division of the U.S. Department of Justice that has 40 lawyers with responsibilities for combating cybercrime and theft of intellectual property, and with expertise in obtaining electronic evidence. Many CCIPS lawyers also have expertise in international assistance. CCIPS has "duty attorneys" available 24-hours a day, 7 days a week to respond to urgent requests for assistance.

Language Capabilities of the Contact : English

	What To Say When Calling Contact Number : *During business hours*, call +1-202-514-1026. Tell the receptionist (1) that you have "a cybercrime 24-7 request"; (2) from what country you are calling; and (3) that you want to be connected to "a duty attorney". *After business hours* and on Saturdays, Sundays and holidays, call +1-202-353-5216. Your call will be connected directly to a duty attorney. **Fax Information** : +1-202-514-6113. This fax machine operates 24 hours a day, 7 days a week, but faxes sent outside of normal working hours will not receive attention until the next business day. **Time Zone** : UTC/GMT -05:00 (Daylight Savings Time : +01:00) **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 35

Appendix: **Solutions in national legislation**

17 USC Sec. 506

TITLE 17 - COPYRIGHTS
CHAPTER 5 - COPYRIGHT INFRINGEMENT AND REMEDIES

(a) Criminal Infringement. - Any person who infringes a copyright willfully either –
(1) for purposes of commercial advantage or private financial gain, or
(2) by the reproduction or distribution, including byelectronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000, shall be punished as provided under section 2319 of title 18,United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.
(b) Forfeiture and Destruction. - When any person is convicted of any violation of subsection (a), the court in its judgment of conviction shall, in addition to the penalty therein prescribed, order the forfeiture and destruction or other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords.
(c) Fraudulent Copyright Notice. - Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than $2,500.
(d) Fraudulent Removal of Copyright Notice. - Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than $2,500.
(e) False Representation. - Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than $2,500.
(f) Rights of Attribution and Integrity. - Nothing in this section applies to infringement of the rights conferred by section 106A(a).

18 USC Sec. 1029

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 47 - FRAUD AND FALSE STATEMENTS

Sec. 1029. Fraud and related activity in connection with access devices

(a) Whoever -
(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;
(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;
(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;
(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -
(A) offering an access device; or
(B) selling information regarding or an application to obtain an access device;
(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;
(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or
(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.
(b)(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.
(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c)
of this section, or both.
(c) Penalties. -
(1) Generally. - The punishment for an offense under subsection (a) of this section is –
(A) in the case of an offense that does not occur after a conviction for another offense under this section - (i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and (ii) if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;
(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and
(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.
(2) Forfeiture procedure. - The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section.
(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
(e) As used in this section -
(1) the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);
(2) the term "counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit
access device;
(3) the term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;
(4) the term "produce" includes design, alter, authenticate, duplicate, or assemble;
(5) the term "traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;
(6) the term "device-making equipment" means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device;
(7) the term "credit card system member" means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system;
(8) the term "scanning receiver" means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial
number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument;
(9) the term "telecommunications service" has the meaning given such term in section 3 of title I of the Communications Act of 1934 (47 U.S.C. 153);

(10) the term "facilities-based carrier" means an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934; and
(11) the term "telecommunication identifying information" means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument.
(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title. For purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.
(g)(1) It is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person engaged in business with, a facilities-based carrier, to engage in conduct (other than trafficking) otherwise prohibited by that subsection for the purpose of protecting the property or legal rights of that carrier, unless such conduct is for the purpose of obtaining telecommunications service provided by another facilities-based carrier without the authorization of such carrier.
(2) In a prosecution for a violation of subsection (a)(9), (other than a violation consisting of producing or trafficking) it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) that the conduct charged was engaged in for research or development in connection with a lawful purpose.
(h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if -
(1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and
(2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

18 USC Sec. 1030

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 47 - FRAUD AND FALSE STATEMENTS

Sec. 1030. Fraud and related activity in connection with computers

(a) Whoever -
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is

exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) - (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if -
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; (!1)
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.
(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section. (c) The punishment for an offense under subsection (a) or (b) of this section is -
(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if - (i) the offense was committed for purposes of commercial advantage or private financial gain; (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or (iii) the value of the information obtained exceeds $5,000; and
(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;
(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;
(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and
(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and
(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.
(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.
(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
(e) As used in this section -
(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
(2) the term "protected computer" means a computer -
(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
(4) the term "financial institution" means -
(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;
(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C) a credit union with accounts insured by the National Credit Union Administration;
(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I) an organization operating under section 25 or section 25(a) (!2) of the Federal Reserve Act;
(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not
entitled so to obtain or alter;
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.
(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.
(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.
(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I – CRIMES
CHAPTER 63 – MAIL FRAUD

Section 1343. Fraud by wire, radio, or television

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

18 USC Sec. 2252

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I – CRIMES
CHAPTER 110 - SEXUAL EXPLOITATION AND OTHER ABUSE OF CHILDREN

Sec. 2252. Certain activities relating to material involving the sexual exploitation of minors

(a) Any person who –
(1) knowingly transports or ships in interstate or foreign commerce by any means including by computer or mails, any visual depiction, if –
(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
(B) such visual depiction is of such conduct;

(2) knowingly receives, or distributes, any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution in interstate or foreign commerce or through the mails, if –
(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
(B) such visual depiction is of such conduct;
(3) either –
(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title, knowingly sells or possesses with intent to sell any visual depiction; or
(B) knowingly sells or possesses with intent to sell any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer, if - (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct; or
(4) either –
(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title, knowingly possesses 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction; or
(B) knowingly possesses 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if - (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct; shall be punished as provided in subsection (b) of this section.
(b)(1) Whoever violates, or attempts or conspires to violate, paragraphs (!1) (1), (2), or (3) of subsection (a) shall be fined under this title and imprisoned not less than 5 years and not more than 20 years, but if such person has a prior conviction under this chapter, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 15 years nor more than 40 years.
(2) Whoever violates, or attempts or conspires to violate, paragraph (4) of subsection (a) shall be fined under this title or imprisoned not more than 10 years, or both, but if such person has a prior conviction under this chapter, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 10 years nor more than 20 years. (c) Affirmative Defense. - It shall be an affirmative defense to a charge of violating paragraph (4) of subsection (a) that the defendant –
(1) possessed less than three matters containing any visual depiction proscribed by that paragraph; and
(2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any visual depiction or copy thereof –
(A) took reasonable steps to destroy each such visual depiction; or
(B) reported the matter to a law enforcement agency and afforded that agency access to each such visual depiction.

18 USC Sec. 2252A

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I – CRIMES
CHAPTER 110 - SEXUAL EXPLOITATION AND OTHER ABUSE OF CHILDREN

Sec. 2252A. Certain activities relating to material constituting or containing child pornography

(a) Any person who –
(1) knowingly mails, or transports or ships in interstate or foreign commerce by any means, including by computer, any child pornography;
(2) knowingly receives or distributes –
(A) any child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer; or
(B) any material that contains child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer;
(3) knowingly –
(A) reproduces any child pornography for distribution through the mails, or in interstate or foreign commerce by any means, including by computer; or
(B) advertises, promotes, presents, distributes, or solicits through the mails, or in interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains - (i) an obscene visual depiction of a minor engaging in sexually explicit conduct; or (ii) a visual depiction of an actual minor engaging in sexually explicit conduct;
(4) either –
(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the United States Government, or in the Indian country (as defined in section 1151), knowingly sells or possesses with the intent to sell any child pornography; or
(B) knowingly sells or possesses with the intent to sell any child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer;
(5) either –
(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the United States Government, or in the Indian country (as defined in section 1151), knowingly possesses any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography; or
(B) knowingly possesses any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer; or
(6) knowingly distributes, offers, sends, or provides to a minor any visual depiction, including any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, where such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct –
(A) that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer;
(B) that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer; or
(C) which distribution, offer, sending, or provision is accomplished using the mails or by transmitting or causing to be transmitted any wire communication in interstate or foreign commerce, including by computer, for purposes of inducing or persuading a minor to participate in any activity that is illegal (!1) shall be punished as provided in subsection (b).
b)(1) Whoever violates, or attempts or conspires to violate, paragraph (1), (2), (3), (4), or (6) of subsection (a) shall be fined under this title and imprisoned not less than 5 years and not more than 20 years, but, if such person has a prior conviction under this chapter, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 15 years nor more than 40 years.
(2) Whoever violates, or attempts or conspires to violate, subsection (a)(5) shall be fined under this title or imprisoned not more than 10 years, or both, but, if such person has a prior conviction under this chapter, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 10 years nor more than 20 years.

(c) It shall be an affirmative defense to a charge of violating paragraph (1), (2), (3)(A), (4), or (5) of subsection (a) that -
(1)(A) the alleged child pornography was produced using an actual person or persons engaging in sexually explicit conduct; and
(B) each such person was an adult at the time the material was produced; or
(2) the alleged child pornography was not produced using any actual minor or minors.
No affirmative defense under subsection (c)(2) shall be available in any prosecution that involves child pornography as described in section 2256(8)(C). A defendant may not assert an affirmative defense to a charge of violating paragraph (1), (2), (3)(A), (4), or (5) of subsection (a) unless, within the time provided for filing pretrial motions or at such time prior to trial as the judge may direct, but in no event later than 10 days before the commencement of the trial, the defendant provides the court and the United States with notice of the intent to assert such defense and the substance of any expert or other specialized testimony or evidence upon which the defendant intends to rely. If the defendant fails to comply with this subsection, the court shall, absent a finding of extraordinary circumstances that prevented timely compliance, prohibit the defendant from asserting such defense to a charge of violating paragraph (1), (2), (3)(A), (4), or (5) of subsection (a) or presenting any evidence for which the defendant has failed to provide proper and timely notice. (d) Affirmative Defense. - It shall be an affirmative defense to a charge of violating subsection (a)(5) that the defendant –
(1) possessed less than three images of child pornography; and
(2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any image or copy thereof –
(A) took reasonable steps to destroy each such image; or
(B) reported the matter to a law enforcement agency and afforded that agency access to each such image.
(e) Admissibility of Evidence. - On motion of the government, in any prosecution under this chapter or section 1466A, except for good cause shown, the name, address, social security number, or other nonphysical identifying information, other than the age or approximate age, of any minor who is depicted in any child pornography shall not be admissible and may be redacted from any otherwise admissible evidence, and the jury shall be instructed, upon request of the United States, that it can draw no inference from the absence of such evidence in deciding whether the child pornography depicts an actual minor.
(f) Civil Remedies. -
(1) In general. - Any person aggrieved by reason of the conduct prohibited under subsection (a) or (b) or section 1466A may commence a civil action for the relief set forth in paragraph (2).
(2) Relief. - In any action commenced in accordance with paragraph (1), the court may award appropriate relief, including-
(A) temporary, preliminary, or permanent injunctive relief;
(B) compensatory and punitive damages; and
(C) the costs of the civil action and reasonable fees for attorneys and expert witnesses.

18 USC Sec. 2319

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I – CRIMES
CHAPTER 113 - STOLEN PROPERTY

Sec. 2319. Criminal infringement of a copyright

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.
(b) Any person who commits an offense under section 506(a)(1) of title 17 –
(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;
(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.
(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code –

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;
(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.
(d)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss uffered by the victim, including the estimated economic impact of the offense on that victim.
(2) Persons permitted to submit victim impact statements shall include –
(A) producers and sellers of legitimate works affected by conduct involved in the offense;
(B) holders of intellectual property rights in such works; and
(C) the legal representatives of such producers, sellers, and holders.
(e) As used in this section –
(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and
(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17.

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I – CRIMES
CHAPTER 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec. 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who -
(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when - (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;
(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or (e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. (ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with –
(A) a court order directing such assistance signed by the authorizing judge, or
(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.
(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.
(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.
(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.
(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.
(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.
(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person - (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public; (ii) to intercept any radio communication which is transmitted –
(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by any marine or aeronautical communications system; (iii) to engage in any conduct which - (I) is prohibited by section 633 of the Communications Act of 1934; or (II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act; (iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or (v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.
(h) It shall not be unlawful under this chapter - (i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or (ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.
(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if –
(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
(II) the person acting under color of law is lawfully engaged in an investigation; (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.
(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.
(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication - (i) as otherwise authorized in section 2511(2)(a) or 2517 of this title; (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.
(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.
(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted - (i) to a broadcasting station for purposes of retransmission to the general public; or (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.
(5)(a)(i) If the communication is –
(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or
(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction. (ii) In an action under this subsection - (A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and (B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

18 USC Sec. 2513

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Section 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally -
(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;
(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reasonto know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or
(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of -
(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,
shall be fined under this title or imprisoned not more than five years, or both.
(2) It shall not be unlawful under this section for -
(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or
(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.
(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

18 USC Sec. 2513

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec. 2513. Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary

and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

18 USC Sec. 2702

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I – CRIMES
CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec. 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions. - Except as provided in subsection (b) –
(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.
(b) Exceptions for disclosure of communications. - A provider described in subsection (a) may divulge the contents of a communication -
(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);
(7) to a law enforcement agency –
(A) if the contents – (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; or [(B) Repealed. Pub. L. 108-21, title V, Sec. 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]
(8) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.
(c) Exceptions for Disclosure of Customer Records. - A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) –
(1) as otherwise authorized in section 2703;
(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;
(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or
(6) to any person other than a governmental entity.

18 USC Sec. 2703

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I – CRIMES
CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec. 2703. Required disclosure of customer communications or Records

(a) Contents of Wire or Electronic Communications in Electronic Storage. - A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
(b) Contents of Wire or Electronic Communications in a Remote Computing Service. - (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity - (i) uses an administrative subpoena authorized by a Federal
or State statute or a Federal or State grand jury or trial subpoena; or (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.
(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
(c) Records Concerning Electronic Communication Service or Remote Computing Service. - (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity - (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; (B) obtains a court order for such disclosure under subsection
(d) of this section; (C) has the consent of the subscriber or customer to such disclosure; or (!1)
(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or (E) seeks information under paragraph (2).
(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the - (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of

payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).
(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscribe or customer.
(d) Requirements for Court Order. - A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.
(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter. - No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.
(f) Requirement To Preserve Evidence. - (1) In general. - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process (2) Period of retention. - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.
(g) Presence of Officer Not Required. - Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

18 USC Sec. 2704

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I – CRIMES
CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec. 2704. Backup preservation

(a) Backup Preservation. –
(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.
(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).
(3) The service provider shall not destroy such backup copy until the later of –
(A) the delivery of the information; or (B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.
(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider –
(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and
(B) has not initiated proceedings to challenge the request of the governmental entity.
(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe

that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.
(b) Customer Challenges. - (1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement (A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and (B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect. (2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure. (3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response. (4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed. (5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

18 USC Sec. 3121

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART II - CRIMINAL PROCEDURE
CHAPTER 206 – PEN REGISTERS AND TRAP AND TRACE DEVICES

Section 3121. General prohibition on pen register and trap and trace device use; exception
(a) In General. - Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).
(b) Exception. - The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service -
(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
(3) where the consent of the user of that service has been obtained.
(c) Limitation. - A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signalling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.
(d) Penalty. - Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

18 USC Sec. 3181

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART II - CRIMINAL PROCEDURE
CHAPTER 209 - EXTRADITION

Sec. 3181. Scope and limitation of chapter

(a) The provisions of this chapter relating to the surrender of persons who have committed crimes in foreign countries shall continue in force only during the existence of any treaty of extradition with such foreign government.
(b) The provisions of this chapter shall be construed to permit, in the exercise of comity, the surrender of persons, other than citizens, nationals, or permanent residents of the United States, who have committed crimes of violence against nationals of the United States in foreign countries without regard to the existence of any treaty of extradition with such foreign government if the Attorney General certifies, in writing, that –
(1) evidence has been presented by the foreign government that indicates that had the offenses been committed in the United States, they would constitute crimes of violence as defined under section 16 of this title; and
(2) the offenses charged are not of a political nature.
(c) As used in this section, the term "national of the United States" has the meaning given such term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22)).

18 USC Sec. 3184

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART II - CRIMINAL PROCEDURE
CHAPTER 209 - EXTRADITION

Sec. 3184. Fugitives from foreign country to United States

Whenever there is a treaty or convention for extradition between the United States and any foreign government, or in cases arising under section 3181(b), any justice or judge of the United States, or any magistrate judge authorized so to do by a court of the United States, or any judge of a court of record of general jurisdiction of any State, may, upon complaint made under oath, charging any person found within his jurisdiction, with having committed within the jurisdiction of any such foreign government any of the crimes provided for by such treaty or convention, or provided for under section 3181(b), issue his warrant for the apprehension of the person so charged, that he may be brought before such justice, judge, or magistrate judge, to the end that the evidence of criminality may be heard and considered. Such complaint may be filed before and such warrant may be issued by a judge or magistrate judge of the United States District Court for the District of Columbia if the whereabouts within the United States of the person charged are not known or, if there is reason to believe the person will shortly enter the United States. If, on such hearing, he deems the evidence sufficient to sustain the charge under the provisions of the proper treaty or convention, or under section 3181(b), he shall certify the same, together with a copy of all the testimony taken before him, to the Secretary of State, that a warrant may issue upon the requisition of the proper authorities of such foreign government, for the surrender of such person, according to the stipulations of the treaty or convention; and he shall issue his warrant for the commitment of the person so charged to the proper jail, there to remain until such surrender shall be made.

18 USC Sec. 3188

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART II - CRIMINAL PROCEDURE
CHAPTER 209 - EXTRADITION

Sec. 3188. Time of commitment pending extradition

Whenever any person who is committed for rendition to a foreign government to remain until delivered up in pursuance of a requisition, is not so delivered up and conveyed out of the United States within two calendar months after such commitment, over and above the time actually required to convey the prisoner from the jail to which he was committed, by the readiest way, out of the United States, any judge of the United States, or of any State, upon application made to him by or on behalf of the person so committed, and upon proof made to him that reasonable notice of the intention to make such application has been given to the Secretary of State, may order the person so committed to be discharged out of custody, unless sufficient cause is shown to such judge why such discharge ought not to be ordered.

18 USC Sec. 3192

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART II - CRIMINAL PROCEDURE
CHAPTER 209 - EXTRADITION

Sec. 3192. Protection of accused

Whenever any person is delivered by any foreign government to an agent of the United States, for the purpose of being brought within the United States and tried for any offense of which he is duly accused, the President shall have power to take all necessary measures for the transportation and safekeeping of such accused person, and for his security against lawless violence, until the final conclusion of his trial for the offenses specified in the warrant of extradition, and until his final discharge from custody or imprisonment for or on account of such offenses, and for a reasonable time thereafter, and may employ such portion of the land or naval forces of the United States, or of the militia thereof, as may be necessary for the safe-keeping and protection of the accused.

18 USC Sec. 3193

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART II - CRIMINAL PROCEDURE
CHAPTER 209 - EXTRADITION

Sec. 3193. Receiving agent's authority over offenders

A duly appointed agent to receive, in behalf of the United States, the delivery, by a foreign government, of any person accused of crime committed within the United States, and to convey him to the place of his trial, shall have all the powers of a marshal of the United States, in the several districts through which it may be necessary for him to pass with such prisoner, so far as such power is requisite for the prisoner's safe-keeping.

18 USC Sec. 3195

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART II - CRIMINAL PROCEDURE
CHAPTER 209 - EXTRADITION

Sec. 3195. Payment of fees and costs

All costs or expenses incurred in any extradition proceeding in apprehending, securing, and transmitting a fugitive shall be paid by the demanding authority. All witness fees and costs of every nature in cases of international extradition, including the fees of the magistrate judge, shall be certified by the judge or magistrate judge before whom the hearing shall take place to the Secretary of State of the United States, and the same shall be paid out of appropriations to defray the expenses of the judiciary or the Department of Justice as the case may be. The Attorney General shall certify to the Secretary of State the amounts to be paid to the United States on account of said fees and costs in extradition cases by the foreign government requesting the extradition, and the Secretary of State shall cause said amounts to be collected and transmitted to the Attorney General for deposit in the Treasury of the United States.

18 USC Sec. 3196

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART II - CRIMINAL PROCEDURE
CHAPTER 209 – EXTRADITION

Sec. 3196. Extradition of United States citizens

If the applicable treaty or convention does not obligate the United States to extradite its citizens to a foreign country, the Secretary of State may, nevertheless, order the surrender to that country of a United States citizen whose extradition has been requested by that country if the other requirements of that treaty or convention are met.