

CYBERCRIME LAWS OF THE UNITED STATES

Compiled October 2006 by Al Rees, CCIPS

Table of Contents

Substantive cybercrime laws (e.g., laws prohibiting online identity theft, hacking, intrusion into computer systems, child pornography, intellectual property, online gambling):

- 18 U.S.C. § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information
- 18 U.S.C. § 1028A – Aggravated identity theft
- 18 U.S.C. § 1029 – Fraud and related activity in connection with access devices
- 18 U.S.C. § 1030 – Fraud and related activity in connection with computers
- 18 U.S.C. § 1037 – Fraud and related activity in connection with electronic mail
- 18 U.S.C. § 1343 – Fraud by wire, radio, or television
- 18 U.S.C. § 1362 – [Malicious mischief related to] Communications lines, stations, or systems
- 18 U.S.C. § 1462 – Importation or transportation of obscene matters
- 18 U.S.C. § 1465 – Transportation of obscene matters for sale or distribution
- 18 U.S.C. § 1466A – Obscene visual representation of the sexual abuse of children
- 18 U.S.C. § 2251 – Sexual exploitation of children
- 18 U.S.C. § 2252 – Certain activities relating to material involving the sexual exploitation of minors
- 18 U.S.C. § 2252A – Certain activities relating to material constituting or containing child pornography
- 18 U.S.C. § 2252B – Misleading domain names on the Internet [to deceive minors]
- 18 U.S.C. § 2252C – Misleading words or digital images on the Internet
- 18 U.S.C. § 2425 – Use of interstate facilities to transmit information about a minor
- 18 U.S.C. § 2319 – Criminal infringement of a copyright
- 17 U.S.C. § 506 – Criminal offenses [related to copyright]
- 47 U.S.C. 605 – Unauthorized publication or use of communications
- The Unlawful Internet Gambling Enforcement Act of 2006

Procedural cybercrime laws (e.g., authority to preserve and obtain electronic data from third parties, including internet service providers; authority to intercept electronic communications; authority to search and seize electronic evidence):

- 18 U.S.C. §§ 2510-2522 – Interception of wire, oral, or electronic communication
- 18 U.S.C. §§ 2701-2712 – Preservation and disclosure of stored wire and electronic communication
- 18 U.S.C. §§ 3121-3127 – Pen registers and trap and trace devices

18 U.S.C. § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information

- (a) Whoever, in a circumstance described in subsection (c) of this section—
- (1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;
 - (2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;
 - (3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;
 - (4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;
 - (5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;
 - (6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;
 - (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or
 - (8) knowingly traffics in false authentication features for use in false identification documents, document-making implements, or means of identification;
- shall be punished as provided in subsection (b) of this section.
- (b) The punishment for an offense under subsection (a) of this section is—
- (1) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 15 years, or both, if the offense is—
 - (A) the production or transfer of an identification document, authentication feature, or false identification document that is or appears to be—
 - (i) an identification document or authentication feature issued by or under the authority of the United States; or
 - (ii) a birth certificate, or a driver's license or personal identification card;
 - (B) the production or transfer of more than five identification documents, authentication features, or false identification documents;
 - (C) an offense under paragraph (5) of such subsection; or
 - (D) an offense under paragraph (7) of such subsection that involves the transfer, possession, or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating \$1,000 or more during any 1-year period;
 - (2) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 5 years, or both, if the offense is—
 - (A) any other production, transfer, or use of a means of identification, an identification document, authentication feature, or a false identification document; or
 - (B) an offense under paragraph (3) or (7) of such subsection;

- (3) a fine under this title or imprisonment for not more than 20 years, or both, if the offense is committed—
- (A) to facilitate a drug trafficking crime (as defined in section 929 (a)(2));
 - (B) in connection with a crime of violence (as defined in section 924 (c)(3)); or
 - (C) after a prior conviction under this section becomes final;
- (4) a fine under this title or imprisonment for not more than 30 years, or both, if the offense is committed to facilitate an act of domestic terrorism (as defined under section 2331 (5) of this title) or an act of international terrorism (as defined in section 2331 (1) of this title);
- (5) in the case of any offense under subsection (a), forfeiture to the United States of any personal property used or intended to be used to commit the offense; and
- (6) a fine under this title or imprisonment for not more than one year, or both, in any other case.
- (c) The circumstance referred to in subsection (a) of this section is that—
- (1) the identification document, authentication feature, or false identification document is or appears to be issued by or under the authority of the United States or the document-making implement is designed or suited for making such an identification document, authentication feature, or false identification document;
 - (2) the offense is an offense under subsection (a)(4) of this section; or
 - (3) either—
 - (A) the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means; or
 - (B) the means of identification, identification document, false identification document, or document-making implement is transported in the mail in the course of the production, transfer, possession, or use prohibited by this section.
- (d) In this section and section 1028A—
- (1) the term “authentication feature” means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified;
 - (2) the term “document-making implement” means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;
 - (3) the term “identification document” means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;
 - (4) the term “false identification document” means a document of a type intended or commonly accepted for the purposes of identification of individuals that—
 - (A) is not issued by or under the authority of a governmental entity or was issued under the authority of a governmental entity but was subsequently altered for purposes of deceit; and
 - (B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization;
 - (5) the term “false authentication feature” means an authentication feature that—
 - (A) is genuine in origin, but, without the authorization of the issuing authority, has been tampered with or altered for purposes of deceit;

(B) is genuine, but has been distributed, or is intended for distribution, without the authorization of the issuing authority and not in connection with a lawfully made identification document, document-making implement, or means of identification to which such authentication feature is intended to be affixed or embedded by the respective issuing authority; or

(C) appears to be genuine, but is not;

(6) the term “issuing authority”—

(A) means any governmental entity or agency that is authorized to issue identification documents, means of identification, or authentication features; and

(B) includes the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international government or quasi-governmental organization;

(7) the term “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029 (e));

(8) the term “personal identification card” means an identification document issued by a State or local government solely for the purpose of identification;

(9) the term “produce” includes alter, authenticate, or assemble;

(10) the term “transfer” includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others;

(11) the term “State” includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession, or territory of the United States; and

(12) the term “traffic” means—

(A) to transport, transfer, or otherwise dispose of, to another, as consideration for anything of value; or

(B) to make or obtain control of with intent to so transport, transfer, or otherwise dispose of.

(e) 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.

(f) Attempt and Conspiracy.— Any person who attempts or conspires to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

(g) Forfeiture Procedures.— The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

(h) Forfeiture; Disposition.— In the circumstance in which any person is convicted of a violation of subsection (a), the court shall order, in addition to the penalty prescribed, the forfeiture and destruction or

other disposition of all illicit authentication features, identification documents, document-making implements, or means of identification.

(i) Rule of Construction.— For purpose of subsection (a)(7), a single identification document or false identification document that contains 1 or more means of identification shall be construed to be 1 means of identification.

18 U.S.C. § 1028A – Aggravated identity theft

(a) Offenses.—

(1) In general.— Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

(2) Terrorism offense.— Whoever, during and in relation to any felony violation enumerated in section 2332b (g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.

(b) Consecutive Sentence.— Notwithstanding any other provision of law—

(1) a court shall not place on probation any person convicted of a violation of this section;

(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identification was transferred, possessed, or used;

(3) in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the Sentencing Commission pursuant to section 994 of title 28.

(c) Definition.— For purposes of this section, the term “felony violation enumerated in subsection (c)” means any offense that is a felony violation of—

(1) section 641 (relating to theft of public money, property, or rewards), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), or section 664 (relating to theft from employee benefit plans);

(2) section 911 (relating to false personation of citizenship);

(3) section 922 (a)(6) (relating to false statements in connection with the acquisition of a firearm);

(4) any provision contained in this chapter (relating to fraud and false statements), other than this section or section 1028 (a)(7);

(5) any provision contained in chapter 63 (relating to mail, bank, and wire fraud);

(6) any provision contained in chapter 69 (relating to nationality and citizenship);

(7) any provision contained in chapter 75 (relating to passports and visas);

(8) section 523 of the Gramm-Leach-Bliley Act (15 U.S.C. 6823) (relating to obtaining customer information by false pretenses);

(9) section 243 or 266 of the Immigration and Nationality Act (8 U.S.C. 1253 and 1306) (relating to willfully failing to leave the United States after deportation and creating a counterfeit alien registration card);

(10) any provision contained in chapter 8 of title II of the Immigration and Nationality Act (8 U.S.C. 1321 et seq.) (relating to various immigration offenses); or

(11) section 208, 811, 1107(b), 1128B(a), or 1632 of the Social Security Act (42 U.S.C. 408, 1011, 1307 (b), 1320a–7b (a), and 1383a) (relating to false statements relating to programs under the Act).

18 U.S.C. § 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 U.S.C. § 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;
- (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) 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).

18 U.S.C. § 1037 – Fraud and related activity in connection with electronic mail

- (a) In General.**— Whoever, in or affecting interstate or foreign commerce, knowingly—
- (1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,
 - (2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,
 - (3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,
 - (4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or
 - (5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,
- or conspires to do so, shall be punished as provided in subsection (b).
- (b) Penalties.**— The punishment for an offense under subsection (a) is—
- (1) a fine under this title, imprisonment for not more than 5 years, or both, if—
 - (A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or
 - (B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;
 - (2) a fine under this title, imprisonment for not more than 3 years, or both, if—
 - (A) the offense is an offense under subsection (a)(1);
 - (B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;
 - (C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;
 - (D) the offense caused loss to one or more persons aggregating \$5,000 or more in value during any 1-year period;
 - (E) as a result of the offense any individual committing the offense obtained anything of value aggregating \$5,000 or more during any 1-year period; or
 - (F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and
 - (3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.
- (c) Forfeiture.**—
- (1) **In general.**— The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States—
 - (A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and
 - (B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

(2) Procedures.— The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

(d) Definitions.— In this section:

(1) Loss.— The term “loss” has the meaning given that term in section 1030 (e) of this title.

(2) Materially.— For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

(3) Multiple.— The term “multiple” means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.

(4) Other terms.— Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003.”.

18 U.S.C. § 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 U.S.C. § 1362 – [Malicious mischief related to] Communications lines, stations, or systems

Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both.

In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defense functions of the United States.

18 U.S.C. § 1462 – Importation or transportation of obscene matters

Whoever brings into the United States, or any place subject to the jurisdiction thereof, or knowingly uses any express company or other common carrier or interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934), for carriage in interstate or foreign commerce—

(a) any obscene, lewd, lascivious, or filthy book, pamphlet, picture, motion-picture film, paper, letter, writing, print, or other matter of indecent character; or

(b) any obscene, lewd, lascivious, or filthy phonograph recording, electrical transcription, or other article or thing capable of producing sound; or

(c) any drug, medicine, article, or thing designed, adapted, or intended for producing abortion, or for any indecent or immoral use; or any written or printed card, letter, circular, book, pamphlet, advertisement, or notice of any kind giving information, directly or indirectly, where, how, or of whom, or by what means any of such mentioned articles, matters, or things may be obtained or made; or

Whoever knowingly takes or receives, from such express company or other common carrier or interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934) any matter or thing the carriage or importation of which is herein made unlawful—

Shall be fined under this title or imprisoned not more than five years, or both, for the first such offense and shall be fined under this title or imprisoned not more than ten years, or both, for each such offense thereafter.

18 U.S.C. § 1465 – Transportation of obscene matters for sale or distribution

Whoever knowingly transports or travels in, or uses a facility or means of, interstate or foreign commerce or an interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934) in or affecting such commerce for the purpose of sale or distribution of any obscene, lewd, lascivious, or filthy book, pamphlet, picture, film, paper, letter, writing, print, silhouette, drawing, figure, image, cast, phonograph recording, electrical transcription or other article capable of producing sound or any other matter of indecent or immoral character, shall be fined under this title or imprisoned not more than five years, or both.

The transportation as aforesaid of two or more copies of any publication or two or more of any article of the character described above, or a combined total of five such publications and articles, shall create a presumption that such publications or articles are intended for sale or distribution, but such presumption shall be rebuttable.

18 U.S.C. § 1466A – Obscene visual representation of the sexual abuse of children

(a) In General.— Any person who, in a circumstance described in subsection (d), knowingly produces, distributes, receives, or possesses with intent to distribute, a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, that—

(1)

(A) depicts a minor engaging in sexually explicit conduct; and

(B) is obscene; or

(2)

(A) depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; and

(B) lacks serious literary, artistic, political, or scientific value;

or attempts or conspires to do so, shall be subject to the penalties provided in section 2252A (b)(1), including the penalties provided for cases involving a prior conviction.

(b) Additional Offenses.— Any person who, in a circumstance described in subsection (d), knowingly possesses a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, that—

(1)

(A) depicts a minor engaging in sexually explicit conduct; and

(B) is obscene; or

(2)

(A) depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; and

(B) lacks serious literary, artistic, political, or scientific value;

or attempts or conspires to do so, shall be subject to the penalties provided in section 2252A

(b)(2), including the penalties provided for cases involving a prior conviction.

(c) Nonrequired Element of Offense.— It is not a required element of any offense under this section that the minor depicted actually exist.

(d) Circumstances.— The circumstance referred to in subsections (a) and (b) is that—

(1) any communication involved in or made in furtherance of the offense is communicated or transported by the mail, or in interstate or foreign commerce by any means, including by computer, or any means or instrumentality of interstate or foreign commerce is otherwise used in committing or in furtherance of the commission of the offense;

(2) any communication involved in or made in furtherance of the offense contemplates the transmission or transportation of a visual depiction by the mail, or in interstate or foreign commerce by any means, including by computer;

(3) any person travels or is transported in interstate or foreign commerce in the course of the commission or in furtherance of the commission of the offense;

(4) any visual depiction involved in the offense has been mailed, or has been shipped or transported in interstate or foreign commerce by any means, including by computer, or was produced using materials that have been mailed, or that have been shipped or transported in interstate or foreign commerce by any means, including by computer; or

(5) the offense is committed in the special maritime and territorial jurisdiction of the United States or in any territory or possession of the United States.

(e) Affirmative Defense.— It shall be an affirmative defense to a charge of violating subsection (b) that the defendant—

- (1) possessed less than 3 such visual depictions; and
- (2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any such visual depiction—
 - (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.

(f) Definitions.— For purposes of this section—

- (1) the term “visual depiction” includes undeveloped film and videotape, and data stored on a computer disk or by electronic means which is capable of conversion into a visual image, and also includes any photograph, film, video, picture, digital image or picture, computer image or picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means;
- (2) the term “sexually explicit conduct” has the meaning given the term in section 2256 (2)(A) or 2256 (2)(B); and
- (3) the term “graphic”, when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.

18 U.S.C. § 2251 – Sexual exploitation of children

(a) Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported in interstate or foreign commerce or mailed, if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported in interstate or foreign commerce or mailed.

(b) Any parent, legal guardian, or person having custody or control of a minor who knowingly permits such minor to engage in, or to assist any other person to engage in, sexually explicit conduct for the purpose of producing any visual depiction of such conduct shall be punished as provided under subsection (e) of this section, if such parent, legal guardian, or person knows or has reason to know that such visual depiction will be transported in interstate or foreign commerce or mailed, if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported in interstate or foreign commerce or mailed.

(c)

(1) Any person who, in a circumstance described in paragraph (2), employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, any sexually explicit conduct outside of the United States, its territories or possessions, for the purpose of producing any visual depiction of such conduct, shall be punished as provided under subsection (e).

(2) The circumstance referred to in paragraph (1) is that—

(A) the person intends such visual depiction to be transported to the United States, its territories or possessions, by any means, including by computer or mail; or

(B) the person transports such visual depiction to the United States, its territories or possessions, by any means, including by computer or mail.

(d)

(1) Any person who, in a circumstance described in paragraph (2), knowingly makes, prints, or publishes, or causes to be made, printed, or published, any notice or advertisement seeking or offering—

(A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or

(B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

shall be punished as provided under subsection (e).

(2) The circumstance referred to in paragraph (1) is that—

(A) such person knows or has reason to know that such notice or advertisement will be transported in interstate or foreign commerce by any means including by computer or mailed; or

(B) such notice or advertisement is transported in interstate or foreign commerce by any means including by computer or mailed.

(e) Any individual who violates, or attempts or conspires to violate, this section shall be fined under this title and imprisoned not less than 15 years nor more than 30 years, but if such person has one 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 the sexual exploitation of children, such person shall be fined under this title and imprisoned for not less than 25 years nor more than 50 years, but if such person has 2 or more prior convictions 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 the sexual exploitation of children, such person shall be fined under this title and imprisoned not less than 35 years nor more than life. Any organization that violates, or attempts or conspires to violate, this section shall be fined under this title. Whoever, in the course of an offense under this section, engages in conduct that results in the death of a person, shall be punished by death or imprisoned for any term of years or for life.

18 U.S.C. § 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), (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 U.S.C. § 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.
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 U.S.C. § 2252B – Misleading domain names on the Internet [to deceive minors]

(a) Whoever knowingly uses a misleading domain name on the Internet with the intent to deceive a person into viewing material constituting obscenity shall be fined under this title or imprisoned not more than 2 years, or both.

(b) Whoever knowingly uses a misleading domain name on the Internet with the intent to deceive a minor into viewing material that is harmful to minors on the Internet shall be fined under this title or imprisoned not more than 4 years, or both.

(c) For the purposes of this section, a domain name that includes a word or words to indicate the sexual content of the site, such as “sex” or “porn”, is not misleading.

(d) For the purposes of this section, the term “material that is harmful to minors” means any communication, consisting of nudity, sex, or excretion, that, taken as a whole and with reference to its context—

- (1) predominantly appeals to a prurient interest of minors;
- (2) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
- (3) lacks serious literary, artistic, political, or scientific value for minors.

(e) For the purposes of subsection (d), the term “sex” means acts of masturbation, sexual intercourse, or physical contact with a person’s genitals, or the condition of human male or female genitals when in a state of sexual stimulation or arousal.

18 U.S.C. § 2252C – Misleading words or digital images on the Internet

(a) Whoever knowingly uses a misleading domain name on the Internet with the intent to deceive a person into viewing material constituting obscenity shall be fined under this title or imprisoned not more than 2 years, or both.

(b) Whoever knowingly uses a misleading domain name on the Internet with the intent to deceive a minor into viewing material that is harmful to minors on the Internet shall be fined under this title or imprisoned not more than 4 years, or both.

(c) For the purposes of this section, a domain name that includes a word or words to indicate the sexual content of the site, such as “sex” or “porn”, is not misleading.

(d) For the purposes of this section, the term “material that is harmful to minors” means any communication, consisting of nudity, sex, or excretion, that, taken as a whole and with reference to its context—

- (1) predominantly appeals to a prurient interest of minors;
- (2) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
- (3) lacks serious literary, artistic, political, or scientific value for minors.

(e) For the purposes of subsection (d), the term “sex” means acts of masturbation, sexual intercourse, or physical contact with a person’s genitals, or the condition of human male or female genitals when in a state of sexual stimulation or arousal.

18 U.S.C. § 2425 – Use of interstate facilities to transmit information about a minor

Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, knowingly initiates the transmission of the name, address, telephone number, social security number, or electronic mail address of another individual, knowing that such other individual has not attained the age of 16 years, with the intent to entice, encourage, offer, or solicit any person to engage in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title, imprisoned not more than 5 years, or both.

18 U.S.C. § 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 suffered 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.

17 U.S.C. § 506 – Criminal offenses [related to copyright]

(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 by electronic 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).

47 U.S.C. 605 – Unauthorized publication or use of communications

(a) Practices prohibited

Except as authorized by chapter 119, title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception,

- (1) to any person other than the addressee, his agent, or attorney,
- (2) to a person employed or authorized to forward such communication to its destination,
- (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed,
- (4) to the master of a ship under whom he is serving,
- (5) in response to a subpoena issued by a court of competent jurisdiction, or
- (6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.

(b) Exceptions

The provisions of subsection (a) of this section shall not apply to the interception or receipt by any individual, or the assisting (including the manufacture or sale) of such interception or receipt, of any satellite cable programming for private viewing if—

- (1) the programming involved is not encrypted; and
- (2)
 - (A) a marketing system is not established under which—
 - (i) an agent or agents have been lawfully designated for the purpose of authorizing private viewing by individuals, and
 - (ii) such authorization is available to the individual involved from the appropriate agent or agents; or
 - (B) a marketing system described in subparagraph (A) is established and the individuals receiving such programming has obtained authorization for private viewing under that system.

(c) Scrambling of Public Broadcasting Service programming

No person shall encrypt or continue to encrypt satellite delivered programs included in the National Program Service of the Public Broadcasting Service and intended for public viewing by retransmission by television broadcast stations; except that as long as at least one unencrypted satellite transmission of any program subject to this subsection is provided, this subsection shall not prohibit additional encrypted satellite transmissions of the same program.

(d) Definitions

For purposes of this section—

- (1) the term “satellite cable programming” means video programming which is transmitted via satellite and which is primarily intended for the direct receipt by cable operators for their retransmission to cable subscribers;
- (2) the term “agent”, with respect to any person, includes an employee of such person;
- (3) the term “encrypt”, when used with respect to satellite cable programming, means to transmit such programming in a form whereby the aural and visual characteristics (or both) are modified or altered for the purpose of preventing the unauthorized receipt of such programming by persons without authorized equipment which is designed to eliminate the effects of such modification or alteration;
- (4) the term “private viewing” means the viewing for private use in an individual’s dwelling unit by means of equipment, owned or operated by such individual, capable of receiving satellite cable programming directly from a satellite;
- (5) the term “private financial gain” shall not include the gain resulting to any individual for the private use in such individual’s dwelling unit of any programming for which the individual has not obtained authorization for that use; and
- (6) the term “any person aggrieved” shall include any person with proprietary rights in the intercepted communication by wire or radio, including wholesale or retail distributors of satellite cable programming, and, in the case of a violation of paragraph (4) of subsection (e) of this section, shall also include any person engaged in the lawful manufacture, distribution, or sale of equipment necessary to authorize or receive satellite cable programming.

(e) Penalties; civil actions; remedies; attorney’s fees and costs; computation of damages; regulation by State and local authorities

- (1) Any person who willfully violates subsection (a) of this section shall be fined not more than \$2,000 or imprisoned for not more than 6 months, or both.
- (2) Any person who violates subsection (a) of this section willfully and for purposes of direct or indirect commercial advantage or private financial gain shall be fined not more than \$50,000 or imprisoned for not more than 2 years, or both, for the first such conviction and shall be fined not more than \$100,000 or imprisoned for not more than 5 years, or both, for any subsequent conviction.
- (3)
 - (A) Any person aggrieved by any violation of subsection (a) of this section or paragraph (4) of this subsection may bring a civil action in a United States district court or in any other court of competent jurisdiction.
 - (B) The court—
 - (i) may grant temporary and final injunctions on such terms as it may deem reasonable to prevent or restrain violations of subsection (a) of this section;
 - (ii) may award damages as described in subparagraph (C); and
 - (iii) shall direct the recovery of full costs, including awarding reasonable attorneys’ fees to an aggrieved party who prevails.
 - (C)
 - (i) Damages awarded by any court under this section shall be computed, at the election of the aggrieved party, in accordance with either of the following subclauses:
 - (I) the party aggrieved may recover the actual damages suffered by him as a result of the violation and any profits of the violator that are attributable to the violation which are not taken into account in computing the actual damages; in determining the violator’s profits, the party aggrieved shall be required to prove only the violator’s gross revenue, and the violator shall be required to prove his deductible expenses and the elements of profit attributable to factors other than the violation; or
 - (II) the party aggrieved may recover an award of statutory damages for each violation of subsection (a) of this section involved in the action in a sum of not less than \$1,000 or

more than \$10,000, as the court considers just, and for each violation of paragraph (4) of this subsection involved in the action an aggrieved party may recover statutory damages in a sum not less than \$10,000, or more than \$100,000, as the court considers just.

(ii) In any case in which the court finds that the violation was committed willfully and for purposes of direct or indirect commercial advantage or private financial gain, the court in its discretion may increase the award of damages, whether actual or statutory, by an amount of not more than \$100,000 for each violation of subsection (a) of this section.

(iii) In any case where the court finds that the violator was not aware and had no reason to believe that his acts constituted a violation of this section, the court in its discretion may reduce the award of damages to a sum of not less than \$250.

(4) Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a) of this section, shall be fined not more than \$500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both. For purposes of all penalties and remedies established for violations of this paragraph, the prohibited activity established herein as it applies to each such device shall be deemed a separate violation.

(5) The penalties under this subsection shall be in addition to those prescribed under any other provision of this subchapter.

(6) Nothing in this subsection shall prevent any State, or political subdivision thereof, from enacting or enforcing any laws with respect to the importation, sale, manufacture, or distribution of equipment by any person with the intent of its use to assist in the interception or receipt of radio communications prohibited by subsection (a) of this section.

(f) Rights, obligations, and liabilities under other laws unaffected

Nothing in this section shall affect any right, obligation, or liability under title 17, any rule, regulation, or order thereunder, or any other applicable Federal, State, or local law.

(g) Universal encryption standard

The Commission shall initiate an inquiry concerning the need for a universal encryption standard that permits decryption of satellite cable programming intended for private viewing. In conducting such inquiry, the Commission shall take into account—

- (1) consumer costs and benefits of any such standard, including consumer investment in equipment in operation;
- (2) incorporation of technological enhancements, including advanced television formats;
- (3) whether any such standard would effectively prevent present and future unauthorized decryption of satellite cable programming;
- (4) the costs and benefits of any such standard on other authorized users of encrypted satellite cable programming, including cable systems and satellite master antenna television systems;
- (5) the effect of any such standard on competition in the manufacture of decryption equipment; and
- (6) the impact of the time delay associated with the Commission procedures necessary for establishment of such standards.

(h) Rulemaking for encryption standard

If the Commission finds, based on the information gathered from the inquiry required by subsection (g) of this section, that a universal encryption standard is necessary and in the public interest, the Commission shall initiate a rulemaking to establish such a standard.

The Unlawful Internet Gambling Enforcement Act of 2006

Came into effect on October 13, 2006, and amends United States Code, Title 53, Chapter 31

THIS IS A SUMMARY OF THE ACT, PREPARED BY THE U.S. CONGRESSIONAL RESEARCH SERVICE:

Title I: Modernization of the Wire Act of 1961 –

(Sec. 101) Amends the federal criminal code to expand the definition of "wire communication facility" (renamed "communication facility") to include fixed or mobile (i.e., wireless) communication facilities.

Defines "bets and wagers" to include bets for contests, sporting events, games predominantly subject to chance, and lotteries. Excludes from such definition: (1) activities governed by securities laws; (2) transactions under the Commodity Exchange Act; (3) over-the-counter derivative instruments; (4) contracts of indemnity or guarantee; (4) contracts for life, health, or accident insurance; and (5) reward programs or contests conducted by businesses.

(Sec. 102) Modifies existing prohibitions against interstate gambling to prohibit the use of a communication facility to transmit: (1) bets or wagers; (2) information assisting in the placing of bets or wagers; or (3) a communication which entitles the recipient to receive money or credit as a result of bets or wages or for information assisting in the placing of bets or wagers.

Prohibits any individual from accepting, in connection with the placing of bets or wagers to or from the United States: (1) credit, or the proceeds of credit; (2) electronic funds transfers; (3) checks, drafts, or similar instruments; or (4) the proceeds of any other form of financial transaction as prescribed by Treasury regulations.

Imposes a fine and/or prison term of up to five years for violations.

Requires any common carrier which receives notice of a violation of this Act by one of its communication facilities to discontinue or refuse service to such facility. Grants such common carrier immunity from liability for discontinuing or refusing such service.

(Sec. 103) Grants U.S. district courts original and exclusive jurisdiction to prevent and restrain violations of the Internet gambling ban. Authorizes the Attorney General or any state attorney general to institute proceeding to enforce an Internet gambling ban.

(Sec. 104) Authorizes appropriations to the Department of Justice in FY2007-FY2010 for investigations and prosecutions of unlawful Internet gambling.

(Sec. 105) Declares that nothing in this Act may be construed to prohibit any activity allowed under the Interstate Horseracing Act or to preempt any state law prohibiting gambling.

(Sec. 106) Expresses the sense of Congress that this Act does not address the legality of certain horse racing activities under federal law.

Title II: Policies and Procedures Required to Prevent Payments for Unlawful Gambling - Amends the federal criminal code to prohibit persons engaged in a gambling business from knowingly accepting credit, electronic fund transfers, checks, drafts, or similar financial instruments or the proceeds of any

other financial transaction in connection with unlawful Internet gambling (this prohibition is defined by this Act as a "restricted transaction").

Directs the Secretary of the Treasury and the Board of Governors of the Federal Reserve System to prescribe regulations to identify and block restricted transactions. Grants immunity from civil liability for blocking a restricted transaction or one which is reasonably believed to be a restricted transaction.

Title III: Internet Gambling in or through Foreign Jurisdictions - Calls upon the U.S. government, in deliberations with foreign governments, to: (1) encourage cooperation by foreign governments in identifying whether Internet gambling operations are being used for money laundering, corruption, or other crimes; (2) advance policies that promote international cooperation in enforcing this Act; and (3) encourage the Financial Action Task Force on Money Laundering to study the extent to which Internet gambling operations are being used for money laundering purposes.

Directs the Secretary of the Treasury to report to Congress annually on deliberations between the United States and other countries on Internet gambling.

18 U.S.C. §§ 2510-2522 – Interception of wire, oral, or electronic communication

Title 18, Chapter 119 – WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

§ 2510. Definitions

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

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

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

[§ 2514. Repealed]

§ 2515. Prohibition of use as evidence of intercepted wire or oral communications

§ 2516. Authorization for interception of wire, oral, or electronic communications

§ 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

§ 2518. Procedure for interception of wire, oral, or electronic communications

§ 2519. Reports concerning intercepted wire, oral, or electronic communications

§ 2520. Recovery of civil damages authorized

§ 2521. Injunction against illegal interception

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

18 U.S.C. § 2510. Definitions

As used in this chapter—

(1) “wire communication” means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) “oral communication” means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

(5) “electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof,

(i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

- (6) “person” means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;
- (7) “Investigative or law enforcement officer” means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;
- (8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;
- (9) “Judge of competent jurisdiction” means—
- (a) a judge of a United States district court or a United States court of appeals; and
 - (b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;
- (10) “communication common carrier” has the meaning given that term in section 3 of the Communications Act of 1934;
- (11) “aggrieved person” means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;
- (12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
- (A) any wire or oral communication;
 - (B) any communication made through a tone-only paging device;
 - (C) any communication from a tracking device (as defined in section 3117 of this title); or
 - (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
- (13) “user” means any person or entity who—
- (A) uses an electronic communication service; and
 - (B) is duly authorized by the provider of such service to engage in such use;
- (14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;
- (15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;
- (16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not—
- (A) scrambled or encrypted;
 - (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
 - (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
 - (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
 - (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;
- (17) “electronic storage” means—
- (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
 - (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;
- (18) “aural transfer” means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

- (19)** “foreign intelligence information”, for purposes of section 2517 (6) of this title, means—
- (A)** information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—
 - (i)** actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - (ii)** sabotage or international terrorism by a foreign power or an agent of a foreign power; or
 - (iii)** clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
 - (B)** information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—
 - (i)** the national defense or the security of the United States; or
 - (ii)** the conduct of the foreign affairs of the United States;
- (20)** “protected computer” has the meaning set forth in section 1030; and
- (21)** “computer trespasser”—
- (A)** means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and
 - (B)** does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

18 U.S.C. § 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 U.S.C. § 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 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, 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 U.S.C. § 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 U.S.C. § 2514. Repealed]

18 U.S.C. § 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

18 U.S.C. § 2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501 (c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual

exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521 (b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 175c (relating to variola virus), section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123 (b) (relating to destruction of a natural gas pipeline) or section 46502 (relating to aircraft piracy) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

- (n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);
- (o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);
- (p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or
- (q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h, 2339A, 2339B, or 2339C of this title (relating to terrorism); or
- (r) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnaping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

18 U.S.C. § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the

provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

18 U.S.C. § 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including

- (i) details as to the particular offense that has been, is being, or is about to be committed,
- (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted,
- (iii) a particular description of the type of communications sought to be intercepted,
- (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or

code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)

(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518 (7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

- (1)** the fact of the entry of the order or the application;
- (2)** the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
- (3)** the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)

(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

- (i)** the communication was unlawfully intercepted;
- (ii)** the order of authorization or approval under which it was intercepted is insufficient on its face; or
- (iii)** the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

(a) in the case of an application with respect to the interception of an oral communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

18 U.S.C. § 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

- (a) the fact that an order or extension was applied for;
- (b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518 (1)(b)(ii) and 2518 (3)(d) of this title did not apply by reason of section 2518 (11) of this title);
- (c) the fact that the order or extension was granted as applied for, was modified, or was denied;
- (d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- (e) the offense specified in the order or application, or extension of an order;
- (f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and
- (g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

- (a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;
- (b) a general description of the interceptions made under such order or extension, including
 - (i) the approximate nature and frequency of incriminating communications intercepted,
 - (ii) the approximate nature and frequency of other communications intercepted,
 - (iii) the approximate number of persons whose communications were intercepted,
 - (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and
 - (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;
- (c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;
- (d) the number of trials resulting from such interceptions;
- (e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;
- (f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and
- (g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

18 U.S.C. § 2520. Recovery of civil damages authorized

a) In General.— Except as provided in section 2511 (2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.— In an action under this section, appropriate relief includes—

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c) and punitive damages in appropriate cases; and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of Damages.—

(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is 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 is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511 (5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$50 and not more than \$500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511 (5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$100 and not more than \$1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000.

(d) Defense.— A good faith reliance on—

- (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;
- (2) a request of an investigative or law enforcement officer under section 2518 (7) of this title; or
- (3) a good faith determination that section 2511 (3) or 2511 (2)(i) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation.— A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative Discipline.— If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper Disclosure Is Violation.— Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520 (a).

18 U.S.C. § 2521. Injunction against illegal interception

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

18 U.S.C. § 2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) Enforcement by Court Issuing Surveillance Order.— If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

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

(c) Civil Penalty.—

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

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

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

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

(C) such other matters as justice may require.

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

18 U.S.C. §§ 2701-2712 – Preservation and disclosure of stored wire and electronic communication

Title 18, Chapter 121 – STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

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

18 U.S.C. § 2701. Unlawful access to stored communications

- (a) Offense.**— Except as provided in subsection (c) of this section whoever—
- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
 - (2) intentionally exceeds an authorization to access that facility;
- and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.
- (b) Punishment.**— The punishment for an offense under subsection (a) of this section is—
- (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—
 - (A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and
 - (B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and
 - (2) in any other case—
 - (A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and
 - (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.
- (c) Exceptions.**— Subsection (a) of this section does not apply with respect to conduct authorized—
- (1) by the person or entity providing a wire or electronic communications service;
 - (2) by a user of that service with respect to a communication of or intended for that user; or
 - (3) in section 2703, 2704 or 2518 of this title.

18 U.S.C. § 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, § 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 U.S.C. § 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 subscriber 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 U.S.C. § 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 U.S.C. § 2705. Delayed notice

(a) Delay of Notification.—

(1) A governmental entity acting under section 2703 (b) of this title may—

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703 (b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703 (b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is—

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

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

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

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—

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

(B) informs such customer or subscriber—

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term “supervisory official” means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency’s headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney’s headquarters or regional office.

(b) Preclusion of Notice to Subject of Governmental Access.— A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703 (b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial

18 U.S.C. § 2706. Cost reimbursement

(a) Payment.— Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount.— The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception.— The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

18 U.S.C. § 2707. Civil action

(a) Cause of Action.— Except as provided in section 2703 (e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.— In a civil action under this section, appropriate relief includes—

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c); and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.— The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of \$1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) Administrative Discipline.— If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) Defense.— A good faith reliance on—

- (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703 (f) of this title);
 - (2) a request of an investigative or law enforcement officer under section 2518 (7) of this title; or
 - (3) a good faith determination that section 2511 (3) of this title permitted the conduct complained of;
- is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation.— A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) Improper Disclosure.— Any willful disclosure of a “record”, as that term is defined in section 552a (a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

18 U.S.C. § 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

18 U.S.C. § 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to Provide.— A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required Certification.— The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may—

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of Certain Disclosure.— No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by Bureau.— The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement That Certain Congressional Bodies Be Informed.— On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

18 U.S.C. § 2710. Wrongful disclosure of video tape rental or sale records

(a) Definitions.— For purposes of this section—

(1) the term “consumer” means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term “ordinary course of business” means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term “personally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term “video tape service provider” means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or

similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video Tape Rental and Sale Records.—

(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer—

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if—

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government 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 video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil Action.—

(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award—

(A) actual damages but not less than liquidated damages in an amount of \$2,500;

(B) punitive damages;

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

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

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) Personally Identifiable Information.— Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(e) Destruction of Old Records.— A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) Preemption.— The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

18 U.S.C. § 2711. Definitions for chapter

As used in this chapter—

- (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;
- (2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system; and
- (3) the term “court of competent jurisdiction” has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.

18 U.S.C. § 2712. Civil actions against the United States

(a) In General.— Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages—

- (1) actual damages, but not less than \$10,000, whichever amount is greater; and
- (2) litigation costs, reasonably incurred.

(b) Procedures.—

- (1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.
- (2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.
- (3) Any action under this section shall be tried to the court without a jury.
- (4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) **Administrative Discipline.**— If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) **Exclusive Remedy.**— Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) **Stay of Proceedings.**—

(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms “related criminal case” and “related investigation” mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

18 U.S.C. §§ 3121-3127 – Pen registers and trap and trace devices [relating to recording of dialing, routing, addressing and signaling information]

Title 18, Chapter 206 – PEN REGISTERS AND TRAP AND TRACE DEVICES

- § 3121. General prohibition on pen register and trap and trace device use; exception
- § 3122. Application for an order for a pen register or a trap and trace device
- § 3123. Issuance of an order for a pen register or a trap and trace device
- § 3124. Assistance in installation and use of a pen register or a trap and trace device
- § 3125. Emergency pen register and trap and trace device installation
- § 3126. Reports concerning pen registers and trap and trace devices
- § 3127. Definitions for chapter

18 U.S.C. § 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 signaling 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 U.S.C. § 3122. Application for an order for a pen register or a trap and trace device

(a) Application.—

- (1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.
- (2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or

approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

- (b) Contents of Application.**— An application under subsection (a) of this section shall include—
- (1)** the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
 - (2)** a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

18 U.S.C. § 3123. Issuance of an order for a pen register or a trap and trace device

(a) In General.—

(1) Attorney for the government.— Upon an application made under section 3122 (a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

(2) State investigative or law enforcement officer.— Upon an application made under section 3122 (a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3)

(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify—

- (i)** any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
- (ii)** the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
- (iii)** the configuration of the device at the time of its installation and any subsequent modification thereof; and
- (iv)** any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b) Contents of Order.— An order issued under this section—

- (1)** shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c) Time Period and Extensions.—

(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of Existence of Pen Register or a Trap and Trace Device.— An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that—

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

18 U.S.C. § 3124. Assistance in installation and use of a pen register or a trap and trace device

(a) Pen Registers.— Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123 (b)(2) of this title.

(b) Trap and Trace Device.— Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123 (b)(2) of

this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123 (b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation.— A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(d) 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 a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to section 3125 of this title.

(e) Defense.— A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(f) Communications Assistance Enforcement Orders.— Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

18 U.S.C. § 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(1) an emergency situation exists that involves—

(A) immediate danger of death or serious bodily injury to any person;

(B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use;

may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title.

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

18 U.S.C. § 3126. Reports concerning pen registers and trap and trace devices

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include information concerning—

- (1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- (2) the offense specified in the order or application, or extension of an order;
- (3) the number of investigations involved;
- (4) the number and nature of the facilities affected; and
- (5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

18 U.S.C. § 3127. Definitions for chapter

- (1) the terms “wire communication”, “electronic communication”, “electronic communication service”, and “contents” have the meanings set forth for such terms in section 2510 of this title;
- (2) the term “court of competent jurisdiction” means—
 - (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or
 - (B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;
- (3) the term “pen register” means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;
- (4) the term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;
- (5) the term “attorney for the Government” has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and
- (6) the term “State” means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.