USA

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 1 May 2020

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State: Party	
Signature of the Budapest Convention:	22/11/2001
Ratification/accession:	28/09/2006

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	18 USC 1030(e) 18 USC 2711 18 USC 3127
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when	**18 U.S.C. § 1030(a) (1) – (5)** **Sec. 1030. Fraud and related activity in connection with computers**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	(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;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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;
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**18 U.S.C. § 2511** **Sec. 2511. Interception and disclosure of wire, oral, or electronic communications prohibited** (1) Except as otherwise specifically provided in this chapter any person who - (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when - (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**18 U.S.C. § 1030(a)(5)** **Sec. 1030. Fraud and related activity in connection with computers** (a) Whoever - (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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;
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**18 U.S.C. § 1030(a)(5) (See above for statutory language)**
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with	**18 U.S.C. § 1029; 18 U.S.C. § 1030; 18 U.S.C. 2513** **Sec. 1029. Fraud and related activity in connection with access devices** (a) Whoever - (1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices; (2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period; (3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices; (4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment; (5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000; (6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of - (A) offering an access device; or (B) selling information regarding or an application to obtain an access device;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	(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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Sec. 1030. Fraud and related activity in connection with computers (See above for statutory language) **Sec. 2513. Confiscation of wire, oral, or electronic communication intercepting devices** Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**18 U.S.C. § 1028; 18 U.S.C. § 1029; 18 U.S.C. § 1030(a)(5)** **18 U.S.C. 1028 Fraud and related activity in connection with identification documents, authentication features, and information** 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;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 or a sponsoring entity of an event designated as a special event of national significance 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 or actual 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—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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,,[1] 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 a sponsoring entity of an event designated as a special event of national significance or the document-making implement is designed or suited

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 sponsoring entity of an event designated as a special event of national significance, 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—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 sponsoring entity of an event designated by the President as a special event of national significance, 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 sponsoring entity of an event designated by the President as a special event of national significance, 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;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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. § 1029 related activity in connection with access devices (See above for statutory language)** **18 U.S.C. 1030(a)(5) (See above for statuory language)**
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**18 U.S.C. § 1030(a)(4) and (a)(5); 18 U.S.C. § 1343** **18 U.S.C. § 1030(a)(4) and (a)(5) (See above for statutory language)** **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 occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**18 U.S.C. § 2251; 18 U.S.C. § 2252; 18 U.S.C. § 2252A** **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 or affecting 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 or for the purpose of transmitting a live 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 or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting 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 or for the purpose of transmitting a live 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 or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting 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 using any means or facility of interstate or foreign commerce or mail; or (B) the person transports such visual depiction to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce 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 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 using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(B) such notice or advertisement is transported using any means or facility of interstate or foreign commerce or in or affecting 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, section 1591, 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, abusive sexual contact involving a minor or ward, or sex trafficking of children, 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 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 underthis 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 not less than 30 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 using any means or facility of interstate or foreign commerce or in or affecting 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 using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 using any means or facility of interstate or foreign commerce or in or affecting 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, shipped, or transported using any means or facility of interstate or foreign commerce, or has been shipped or transported in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported using any means or facility of interstate or foreign commerce, 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, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction; or (B) knowingly possesses, or knowingly accesses with intent to view, 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 using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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, paragraph (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, section 1591, 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, or sex trafficking of children, 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 -

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 using any means or facility of interstate or foreign commerce or in or affecting 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 using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; (3) knowingly - (A) reproduces any child pornography for distribution through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer; or (B) advertises, promotes, presents, distributes, or solicits through the mails, or using any means or facility of interstate or foreign commerce or in or affecting 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	control of the United States Government, or in the Indian country (as defined in section 1151), knowingly sells or possesses with the intent tosell 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 using any means or facility of interstate or foreign commerce or in or affecting 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 or affecting 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, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography; or (B) knowingly possesses, or knowingly accesses with intent to view, 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 using any means or facility of interstate or foreign commerce or in or affecting 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 or affecting interstate or foreign commerce by any means, including by computer; (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 using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer; (B) that was produced using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(C) which distribution, offer, sending, or provision is accomplished using the mails or any means or facility of interstate or foreign commerce, for purposes of inducing or persuading a minor to participate in any activity that is illegal; or (7) knowingly produces with intent to distribute, or distributes, by any means, including a computer, in or affecting interstate or foreign commerce, child pornography that is an adapted or modified depiction of an identifiable minor.(!1) shall be punished as provided in subsection (b). (b) (1) Whoever violates, or attempts or conspires to violate, paragraph (1), (2), (3), (4), or (6) of subsection (a) shall be fined under this title and imprisoned not less than 5 years and not more than 20 years, but, if such person has a prior conviction under this chapter, section 1591, 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, or sex trafficking of children, 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. (3)Whoever violates, or attempts or conspires to violate, subsection (a)(7) shall be fined under this title or imprisoned not more than 15 years, or both. (c) It shall be an affirmative defense to a charge of violating paragraph (1), (2), (3)(A), (4), or (5) of subsection (a) that -

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 14 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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. (g) Child Exploitation Enterprises. - (1) Whoever engages in a child exploitation enterprise shall be fined under this title and imprisoned for any term of years not less than 20 or for life. (2) A person engages in a child exploitation enterprise for the purposes of this section if the person violates section 1591, section 1201 if the victim is a minor, or chapter 109A (involving a minor victim), 110 (except for sections 2257 and 2257A), or 117 (involving a minor victim), as a part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	**18 U.S.C. § 2319; 17 U.S.C. § 506** **18 U.S.C. § 2319. Criminal infringement of a copyright** (a) Any person who violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b), (c), and (d) 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)(A) 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	phonorecords, of 1 or more copyrighted works, which have a totalretail 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 felony and is a second or subsequent offense under subsection (a); 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)(1)(B) of title 17 - (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 felony and is a second or subsequent offense under subsection (a); 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) Any person who commits an offense under section 506(a)(1)(C) of title 17 - (1) shall be imprisoned not more than 3 years, fined under this title, or both; (2) shall be imprisoned not more than 5 years, fined under this title, or both, if the offense was committed for purposes of commercial advantage or private financial gain; (3) shall be imprisoned not more than 6 years, fined under this title, or both, if the offense is a felony and is a second or subsequent offense under subsection (a); and (4) shall be imprisoned not more than 10 years, fined under this title, or both, if the offense is a felony and is a second or subsequent offense under paragraph (2). (e) (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	suffered by the victim, including the estimated economic impact of the offense on that victim. (2) Persons permitted to submit victim impact statements 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. (f) 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; (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; (3) the term "financial gain" has the meaning given the term in section 101 of title 17; and (4) the term "work being prepared for commercial distribution" has the meaning given the term in section 506(a) of title 17. **17 U.S.C. § 506. Criminal offenses** (a) Criminal Infringement. - (1) In general. - Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed - (A) for purposes of commercial advantage or private financial gain; (B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phono records of 1 or more copyrighted works, which have a total retail value of more than $1,000; or (C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution. (2) Evidence. - For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright. (3) Definition. - In this subsection, the term "work being prepared for commercial distribution" means - (A) a computer program, a musical work, a motion picture or other audiovisual work, or a sound recording, if, at the time of unauthorized distribution –

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(i) the copyright owner has a reasonable expectation of commercial distribution; and (ii) the copies or phonorecords of the work have not been commercially distributed; or (B) a motion picture, if, at the time of unauthorized distribution, the motion picture - (i) has been made available for viewing in a motion picture exhibition facility; and (ii) has not been made available in copies for sale to the general public in the United States in a format intended to permit viewing outside a motion picture exhibition facility. (b) Forfeiture, Destruction, and Restitution. - Forfeiture, destruction, and restitution relating to this section shall be subject to section 2323 of title 18, to the extent provided in that section, in addition to any other similar remedies provided by law. (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).
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.	**18 U.S.C. § 2; 18 U.S.C. § 1030(c); 18 U.S.C. § 2251(d); 18 U.S.C. § 2252(b); 18 U.S.C. 2252A(b)** **18 U.S.C. § 2 Aiding and Abetting**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal. (b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal. **18 U.S.C. § 1030(c) Attempt (See above for statutory language)** **18 U.S.C. § 1029(b) (See above for statutory language)** **18 U.S.C. § 2251(d) (See above for statutory language)** **18 U.S.C. § 2252(b) (See above for statuatory language)** **18 U.S.C. § 2252A(b) (See above for statutory language)**
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.	Common Law recognizes corporate criminal as well as civil liability. See for example: **18 U.S.C. § 1030(e);** (e) As used in this section – (12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	Penalties for the above offenses are listed in the statutory language.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	The United States Constitution, federal law, regulations, policies, and multiple layers of oversight establish a complex system of safeguards that meet the requirements of the Convention on Cybercrime

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**18 U.S.C. § 2703 (f)** (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.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.	**18 U.S.C. § 2703 (f) (See above for statutory language)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**18 U.S.C. § 2703; 18 U.S.C. § 2713** **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 (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. 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 (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; 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-

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; (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; (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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. § 2713** A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data;	**Fourth Amendment to the United States Constitution; Federal Rule of Criminal Procedure 41; 18 U.S.C. § 2513** **Fourth Amendment** The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. **Fed. Rule of Crim. Proc. 41** (a) SCOPE AND DEFINITIONS. (1) *Scope.* This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances. (2) *Definitions.* The following definitions apply under this rule: (A) "Property" includes documents, books, papers, any other tangible objects, and information.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(B) "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time. (C) "Federal law enforcement officer" means a government agent (other than an attorney for the government) who is engaged in enforcing the criminal laws and is within any category of officers authorized by the Attorney General to request a search warrant. (D) "Domestic terrorism" and "international terrorism" have the meanings set out in 18 U.S.C. §2331. (E) "Tracking device" has the meaning set out in 18 U.S.C. §3117 (b). (b) VENUE FOR A WARRANT APPLICATION. At the request of a federal law enforcement officer or an attorney for the government: (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district; (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed; (3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district; (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following: (A) a United States territory, possession, or commonwealth;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state. (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts. (c) PERSONS OR PROPERTY SUBJECT TO SEARCH OR SEIZURE. A warrant may be issued for any of the following: (1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained. (d) OBTAINING A WARRANT. (1) *In General.* After receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device. (2) *Requesting a Warrant in the Presence of a Judge.* (A) *Warrant on an Affidavit*. When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(B) *Warrant on Sworn Testimony*. The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances. (C) *Recording Testimony*. Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit. (3) *Requesting a Warrant by Telephonic or Other Reliable Electronic Means.* In accordance with Rule 4.1, a magistrate judge may issue a warrant based on information communicated by telephone or other reliable electronic means. (e) ISSUING THE WARRANT. (1) *In General.* The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it. (2) *Contents of the Warrant.* (A) *Warrant to Search for and Seize a Person or Property.* Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: (i) execute the warrant within a specified time no longer than 14 days; (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and (iii) return the warrant to the magistrate judge designated in the warrant. (B) *Warrant Seeking Electronically Stored Information.* A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(C) *Warrant for a Tracking Device.* A tracking-device warrant must identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used. The time must not exceed 45 days from the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. The warrant must command the officer to: (i) complete any installation authorized by the warrant within a specified time no longer than 10 days; (ii) perform any installation authorized by the warrant during the daytime, unless the judge for good cause expressly authorizes installation at another time; and (iii) return the warrant to the judge designated in the warrant. (f) EXECUTING AND RETURNING THE WARRANT. (1) *Warrant to Search for and Seize a Person or Property.* (A) *Noting the Time.* The officer executing the warrant must enter on it the exact date and time it was executed. (B) *Inventory.* An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied. (C) *Receipt.* The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property. For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person. (D) *Return.* The officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant. The officer may do so by reliable electronic means. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant. (2) *Warrant for a Tracking Device.* (A) *Noting the Time.* The officer executing a tracking-device warrant must enter on it the exact date and time the device was installed and the period during which it was used. (B) *Return.* Within 10 days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant. The officer may do so by reliable electronic means. (C) *Service.* Within 10 days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in Rule 41(f)(3). (3) *Delayed Notice.* Upon the government's request, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—may delay any notice required by this rule if the delay is authorized by statute. (g) MOTION TO RETURN PROPERTY. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(h) MOTION TO SUPPRESS. A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides. (i) FORWARDING PAPERS TO THE CLERK. The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized. **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.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and	**18 U.S.C. § 3122 - 3125**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	18 U.S.C. § 3124 Asistance 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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, request pursuant to section 3125 of this title, or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523. **(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, a statutory authorization, or a good faith determination that the conduct complained of was permitted by an order from a foreign government that is subject to executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523, 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 Emegency 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or	**18 U.S.C. § 2516 Authorization for interception of wire, oral, or electronic communications** **(1)**The Attorney General, Deputy Attorney General, Associate Attorney General,[1] 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 or National Security 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	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 10 (relating to biological weapons), 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 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), 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 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit applications generally; renewals and discounts), section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials), 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 1581 (peonage), section 1582 (vessels for slave trade),

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	section 1583 (enticement into slavery), section 1584 (involuntary servitude), section 1585 (seizure, detention, transportation or sale of slaves), section 1586 (service on vessels in slave trade), section 1587 (possession of slaves aboard vessel), section 1588 (transportation of slaves from United States), section 1589 (forced labor), section 1590 (trafficking with respect to peonage, slavery, involuntary servitude, or forced labor), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1592 (unlawful conduct with respect to documents in furtherance of trafficking, peonage, slavery, involuntary servitude, or forced labor), 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), section 1992 (relating to terrorist attacks against mass transportation), 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 2340A (relating to torture), 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 956 (conspiracy to harm persons or property overseas), 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), section 1546 (relating to fraud and misuse of visas, permits, and other documents), or section 555 (relating to construction or use of international border tunnels); **(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), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited); **(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;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline), section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) 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), section 1028A (relating to aggravated identity theft) 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 [2] **(q)** any criminal violation of section 229 (relating to chemical weapons) or section 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h [3] 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism); **(r)** any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, 2, 3); **(s)** any violation of section 670 (relating to theft of medical products); **(t)** any violation of the Export Control Reform Act of 2018; or **(u)** 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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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, kidnapping, human trafficking, child sexual exploitation, child pornography production, prostitution, 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. **See Also the Communications Assistance for Law Enforcement Act, 47 U.S.C. §§1001-1010, available here.**
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or	**18 U.S.C. §§ 3231 (District courts), 3238 (Offenses not commited in any district)** **Section 3231**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	The district courts of the United States shall have original jurisdiction, exclusive of the courts of the States, of all offenses against the laws of the United States. Nothing in this title shall be held to take away or impair the jurisdiction of the courts of the several States under the laws thereof. **Section 3238** The trial of all offenses begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, shall be in the district in which the offender, or any one of two or more joint offenders, is arrested or is first brought; but if such offender or offenders are not so arrested or brought into any district, an indictment or information may be filed in the district of the last known residence of the offender or of any one of two or more joint offenders, or if no such residence is known the indictment or information may be filed in the District of Columbia.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences	The United States has extradition treaties in force with a large number of countries. [A list of these treaties can be found in the notes following 18 U.S.C. § 3181.] In addition, the following laws pertain to the extradition of offenders from the United States to other countries: **18 U.S.C. § 3181. Scope and limitation of chapter.** **(a)** The provisions of this chapter relating to the surrender of persons who have committed crimes in foreign countries shall continue in force only during the existence of any treaty of extradition with such foreign government. **(b)**The provisions of this chapter shall be construed to permit, in the exercise of comity, the surrender of persons, other than citizens, nationals, or permanent residents of the United States, who have committed crimes of violence against nationals of the United States in foreign countries without regard to the existence of any treaty of extradition with such foreign government if the Attorney General certifies, in writing, that—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	**(1)** evidence has been presented by the foreign government that indicates that had the offenses been committed in the United States, they would constitute crimes of violence as defined under section 16 of this title; and **(2)** the offenses charged are not of a political nature. **(c)** As used in this section, the term "national of the United States" has the meaning given such term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22)). **18 U.S.C. § 3184. Fugitives from foreign country to United States** Whenever there is a treaty or convention for extradition between the United States and any foreign government, or in cases arising under section 3181(b), any justice or judge of the United States, or any magistrate judge authorized so to do by a court of the United States, or any judge of a court of record of general jurisdiction of any State, may, upon complaint made under oath, charging any person found within his jurisdiction, with having committed within the jurisdiction of any such foreign government any of the crimes provided for by such treaty or convention, or provided for under section 3181(b), issue his warrant for the apprehension of the person so charged, that he may be brought before such justice, judge, or magistrate judge, to the end that the evidence of criminality may be heard and considered. Such complaint may be filed before and such warrant may be issued by a judge or magistrate judge of the United States District Court for the District of Columbia if the whereabouts within the United States of the person charged are not known or, if there is reason to believe the person will shortly enter the United States. If, on such hearing, he deems the evidence sufficient to sustain the charge under the provisions of the proper treaty or convention, or under section 3181(b), he shall certify the same, together with a copy of all the testimony taken before him, to the Secretary of State, that a warrant may issue upon the requisition of the proper authorities of such foreign government, for the surrender of such person, according to the stipulations of the treaty or convention; and he shall issue his warrant for the commitment of the person so charged to the proper jail, there to remain until such surrender shall be made. **18 U.S.C. § 3186. Secretary of State to surrender fugitive**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	The Secretary of State may order the person committed under sections 3184 or 3185 of this title to be delivered to any authorized agent of such foreign government, to be tried for the offense of which charged. Such agent may hold such person in custody, and take him to the territory of such foreign government, pursuant to such treaty. A person so accused who escapes may be retaken in the same manner as any person accused of any offense. **18 U.S.C. § 3188. Time of commitment pending extradition** Whenever any person who is committed for rendition to a foreign government to remain until delivered up in pursuance of a requisition, is not so delivered up and conveyed out of the United States within two calendar months after such commitment, over and above the time actually required to convey the prisoner from the jail to which he was committed, by the readiest way, out of the United States, any judge of the United States, or of any State, upon application made to him by or on behalf of the person so committed, and upon proof made to him that reasonable notice of the intention to make such application has been given to the Secretary of State, may order the person so committed to be discharged out of custody, unless sufficient cause is shown to such judge why such discharge ought not to be ordered. **18 U.S.C. § 3189. Place and character of hearing.** Hearings in cases of extradition under treaty stipulation or convention shall be held on land, publicly, and in a room or office easily accessible to the public. **18 U.S.C. § 3190. Evidence on hearing.** Depositions, warrants, or other papers or copies thereof offered in evidence upon the hearing of any extradition case shall be received and admitted as evidence on such hearing for all the purposes of such hearing if they shall be properly and legally authenticated so as to entitle them to be received for similar purposes by the tribunals of the foreign country from which the accused party shall have escaped, and the certificate of the principal diplomatic or consular officer of the United States resident in such foreign country shall be proof that the same, so offered, are authenticated in the manner required.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	18.U.S.C. § 3191. Witneses for indigent fugitives. On the hearing of any case under a claim of extradition by a foreign government, upon affidavit being filed by the person charged setting forth that there are witnesses whose evidence is material to his defense, that he cannot safely go to trial without them, what he expects to prove by each of them, and that he is not possessed of sufficient means, and is actually unable to pay the fees of such witnesses, the judge or magistrate judge hearing the matter may order that such witnesses be subpenaed; and the costs incurred by the process, and the fees of witnesses, shall be paid in the same manner as in the case of witnesses subpenaed in behalf of the United States. **18 U.S.C. § 3192. Protection of accused.** Whenever any person is delivered by any foreign government to an agent of the United States, for the purpose of being brought within the United States and tried for any offense of which he is duly accused, the President shall have power to take all necessary measures for the transportation and safekeeping of such accused person, and for his security against lawless violence, until the final conclusion of his trial for the offenses specified in the warrant of extradition, and until his final discharge from custody or imprisonment for or on account of such offenses, and for a reasonable time thereafter, and may employ such portion of the land or naval forces of the United States, or of the militia thereof, as may be necessary for the safe-keeping and protection of the accused. **18 U.S.C. § 3193. Receiving agent's authority over offenders.** A duly appointed agent to receive, in behalf of the United States, the delivery, by a foreign government, of any person accused of crime committed within the United States, and to convey him to the place of his trial, shall have all the powers of a marshal of the United States, in the several districts through which it may be necessary for him to pass with such prisoner, so far as such power is requisite for the prisoner's safe-keeping. **18 U.S.C. § 3195 Payment of fees and costs.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	All costs or expenses incurred in any extradition proceeding in apprehending, securing, and transmitting a fugitive shall be paid by the demanding authority. All witness fees and costs of every nature in cases of international extradition, including the fees of the magistrate judge, shall be certified by the judge or magistrate judge before whom the hearing shall take place to the Secretary of State of the United States, and the same shall be paid out of appropriations to defray the expenses of the judiciary or the Department of Justice as the case may be. The Attorney General shall certify to the Secretary of State the amounts to be paid to the United States on account of said fees and costs in extradition cases by the foreign government requesting the extradition, and the Secretary of State shall cause said amounts to be collected and transmitted to the Attorney General for deposit in the Treasury of the United States. **18 U.S.C. § 3196. Extradition of United States citizens.** If the applicable treaty or convention does not obligate the United States to extradite its citizens to a foreign country, the Secretary of State may, nevertheless, order the surrender to that country of a United States citizen whose extradition has been requested by that country if the other requirements of that treaty or convention are met.
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.	The United States has mutual assistance treaties in force with a large number of countries. In addition, 18 U.S.C. § 3512 pertains to mutual assistance between the United States and other countries: **18 U.S.C. § 3512 Foreign requests for assistance in criminal investigations and prosecutions** **(a)EXECUTION OF REQUEST FOR ASSISTANCE.—** **(1)IN GENERAL.—** Upon application, duly authorized by an appropriate official of the Department of Justice, of an attorney for the Government, a Federal judge may issue such orders as may be necessary to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses, or in proceedings related to the prosecution of criminal offenses, including proceedings regarding forfeiture, sentencing, and restitution. **(2)SCOPE OF ORDERS.—**Any order issued by a Federal judge pursuant to paragraph (1) may include the issuance of—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	**(A)** a search warrant, as provided under Rule 41 of the Federal Rules of Criminal Procedure; **(B)** a warrant or order for contents of stored wire or electronic communications or for records related thereto, as provided under section 2703 of this title; **(C)** an order for a pen register or trap and trace device as provided under section 3123 of this title; or **(D)** an order requiring the appearance of a person for the purpose of providing testimony or a statement, or requiring the production of documents or other things, or both. **(b)APPOINTMENT OF PERSONS TO TAKE TESTIMONY OR STATEMENTS.—** **(1)IN GENERAL.—** In response to an application for execution of a request from a foreign authority as described under subsection (a), a Federal judge may also issue an order appointing a person to direct the taking of testimony or statements or of the production of documents or other things, or both. **(2)AUTHORITY OF APPOINTED PERSON.—**Any person appointed under an order issued pursuant to paragraph (1) may— **(A)** issue orders requiring the appearance of a person, or the production of documents or other things, or both; **(B)** administer any necessary oath; and **(C)** take testimony or statements and receive documents or other things. **(c)FILING OF REQUESTS.—**Except as provided under subsection (d), an application for execution of a request from a foreign authority under this section may be filed— **(1)** in the district in which a person who may be required to appear resides or is located or in which the documents or things to be produced are located; **(2)** in cases in which the request seeks the appearance of persons or production of documents or things that may be located in multiple districts, in any one of the districts in which such a person, documents, or things may be located; or **(3)** in any case, the district in which a related Federal criminal investigation or prosecution is being conducted, or in the District of Columbia. **(d)SEARCH WARRANT LIMITATION.—** An application for execution of a request for a search warrant from a foreign authority under this section, other than an application for a warrant issued as

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	provided under section 2703 of this title, shall be filed in the district in which the place or person to be searched is located. **(e)SEARCH WARRANT STANDARD.—** A Federal judge may issue a search warrant under this section only if the foreign offense for which the evidence is sought involves conduct that, if committed in the United States, would be considered an offense punishable by imprisonment for more than one year under Federal or State law. **(f)SERVICE OF ORDER OR WARRANT.—** Except as provided under subsection (d), an order or warrant issued pursuant to this section may be served or executed in any place in the United States. **(g)RULE OF CONSTRUCTION.—** Nothing in this section shall be construed to preclude any foreign authority or an interested person from obtaining assistance in a criminal investigation or prosecution pursuant to section 1782 of title 28, United States Code. **(h)DEFINITIONS.—**As used in this section, the following definitions shall apply: **(1)FEDERAL JUDGE.—** The terms "Federal judge" and "attorney for the Government" have the meaning given such terms for the purposes of the Federal Rules of Criminal Procedure. **(2)FOREIGN AUTHORITY.—** The term "foreign authority" means a foreign judicial authority, a foreign authority responsible for the investigation or prosecution of criminal offenses or for proceedings related to the prosecution of criminal offenses, or an authority designated as a competent authority or central authority for the purpose of making requests for assistance pursuant to an agreement or treaty with the United States regarding assistance in criminal matters.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.	A large number of United States laws govern the use of information by U.S. law enforcement agencies and permit them to share information spontaneously with their counterparts in other countries when in accordance with applicable law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	The United States has a large number of mutual assistance treaties, including with most Parties to the Convention (see response to Article 25 above). In the absence thereof, the Convention serves as the legal basis for implementing Article 27.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	See response to Article 27 above.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence;	**18 U.S.C. § 2703(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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	The United States applies its mutual assistance treaties and 18 U.S.C. § 3512 (see above); see response to Article 25 above.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	The United States applies its mutual assistance treaties and 18 U.S.C. § 3512 (see above); see response to Article 25 above.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and	General principles of United States law permit the collection of publicly available information and of information with consent. In addition, 18 U.S.C. § 2703(b)(3) may apply with respect to voluntary consent: **18 U.S.C. § 2702(b)(3). Voluntary disclosure of customer communications or records** **(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—**A provider described in subsection (a) may divulge the contents of a communication—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	. . . **(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;
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	The United States applies its mutual assistance treaties and 18 U.S.C. § 3512 (see above); see response to Article 25 above.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	Assistance under Article 34 is to be provided to the extent permitted by the Parties' applicable treaties and domestic laws. U.S. domestic law currently does not permit the real-time collection or recording of content data in response to a mutual assistance request concerning a purely foreign investigation. However, United States law permits providers to disclose real-time content data pursuant to an executive agreement under the CLOUD Act, 18 USC § 2523. **18 USC § 2523. Executive agreements on access to data by foreign governments.** **(a)DEFINITIONS.—**In this section— **(1)** the term "lawfully admitted for permanent residence" has the meaning given the term in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)); and **(2)** the term "United States person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States. **(b)EXECUTIVE AGREEMENT REQUIREMENTS.—**For purposes of this chapter, chapter 121, and chapter 206, an executive agreement governing access by a foreign government to data subject to this chapter, chapter 121, or chapter 206 shall be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	considered to satisfy the requirements of this section if the Attorney General, with the concurrence of the Secretary of State, determines, and submits a written certification of such determination to Congress, including a written certification and explanation of each consideration in paragraphs (1), (2), (3), and (4), that— **(1)**the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, if— **(A)** such a determination under this section takes into account, as appropriate, credible information and expert input; and **(B)**the factors to be met in making such a determination include whether the foreign government— **(i)** has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated by being a party to the Convention on Cybercrime, done at Budapest November 23, 2001, and entered into force January 7, 2004, or through domestic laws that are consistent with definitions and the requirements set forth in chapters I and II of that Convention; **(ii)** demonstrates respect for the rule of law and principles of nondiscrimination; **(iii)**adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights, including— **(I)** protection from arbitrary and unlawful interference with privacy; **(II)** fair trial rights; **(III)** freedom of expression, association, and peaceful assembly; **(IV)** prohibitions on arbitrary arrest and detention; and **(V)** prohibitions against torture and cruel, inhuman, or degrading treatment or punishment; **(iv)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities; **(v)** has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government; and **(vi)** demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet; **(2)** the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement; **(3)** the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data; and **(4)**the agreement requires that, with respect to any order that is subject to the agreement— **(A)** the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement; **(B)** the foreign government may not target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States; **(C)** the foreign government may not issue an order at the request of or to obtain information to provide to the United States Government or a third-party government, nor shall the foreign government be required to share any

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	information produced with the United States Government or a third-party government; **(D)**an order issued by the foreign government— **(i)** shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism; **(ii)** shall identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order; **(iii)** shall be in compliance with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law; **(iv)** shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation; **(v)** shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order; and **(vi)**in the case of an order for the interception of wire or electronic communications, and any extensions thereof, shall require that the interception order— **(I)** be for a fixed, limited duration; and **(II)** may not last longer than is reasonably necessary to accomplish the approved purposes of the order; and **(III)** be issued only if the same information could not reasonably be obtained by another less intrusive method; **(E)** an order issued by the foreign government may not be used to infringe freedom of speech;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(F) the foreign government shall promptly review material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those persons trained in applicable procedures; **(G)** the foreign government shall, using procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily harm to any person; **(H)** the foreign government may not disseminate the content of a communication of a United States person to United States authorities unless the communication may be disseminated pursuant to subparagraph (G) and relates to significant harm, or the threat thereof, to the United States or United States persons, including crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud; **(I)** the foreign government shall afford reciprocal rights of data access, to include, where applicable, removing restrictions on communications service providers, including providers subject to United States jurisdiction, and thereby allow them to respond to valid legal process sought by a governmental entity (as defined in section 2711) if foreign law would otherwise prohibit communications-service providers from disclosing the data; **(J)** the foreign government shall agree to periodic review of compliance by the foreign government with the terms of the agreement to be conducted by the United States Government; and **(K)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the United States Government shall reserve the right to render the agreement inapplicable as to any order for which the United States Government concludes the agreement may not properly be invoked. **(c)LIMITATION ON JUDICIAL REVIEW.—** A determination or certification made by the Attorney General under subsection (b) shall not be subject to judicial or administrative review. **(d)EFFECTIVE DATE OF CERTIFICATION.—** **(1)NOTICE.—**Not later than 7 days after the date on which the Attorney General certifies an executive agreement under subsection (b), the Attorney General shall provide notice of the determination under subsection (b) and a copy of the executive agreement to Congress, including— **(A)** the Committee on the Judiciary and the Committee on Foreign Relations of the Senate; and **(B)** the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives. **(2)ENTRY INTO FORCE.—** An executive agreement that is determined and certified by the Attorney General to satisfy the requirements of this section shall enter into force not earlier than the date that is 180 days after the date on which notice is provided under paragraph (1), unless Congress enacts a joint resolution of disapproval in accordance with paragraph (4). **(3)REQUESTS FOR INFORMATION.—** Upon request by the Chairman or Ranking Member of a congressional committee described in paragraph (1), the head of an agency shall promptly furnish a summary of factors considered in determining that the foreign government satisfies the requirements of this section. **(4)CONGRESSIONAL REVIEW.—** **(A)**Joint resolution defined.—In this paragraph, the term "joint resolution" means only a joint resolution— **(i)** introduced during the 180-day period described in paragraph (2); **(ii)** which does not have a preamble;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iii) the title of which is as follows: "Joint resolution disapproving the executive agreement signed by the United States and __.", the blank space being appropriately filled in; and **(iv)** the matter after the resolving clause of which is as follows: "That Congress disapproves the executive agreement governing access by ___ to certain electronic data as submitted by the Attorney General on ___", the blank spaces being appropriately filled in. **(B)**Joint resolution enacted.— Notwithstanding any other provision of this section, if not later than 180 days after the date on which notice is provided to Congress under paragraph (1), there is enacted into law a joint resolution disapproving of an executive agreement under this section, the executive agreement shall not enter into force. **(C)**Introduction.—During the 180-day period described in subparagraph (B), a joint resolution of disapproval may be introduced— **(i)** in the House of Representatives, by the majority leader or the minority leader; and **(ii)** in the Senate, by the majority leader (or the majority leader's designee) or the minority leader (or the minority leader's designee). **(5)FLOOR CONSIDERATION IN HOUSE OF REPRESENTATIVES.—** If a committee of the House of Representatives to which a joint resolution of disapproval has been referred has not reported the joint resolution within 120 days after the date of referral, that committee shall be discharged from further consideration of the joint resolution. **(6)CONSIDERATION IN THE SENATE.—** **(A)**Committee referral.—A joint resolution of disapproval introduced in the Senate shall be referred jointly— **(i)** to the Committee on the Judiciary; and **(ii)** to the Committee on Foreign Relations.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(B) Reporting and discharge.— If a committee to which a joint resolution of disapproval was referred has not reported the joint resolution within 120 days after the date of referral of the joint resolution, that committee shall be discharged from further consideration of the joint resolution and the joint resolution shall be placed on the appropriate calendar. **(C)**Proceeding to consideration.— It is in order at any time after both the Committee on the Judiciary and the Committee on Foreign Relations report a joint resolution of disapproval to the Senate or have been discharged from consideration of such a joint resolution (even though a previous motion to the same effect has been disagreed to) to move to proceed to the consideration of the joint resolution, and all points of order against the joint resolution (and against consideration of the joint resolution) are waived. The motion is not debatable or subject to a motion to postpone. A motion to reconsider the vote by which the motion is agreed to or disagreed to shall not be in order. **(D)**Consideration in the senate.— In the Senate, consideration of the joint resolution, and on all debatable motions and appeals in connection therewith, shall be limited to not more than 10 hours, which shall be divided equally between those favoring and those opposing the joint resolution. A motion further to limit debate is in order and not debatable. An amendment to, or a motion to postpone, or a motion to proceed to the consideration of other business, or a motion to recommit the joint resolution is not in order. **(E)**Consideration of veto messages.— Debate in the Senate of any veto message with respect to a joint resolution of disapproval, including all debatable motions and appeals in connection with the joint resolution, shall be limited to 10 hours, to be equally divided between, and controlled by, the majority leader and the minority leader or their designees. **(7)RULES RELATING TO SENATE AND HOUSE OF REPRESENTATIVES.—** **(A)**Treatment of senate joint resolution in house.—In the House of Representatives, the following procedures shall apply to a joint resolution of disapproval received from the Senate (unless the House has already passed a joint resolution relating to the same proposed action):

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(i) The joint resolution shall be referred to the appropriate committees. **(ii)** If a committee to which a joint resolution has been referred has not reported the joint resolution within 7 days after the date of referral, that committee shall be discharged from further consideration of the joint resolution. **(iii)** Beginning on the third legislative day after each committee to which a joint resolution has been referred reports the joint resolution to the House or has been discharged from further consideration thereof, it shall be in order to move to proceed to consider the joint resolution in the House. All points of order against the motion are waived. Such a motion shall not be in order after the House has disposed of a motion to proceed on the joint resolution. The previous question shall be considered as ordered on the motion to its adoption without intervening motion. The motion shall not be debatable. A motion to reconsider the vote by which the motion is disposed of shall not be in order. **(iv)** The joint resolution shall be considered as read. All points of order against the joint resolution and against its consideration are waived. The previous question shall be considered as ordered on the joint resolution to final passage without intervening motion except 2 hours of debate equally divided and controlled by the sponsor of the joint resolution (or a designee) and an opponent. A motion to reconsider the vote on passage of the joint resolution shall not be in order. **(B)**Treatment of house joint resolution in senate.— **(i)**If, before the passage by the Senate of a joint resolution of disapproval, the Senate receives an identical joint resolution from the House of Representatives, the following procedures shall apply: **(I)** That joint resolution shall not be referred to a committee. **(II)**With respect to that joint resolution— **(aa)** the procedure in the Senate shall be the same as if no joint resolution had been received from the House of Representatives; but **(bb)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the vote on passage shall be on the joint resolution from the House of Representatives. **(ii)** If, following passage of a joint resolution of disapproval in the Senate, the Senate receives an identical joint resolution from the House of Representatives, that joint resolution shall be placed on the appropriate Senate calendar. **(iii)** If a joint resolution of disapproval is received from the House, and no companion joint resolution has been introduced in the Senate, the Senate procedures under this subsection shall apply to the House joint resolution. **(C)**Application to revenue measures.— The provisions of this paragraph shall not apply in the House of Representatives to a joint resolution of disapproval that is a revenue measure. **(8)RULES OF HOUSE OF REPRESENTATIVES AND SENATE.—**This subsection is enacted by Congress— **(A)** as an exercise of the rulemaking power of the Senate and the House of Representatives, respectively, and as such is deemed a part of the rules of each House, respectively, and supersedes other rules only to the extent that it is inconsistent with such rules; and **(B)** with full recognition of the constitutional right of either House to change the rules (so far as relating to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House. **(e)RENEWAL OF DETERMINATION.—** **(1)IN GENERAL.—** The Attorney General, with the concurrence of the Secretary of State, shall review and may renew a determination under subsection (b) every 5 years. **(2)REPORT.—**Upon renewing a determination under subsection (b), the Attorney General shall file a report with the Committee on the Judiciary and the Committee on Foreign Relations of the Senate and the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives describing—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(A) the reasons for the renewal; **(B)** any substantive changes to the agreement or to the relevant laws or procedures of the foreign government since the original determination or, in the case of a second or subsequent renewal, since the last renewal; and **(C)** how the agreement has been implemented and what problems or controversies, if any, have arisen as a result of the agreement or its implementation. **(3)NONRENEWAL.—** If a determination is not renewed under paragraph (1), the agreement shall no longer be considered to satisfy the requirements of this section. **(f)REVISIONS TO AGREEMENT.—**A revision to an agreement under this section shall be treated as a new agreement for purposes of this section and shall be subject to the certification requirement under subsection (b), and to the procedures under subsection (d), except that for purposes of a revision to an agreement— **(1)** the applicable time period under paragraphs (2), (4)(A)(i), (4)(B), and (4)(C) of subsection (d) shall be 90 days after the date notice is provided under subsection (d)(1); and **(2)** the applicable time period under paragraphs (5) and (6)(B) of subsection (d) shall be 60 days after the date notice is provided under subsection (d)(1). **(g)PUBLICATION.—** Any determination or certification under subsection (b) regarding an executive agreement under this section, including any termination or renewal of such an agreement, shall be published in the Federal Register as soon as is reasonably practicable. **(h)MINIMIZATION PROCEDURES.—** A United States authority that receives the content of a communication described in subsection (b)(4)(H) from a foreign government in accordance with an executive agreement under this section shall use procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	1801) to appropriately protect nonpublicly available information concerning United States persons.
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** Pursuant to Article 35, paragraph 1, of the Convention, the Computer Crime and Intellectual Property Section, United States Department of Justice, Criminal Division, Washington, D.C., 20530, is designated as the point of contact available on a twenty-four hour, seven-day-a-week basis to ensure the provision of immediate assistance under the Convention. Contact Information for the Computer Crime and Intellectual Property Section is given below :24/7 Contact: United States of America **Contact and Telephone Number:** Computer Crime and Intellectual Property Section (CCIPS) U.S. Department of Justice, Washington, DC **Description of Contact** CCIPS is a section of the Criminal Division of the U.S. Department of Justice that has 40 lawyers with responsibilities for combating cybercrime and theft of intellectual property, and with expertise in obtaining electronic evidence. Many CCIPS lawyers also have expertise in international assistance. CCIPS has "duty attorneys" available 24-hours a day, 7 days a week to respond to urgent requests for assistance. Language Capabilities of the Contact : **English**
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11,	**Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America declares, pursuant to Articles 2 and 40, that under United States law, the offenses set forth in Article 2 ("Illegal access") includes an additional requirement of intent to obtain computer data. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 2

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	**Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America declares, pursuant to Articles 6 and 40, that under United States law, the offense set forth in paragraph (1) (b) of Article 6 ("Misuse of devices") includes a requirement that a minimum number of items be possessed. The minimum number shall be the same as that provided for by applicable United States federal law. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 6 **Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America declares, pursuant to Articles 7 and 40, that under United States law, the offense set forth in Article 7 ("Computer-related forgery") includes a requirement of intent to defraud. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 7 **Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America declares, pursuant to Articles 27 and 40, that requests made to the United States under paragraph 9(e) of Article 27 ("Procedures pertaining to mutual assistance requests in the absence of applicable international agreements") are to be addressed to its central authority for mutual assistance. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 27 **Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America, pursuant to Articles 4 and 42 of the Convention, reserves the right to require that the conduct result in serious harm, which shall be determined in accordance with applicable United States federal law. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 4 **Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	The United States of America, pursuant to Articles 6 and 42 of the Convention, reserves the right not to apply paragraphs (1) (a) (i) and (1) (b) of Article 6 ("Misuses of devices") with respect to devices designed or adapted primarily for the purpose of committing the offenses established in Article 4 ("Data interference") and Article 5 ("System interference"). **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 6 **Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America, pursuant to Articles 9 and 42 of the Convention, reserves the right to apply paragraphs (2) (b) and (c) of Article 9 only to the extent consistent with the Constitution of the United States as interpreted by the United States and as provided for under its federal law, which includes, for example, crimes of distribution of material considered to be obscene under applicable United States standards. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 9 **Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America, pursuant to Articles 10 and 42 of the Convention, reserves the right to impose other effective remedies in lieu of criminal liability under paragraphs 1 and 2 of Article 10 ("Offenses related to infringement of copyright and related rights") with respect to infringements of certain rental rights to the extent the criminalisation of such infringements is not required pursuant to the obligations the United States has undertaken under the agreements referenced in paragraphs 1 and 2. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 10 **Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America, pursuant to Articles 22 and 42 of the Convention, reserves the right not to apply in part paragraphs (1) (b), (c) and (d) of Article 22 ("Jurisdiction"). The United States does not provide for plenary jurisdiction over offenses that are committed outside its territory by its citizens or on board ships flying its flag or aircraft registered under its laws. However, United States law does provide for jurisdiction over a number of offenses to be established under the Convention that are committed abroad by United States nationals in circumstances implicating particular federal interests, as well as over a number of such offenses committed on board United States-flagged ships or aircraft registered under

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	United States law. Accordingly, the United States will implement paragraphs (1) (b), (c) and (d) to the extent provided for under its federal law. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 22 **Reservation contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** The United States of America, pursuant to Articles 41 and 42 of the Convention, reserves the right to assume obligations under Chapter II of the Convention in a manner consistent with its fundamental principles of federalism. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 41 **Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** Pursuant to Article 24, paragraph 7, of the Convention, the United States of America is not designating an authority responsible for extradition or provisional arrest in the absence of a treaty, as the United States will continue to rely on bilateral extradition treaties, and the authority responsible for making or receiving extradition requests on behalf of the United States is set forth in the applicable bilateral extradition treaties. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 24 **Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** Pursuant to Article 27, paragraph 2, of the Convention, the Office of International Affairs, United States Department of Justice, Criminal Division, Washington, D.C., 20530, is designated as the central authority of the United States of America for mutual assistance under the Convention. **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 27 **Declaration contained in the instrument of ratification deposited on 29 September 2006 - Or. Engl.** Pursuant to Article 35, paragraph 1, of the Convention, the Computer Crime and Intellectual Property Section, United States Department of Justice, Criminal Division, Washington, D.C., 20530, is designated as the point of contact available on a twenty-four hour, seven-day-a-week basis to ensure the provision of immediate assistance under the Convention. Contact

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Information for the Computer Crime and Intellectual Property Section is given below :24/7 Contact: United States of America **Contact and Telephone Number:** Computer Crime and Intellectual Property Section (CCIPS) U.S. Department of Justice, Washington, DC Tel: +1-202-514-1026 / Monday - Friday 0900 - 1800 hrs Tel: +1-202-353-5216 / Mon - Fri after hours, Saturdays, Sundays, holidays Tel: +1-202-514-6113 / Always on, but only monitored Monday - Friday 0900 - 1800 hrs **Description of Contact** CCIPS is a section of the Criminal Division of the U.S. Department of Justice that has 40 lawyers with responsibilities for combating cybercrime and theft of intellectual property, and with expertise in obtaining electronic evidence. Many CCIPS lawyers also have expertise in international assistance. CCIPS has "duty attorneys" available 24-hours a day, 7 days a week to respond to urgent requests for assistance. **Language Capabilities of the Contact** : English **What To Say When Calling Contact Number** : *During business hours*, call +1-202-514-1026. Tell the receptionist (1) that you have "a cybercrime 24-7 request"; (2) from what country you are calling; and (3) that you want to be connected to "a duty attorney". *After business hours* and on Saturdays, Sundays and holidays, call +1-202-353-5216. Your call will be connected directly to a duty attorney. **Fax Information** : +1-202-514-6113. This fax machine operates 24 hours a day, 7 days a week, but faxes sent outside of normal working hours will not receive attention until the next business day. **Time Zone** : UTC/GMT -05:00 (Daylight Savings Time : +01:00) **Period covered: 1/1/2007 -** The preceding statement concerns Article(s) : 35

Back to the Table of Contents