108TH CONGRESS
1st Session

SENATE

TREATY DOC.
108–11

CONVENTION ON CYBERCRIME

MESSAGE

FROM

THE PRESIDENT OF THE UNITED STATES

TRANSMITTING

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (THE "CYBERCRIME CONVENTION" OR THE "CONVENTION"), WHICH WAS SIGNED BY THE UNITED STATES ON NOVEMBER 23, 2001

NOVEMBER 17, 2003.—Convention was read the first time, and together with the accompanying papers, referred to the Committee on Foreign Relations and ordered to be printed for the use of the Senate

---

U.S. GOVERNMENT PRINTING OFFICE

29–118

WASHINGTON : 2003

LETTER OF TRANSMITTAL

THE WHITE HOUSE,
November 17, 2003.

To the Senate of the United States:

With a view to receiving the advice and consent of the Senate to ratification, I transmit herewith the Council of Europe Convention on Cybercrime (the "Cybercrime Convention" or the "Convention"), which was signed by the United States on November 23, 2001. In addition, for the information of the Senate, I transmit the report of the Department of State with respect to the Convention and the Convention's official Explanatory Report.

The United States, in its capacity as an observer at the Council of Europe, participated actively in the elaboration of the Convention, which is the only multilateral treaty to address the problems of computer-related crime and electronic evidence gathering. An overview of the Convention's provisions is provided in the report of the Department of State. The report also sets forth proposed reservations and declarations that would be deposited by the United States with its instrument of ratification. With these reservations and declarations, the Convention would not require implementing legislation for the United States.

The Convention promises to be an effective tool in the global effort to combat computer-related crime. It requires Parties to criminalize, if they have not already done so, certain conduct that is committed through, against, or related to computer systems. Such substantive crime include offenses against the "confidentiality, integrity and availability" of computer data and systems, as well as using computer systems to engage in conduct that would be criminal if committed outside the cyber-realm, i.e., forgery, fraud, child pornography, and certain copyright-related offenses. The Convention also requires Parties to have the ability to investigate computer-related crime effectively and to obtain electronic evidence in all types of criminal investigations and proceedings.

By providing for broad international cooperation in the form of extradition and mutual legal assistance, the Cybercrime Convention would remove or minimize legal obstacles to international cooperation that delay or endanger U.S. investigations and prosecutions of computer-related crime. As such, it would help deny "safe havens" to criminals, including terrorists, who can cause damage to U.S. interests from abroad using computer systems. At the same time, the Convention contains safeguards that protect civil liberties and other legitimate interests.

I recommend that the Senate give early and favorable consideration to the Cybercrime Convention, and that it give its advice and consent to ratification, subject to the reservations, declarations,

and understanding described in the accompanying report of the Department of State.

GEORGE W. BUSH.

LETTER OF SUBMITTAL

DEPARTMENT OF STATE,
Washington, September 11, 2003.

The PRESIDENT,
The White House.

THE PRESIDENT: I have the honor to submit to you, with a view to its transmittal to the Senate for advice and consent to ratification, the Council of Europe ("COE") Convention on Cybercrime ("the Cybercrime Convention" or "the Convention"), which was adopted by the COE's Committee of Ministers on November 8, 2001. On November 23, 2001, the United States, which actively participated in the negotiations in its capacity as an observer state at the COE, signed the Convention at Budapest. I recommend that the Convention be transmitted to the Senate for its advice and consent to ratification.

Accompanying the Convention is its official Explanatory Report, which was also adopted by the COE's Committee of Ministers on November 8, 2001. The Explanatory Report, which was drafted by the Secretariat of the COE and the delegations participating in the negotiations, provides a thorough analysis of the Convention. It is customary for the COE to prepare such reports in connection with its conventions. Under established COE practice, such reports reflect the understanding of the Parties in drafting convention provisions and, as such, are accepted as fundamental bases for interpretation of COE conventions. The Explanatory Report would be provided to the Senate for its information.

The Cybercrime Convention is the first multilateral treaty to address specifically the problem of computer-related crime and electronic evidence gathering. With the growth of the Internet, attacks on computer networks have caused large economic losses and created great risks for critical infrastructure systems. Examples of such cybercrime activities include the deliberate transmission of "viruses," "denial of service" attacks, and "hacking" into government and financial institution computer systems. Criminals around the world are also using computers to commit traditional crimes, such as fraud, child pornography and copyright piracy. In addition, computer networks provide organized crime syndicates and terrorists means with which to plan, support, coordinate, and commit their criminal activities.

In response to this growing problem of computer-related crime, the COE established in 1997 the Committee of Experts on Crime in Cyber-space ("PC–CY") to undertake negotiation of the Cybercrime Convention. States participating in the work of the PC–CY included the United States, COE member states, Canada, Japan, and South Africa. Beginning in April 2000, drafts of the

Convention were made public by the COE, so that interested members of the public could review and provide comments to the PC–CY. In addition, U.S. Government officials sought to make information about the Convention available to interested members of the public. Since its adoption, 37 states have signed the Convention, including three COE member states that have also ratified it.

The Convention establishes a treaty-based framework that requires Parties to criminalize certain conduct related to computer systems and to ensure that certain investigative procedures are available to enable their domestic law enforcement authorities to investigate cybercrime offenses effectively and obtain electronic evidence (such as computer data) of crime. In a manner analogous to other law enforcement treaties to which the United States is a party, the Convention also requires Parties to provide broad international cooperation in investigating computer-related crime and obtaining electronic evidence.

By requiring Parties to establish certain substantive offenses, the Convention will help deny "safe havens" to criminals, including terrorists, who can cause damage to U.S. interests from abroad using computer systems. Similarly, by requiring Parties to have certain procedural authorities, the Convention will enhance the ability of foreign law enforcement authorities to investigate crimes effectively and expeditiously, including those committed by local criminals against U.S. individuals, institutions and interests. Since cybercrimes are often committed via transmissions routed through foreign Internet Service Providers ("ISPs") and criminals increasingly seek to hide evidence of their crimes abroad, the Convention would also provide mechanisms for U.S. law enforcement authorities to work cooperatively with their foreign counterparts to trace the source of a computer attack and to obtain electronic evidence stored outside the United States. Thus, the Convention's obligations on Parties to establish domestic law enforcement frameworks and create a regime of international cooperation would enhance the United States' ability to receive, as well as render, international cooperation in preventing, investigating and prosecuting computer-related crime.

The Convention would not require implementing legislation for the United States. As discussed below, existing U.S. federal law, coupled with six reservations and four declarations, would be adequate to satisfy the Convention's requirements for legislation. All of these reservations and declarations are envisaged by the Convention itself. Since other provisions contained in the Convention are self-executing (e.g., articles relating to extradition and mutual assistance), they would not require implementing legislation either.

The Cybercrime Convention consists of 48 articles divided among four chapters: (1) "Use of terms"; (2) "Measures to be taken at the national level"; (3) "International co-operation"; and (4) "Final provisions." A detailed, article-by-article analysis is contained in the accompanying Explanatory Report. In addition, the following is an overview of the major Convention obligations and a description of the proposed reservations, declarations, and understanding.

CHAPTER I—USE OF TERMS (ARTICLE 1)

Chapter I, Article 1, contains definitions of four key terms that are used throughout the Convention: "computer system," "computer data," "service provider," and "traffic data." "[C]omputer system" is defined to mean any device or group of inter-connected or related devices, where one or more of them performs automatic processing of data pursuant to a program. As elaborated upon in the Explanatory Report (paragraph 23), the Convention's definition of "computer system" may include input, output and storage facilities and can be either a "stand alone" system or one that is networked with similar devices. The term "service provider" includes public and private entities that provide users with the ability to communicate by means of a computer system, as well as other entities that process or store computer data for such entities or users. The definition of "computer data" encompasses data in electronic or another form suitable for processing by a computer system. As defined in Article 1, "traffic data" does not relate to the content of a communication but instead is data generated by computers in a communication chain that relates to the communication's origin, destination, route, time, date, size, duration, or type of underlying service. As such, traffic data can provide information about the source of a computer-related crime as well as other evidence of the crime. The Explanatory Report (paragraph 22) explains that it is not necessary for Parties to copy verbatim these definitions into their laws provided the concepts are covered, as they are under existing U.S. domestic law.

CHAPTER II—MEASURES TO BE TAKEN AT THE NATIONAL LEVEL (ARTICLES 2–22)

Chapter II consists of three parts, covering substantive criminal offenses that Parties are to establish; procedural mechanisms that Parties must have under their respective laws; and provisions requiring Parties to establish jurisdiction over the offences to be established. As discussed further in connection with Article 41 ("Federal clause"), a federal state may reserve the right to assume obligations under Chapter II "consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities." In explaining this provision, the Explanatory Report (paragraph 317) makes clear that the United States could therefore implement its obligations under Chapter II through its federal criminal law, which "generally regulates conduct based on its effects on interstate or foreign commerce, while matters of minimal or purely local concern are traditionally regulated by constituent States." Thus, provided it invokes the Federal clause reservation provided for in Article 41, the United States would be able to rely on its existing federal laws, which, because of the architecture of the Internet and computer networks, provide for broad coverage of the obligations contained in Chapter II. The United States would not be obligated to criminalize activity that otherwise would not merit an exercise of federal jurisdiction. Similarly, whether or not constituent State laws conform to the Convention would not be an issue since the United States, having invoked the federal clause reservation, would

not be required to implement the Convention's obligations at that level.

Substantive criminal law (Articles 2–13):

Articles 2–10 of the Convention require Parties to criminalize domestically, if they have not already done so, certain conduct that is committed through, against or related to computer systems. Included in these substantive crimes are the following offenses against the "confidentiality, integrity and availability" of computer data and systems: "Illegal access" (Article 2), "Illegal interception" (Article 3), "Data interference" (Article 4), "System interference" (Article 5), and "Misuse of devices" (Article 6). Also included are offenses involving the use of computer systems to engage in conduct that is presently criminalized outside the cyber-realm, i.e., "Computerrelated forgery" (Article 7), "Computer-related fraud" (Article 8), "Offences related to child pornography" (Article 9), and "Offences related to infringements of copyright and related rights" (Article 10).

For criminal liability to attach under the offenses to be established pursuant to Articles 2–10, the conduct in question must be committed intentionally. As the Explanatory Report (paragraph 113) notes, "wilfully" was used in lieu of "intentionally" in the context of Article 10 infringements so as to conform with Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"), which employs the term "wilful." In addition, the Report (paragraph 39) explains that determinations of what constitutes the necessary criminal intent are left to each Party's interpretation under its laws.

The obligation to establish offenses under the Convention extends only to acts committed "without right." This concept recognizes that in certain instances conduct may be legal or justified by established legal defenses, such as consent, or by other principles or interests that preclude criminal liability. Thus, as explained in the Explanatory Report (paragraph 38), the Convention does not require the criminalization of actions undertaken pursuant to lawful government authority (e.g., steps taken by a Party's government to investigate criminal offenses or to protect national security). Additional guidance regarding the contours of "without right" is provided in the Explanatory Report (e.g., paragraphs 43, 47, 48, 58, 62, 68, 76, 77, 89, 103) in the context of the various offenses to be established. Such guidance makes it clear that authorized transmissions, legitimate and common activities inherent in the design of computer networks, and legitimate and common operating or commercial practices should not be criminalized. The condition that conduct be committed "without right" is explicitly stated in all but one of the enumerated offenses. The one exception is Article 10 ("Offences related to infringement of copyright and related rights"), where it was determined that the term "infringement" already captured the concept of "without right" (Explanatory Report, paragraph 115).

The requisite elements for the various offenses are set forth in Articles 2–10. Except for Article 5 ("System interference") and Article 8 ("Computer-related fraud"), these articles also provide that a Party may require certain additional criminalization elements or

may otherwise limit application of a criminalization obligation, provided a permitted declaration or reservation is made in accordance with Articles 40 and 42. This approach seeks to promote uniform application of the Convention while recognizing that permitting Parties to maintain established concepts in their domestic law will broaden acceptance of the Convention. As discussed below, in order to implement the Convention's substantive criminal law obligations under existing federal criminal law, the United States would avail itself of declarations and reservations provided for in Articles 2, 4, 6, 7, 9, 10, and 41.

In terms of the specific offenses against the confidentiality, integrity and availability of computer data and systems, Article 2 ("Illegal access") requires a Party to criminalize unauthorized intrusions into computer systems (often referred to as "hacking," "cracking" or "computer trespass"). Such intrusions can result in damage to computer systems and data, and compromise the confidentiality of data. Under Article 2, a Party may require certain additional elements for there to be criminal liability, including that the offense must be committed with an intent to obtain computer data. In order to correspond with the requirement contained in existing U.S. computer crime law, 18 U.S.C. § 1030(a)(2) & (b), I recommend that the following declaration be included in the U.S. instrument of ratification:

> The Government of the United States of America declares, pursuant to Articles 2 and 40, that under United States law, the offense set forth in Article 2 ("Illegal access") includes an additional requirement of intent to obtain computer data.

Article 3 ("Illegal interception") seeks to protect the privacy of non-public computer data transmissions from activities such as monitoring and recording through technical means (Explanatory Report, paragraph 54).

Article 4 ("Data interference") requires a Party to criminalize "the damaging, deletion, deterioration, alteration or suppression of computer data," which the Explanatory Report (paragraphs 60 and 61) makes clear would include the inputting of malicious codes, such as viruses, that can threaten the integrity, functioning or use of computer data and programs. Under Article 4(2), a Party may reserve the right to require that such conduct result in serious harm. In order to maintain federal jurisdictional damage thresholds, e.g., 18 U.S.C. § 1030(a)(5)(B), I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 4 and 42, reserves the right to require that the conduct result in serious harm, which shall be determined in accordance with applicable United States federal law.

Article 5 ("System interference") requires a Party to criminalize acts with respect to data which seriously hinder the functioning of a computer system. Examples of such acts are provided by the Explanatory Report (paragraph 67) and include using programs to generate denial of service attacks and transmitting malicious code, such as viruses, to stop or slow the functioning of a computer system.

The offenses to be established under Articles 2–5 are frequently committed using computer programs or access tools, such as stolen

passwords or access codes. To deter their use for the purpose of committing Article 2–5 offenses, Article 6 ("Misuse of devices") requires a Party to criminalize the possession, production, sale, procurement for use, import, distribution, or making available of such items. As recognized in the Explanatory Report (paragraph 73), however, devices such as computer programs can be used for either criminal or non-criminal purposes (so-called "dual use" devices). To avoid criminalizing activities related to devices intended for legitimate purposes, the Article provides that devices must be "designed or adapted primarily for the purpose of committing" an Article 2–5 offense. Moreover, Article 6 provides that activities in relation to devices, passwords or access codes, including their production and distribution, must be done with the intent that such devices, passwords or access codes be used for the purpose of committing an Article 2–5 offense. The Article also makes clear that it "shall not be interpreted" to impose criminal liability on the authorized testing or protection of a computer system.

With respect to the possession offense, Article 6(1)(b) provides that a Party may require that a number of items be possessed before criminal liability attaches. United States law, 18 U.S.C. § 1029(a)(3), requires that a person possess fifteen or more access devices in order for there to be federal jurisdiction. I therefore recommend that the following declaration be included in the U.S. instrument of ratification:

> The Government of 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.

Article 6(3) provides that a Party may reserve the right not to apply the criminalization requirement for the misuse of items, so long as the reservation does not concern the sale, distribution or making available of passwords, access codes or similar data with the intent that they be used for committing an Article 2–5 offense. United States law does not directly criminalize the possession or distribution of data interference and system interference devices. Therefore, I recommend that the United States limit its obligations accordingly by including the following reservation in its instrument of ratification:

> The Government of the United States of America, pursuant to Articles 6 and 42, reserves the right not to apply paragraph (1)(a)(i) and (1)(b) of Article 6 ("Misuse 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").

With respect to the substantive crimes to be established which involve the use of computer systems to commit acts that would normally be considered criminal if committed outside the cyber-realm, Article 7 ("Computer-related forgery") seeks to protect the security and reliability of data by creating an offense akin to the forgery of tangible documents. The Article requires a Party to criminalize 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 of whether the data is directly readable and intelligible. It also allows a Party to require intent to defraud, or similar dishonest intent, before criminal liability attaches. In order to enable the offense to be covered under applicable U.S. fraud statutes, I recommend that the following declaration be included in the U.S. instrument of ratification:

> The Government of 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.

Article 8 ("Computer-related fraud") requires a Party to criminalize manipulations of data that are done with fraudulent intent and to procure an unlawful economic benefit. As indicated in the Explanatory Report (paragraph 86), an example of an activity that would be encompassed by the Article 8 offense is the serious problem of on-line credit card fraud.

Articles 9 and 10 deal with content-related offenses. Article 9. ("Offences related to child pornography") requires a Party to criminalize various aspects of the production, possession, procurement, and distribution of child pornography through computer systems. The Explanatory Report (paragraph 93) notes that it was believed important to include Article 9 because of the increasing use of the Internet to distribute materials created through sexual exploitation of children. In addition to covering visual depictions of an actual minor engaged in sexually explicit conduct, the Article covers images of a person appearing to be a minor engaged in such conduct as well as realistic images representing a minor engaged in such conduct (so-called "virtual" child pornography). Article 9(4), however, provides that a Party may reserve the right not to criminalize cases of a person appearing to be a minor or realistic images representing a minor engaged in such conduct. These categories were covered under U.S. law by 18 U.S.C. §2256(8)(B), (C) & (D), and to the extent that such images are obscene, certain conduct relating to such obscene images is also covered by federal obscenity law. In light of the U.S. Supreme Court's decision in *Ashcroft* v. *Free Speech Coalition*, 535 U.S. 234 (2002), ruling §2256(8)(B) & (D) unconstitutional, I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 9 and 42, 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.

Article 10 ("Offences related to infringement of copyright and related rights") is directed at infringements of intellectual property rights, i.e., copyright and related rights, by means of a computer system and on a commercial scale. Its approach differs from the other articles requiring the establishment of offenses in that it defines the offenses by reference to other international agreements, which are set forth in the Article. Specifically, a Party is required under Article 10 to establish as criminal offenses acts that are com-

mitted "wilfully, on a commercial scale and by means of a computer system" and that are defined as infringements of copyright or related rights, under its domestic law, pursuant to obligations it has undertaken in the referenced agreements. As indicated in the Explanatory Report (paragraphs 110 and 111), a Party's obligations under this Article are framed only by those agreements that have entered into force and to which it is party. Moreover, a Party's obligations under Article 10 may be limited by reservations or declarations it has made with respect to the referenced agreements. For the purpose of determining the United States' obligations under Article 10, the relevant referenced agreements are the four to which the United States is party, i.e., the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on the Trade-Related Aspects of Intellectual Property Rights, the WIPO Copyright Treaty, and the WIPO Performances and Phonograms Treaty. Of these, the latter two entered into force after the Cybercrime Convention was opened for signature.

Because, among the referenced agreements, only TRIPS requires criminal sanctions, Article 10 permits a Party to reserve the right not to impose criminal liability in limited circumstances provided other "effective remedies" are available and the reservation does not derogate from its minimum obligations under applicable international instruments, which the Explanatory Report (paragraph 116) makes clear refers to TRIPS. Because U.S. law provides for other effective remedies but not criminal liability for infringements of certain rental rights, I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 10 and 42, 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 criminalization of such infringements is not required pursuant to the obligations the United States has undertaken under the agreements referenced in paragraphs 1 and 2.

Article 11 ("Attempt and aiding or abetting") provides that aiding or abetting the commission of any of the offenses set forth in Articles 2–10 shall also be made criminal. Similarly, a Party is required to criminalize an attempt to commit certain of these offenses, to the extent specified in paragraph 2 of the Article. As with the Article 2–10 offenses, aiding or abetting or an attempt must be committed intentionally. Thus, as indicated in the Explanatory Report (paragraph 119), the fact that an ISP is a mere conduit for criminal activity, such as the transmission of child pornography or a computer virus, does not give rise to criminal liability for the ISP, because it would not share the criminal intent required for aiding and abetting liability. Further, the Explanatory Report (paragraph 119) makes clear the Parties' understanding that "there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision."

Article 12 ("Corporate liability") requires the adoption of criminal, civil or administrative measures to ensure that a corporation or similar legal person can be held liable for the offenses to be es-

tablished in accordance with the Convention, where such offenses are committed for its benefit by a natural person who has a leading position in the corporation or legal person. The Article also provides for liability where a lack of supervision or control by a leading person makes possible the commission of one of the criminal offenses for the benefit of the legal person by a natural person acting under its authority. Per the Explanatory Report (paragraph 125), a "natural person acting under its authority" is understood to be an employee or agent acting within the scope of their authority. Further, the Explanatory Report (paragraph 125) notes that a "failure to supervise should be interpreted to include the failure to take appropriate and reasonable measures to prevent employees or agents from committing criminal activities on behalf of the legal person." The Explanatory Report (paragraph 125) also makes clear, however, that such appropriate and reasonable measures "should not be interpreted as requiring a general surveillance regime over employee communications." The concepts set forth in Article 12 are already reflected in U.S. law.

Under Article 13 ("Sanctions and measures"), each Party is to ensure that Articles 2–11 offenses committed by natural persons are subject to "effective, proportionate and dissuasive sanctions, which include deprivation of liberty." As elucidated in the Explanatory Report (paragraph 130), the Article leaves open the possibility of other sanctions or measures, such as forfeiture, for these offenses. Consistent with the approach set forth in Article 12 ("Corporate liability"), sanctions to be imposed against legal persons may be criminal, civil or administrative in nature.

Procedural law (Articles 14–21):

As recognized by the Explanatory Report (paragraph 133), evidence in electronic form can be difficult to secure, as it may be flowing swiftly in the process of communication and can be quickly altered, moved or deleted. In an effort to ensure that Parties are able to investigate effectively the offenses established under the Convention and other criminal offenses committed by means of a computer system, as well as to collect evidence in electronic form of a criminal offense, the Convention requires each Party to ensure that its competent authorities have certain powers and procedures for use in specific criminal investigations or proceedings. These powers and procedures are set forth in articles on: "Expedited preservation of stored computer data" (Article 16), "Expedited preservation and partial disclosure of traffic data" (Article 17), "Production order" (Article 18), "Search and seizure of stored computer data" (Article 19), "Real-time collection of traffic data" (Article 20), and "Interception of content data" (Article 21). All of these powers and procedures are already provided for under U.S. law.

A number of important limitations on the powers and procedures to be established pursuant to Articles 16–21 are set forth throughout the procedural law articles. Under Article 14 ("Scope of procedural provisions"), for example, the powers and procedures are to be invoked to obtain or collect data in connection with "specific" criminal investigations or proceedings. Thus, as the Explanatory Report explains (paragraphs 151 and 152), the Convention does not impose a general obligation on service providers to collect and re-

tain data on a routine basis simply because such data might one day be useful to some yet-to-be determined criminal investigation or proceeding. The preservation measures apply to data already stored by means of a computer system, thus presupposing that the data already exists, has been collected and is being stored. Further, Article 15 ("Conditions and safeguards") provides that the establishment, implementation and application of the powers and procedures called for by the Convention are to be subject to conditions and safeguards provided for under a Party's domestic law, which law shall provide for the adequate protection of human rights and liberties, including rights arising in accordance with obligations a Party has undertaken under applicable human rights instruments. This Article depends on implementation through a Party's domestic law. For the United States, no implementing legislation would be required as the U.S. Constitution and U.S. law already provide for adequate conditions and safeguards.

Article 15 and its accompanying text in the Explanatory Report (paragraph 147) recognize that, depending on the power or procedure, different conditions and safeguards under domestic law may be appropriate. For example, the Explanatory Report (paragraph 215) notes that, due to its high degree of intrusiveness, interception of content data pursuant to Article 21 merits more stringent safeguards, such as judicial or other independent supervision, as well as limitations on its duration. Article 15 also requires a Party, to the extent consistent with the public interest, to consider the impact of the powers and procedures upon the rights, responsibilities and legitimate interests of third parties. In this regard, the Explanatory Report (paragraph 148) indicates that a Party should consider mitigating the impact of such powers and procedures through such steps as minimizing disruption of consumer services, protecting service providers from liability for disclosing or facilitating the disclosure of data, or protecting proprietary interests.

The preservation regime to be established pursuant to Article 16 ("Expedited preservation of stored computer data") and Article 17 ("Expedited preservation and partial disclosure of traffic data") requires a Party to enable its competent authorities to order or similarly obtain the expedited preservation of specified computer data, including traffic data, for use in a specific investigation or proceeding. This power, which already exists in U.S. law, is important to ensuring that evidence is not moved, altered or deleted while further processes for obtaining a search warrant or subpoena for its disclosure are pursued.

As indicated in the Explanatory Report (paragraph 160), preservation under Article 16 may be accomplished by different legal means, including by ordering a person, including a service provider, not to destroy or delete computer data within that person's possession or control. The person may be required to preserve that data for a period of up to 90 days to allow the competent authorities to seek its disclosure. (A Party may provide for renewal of the preservation order.) The person who is to preserve the data may also be required to keep confidential for a period of time the undertaking of the preservation. With respect to traffic data, Article 17 provides that a sufficient amount of data must be able to be disclosed expeditiously in order to enable a Party to identify other service pro-

viders and the path through which a communication was transmitted. Such expedited disclosure is intended to enable authorities to take steps to preserve additional computer data that otherwise might be lost, which can be critical to tracing a communication back to the source of a computer-related crime (Explanatory Report, paragraphs 166–168). The U.S. Government would comply with this requirement by moving expeditiously, using existing preservation and disclosure procedures provided for under U.S. law.

As stated in the Explanatory Report (paragraphs 151 and 152), the data preservation measures contained in Articles 16 and 17 are distinguishable from so-called "data retention" measures in that they "do not mandate the collection of all, or even some, data collected by a service provider or other entity in the course of its activities." Instead, as indicated above, data preservation measures apply only to data that already exists, is being stored, and is specified by competent authorities as being sought in connection with a specific criminal investigation or proceeding.

Article 18 ("Production order") and Article 19 ("Search and seizure of stored computer data") require Parties to establish additional measures by which their competent authorities can obtain stored computer data. Under Article 18, authorities must be able to order a person, including third party custodian of data, such as an ISP, to produce data, including subscriber information, that is in that person's possession or control. The Explanatory Report (paragraph 177) makes clear that such subscriber information, which includes various types of information about the use and user of a service, may be in computer data form as well as in other forms (e.g., paper records). The Article, however, does not impose an obligation on service providers to compile and maintain such subscriber information in the normal course of their business. Instead, as the Explanatory Report (paragraph 181) describes, it requires a Party to be able to order a service provider to produce subscriber information that it does in fact keep. For its part, Article 19 is intended to enable authorities themselves to search and seize a computer system, data stored in a computer system and data contained in storage mediums, such as diskettes (Explanatory Report, paragraphs 187–189).

Article 20 ("Real time collection of traffic data") and Article 21 ("Interception of content data") require Parties to establish measures to enable their competent authorities to collect data associated with specified communications in their territory at the time of the data's communication (i.e., in "real time"). "Traffic data" is defined in Article 1, while guidance in the Explanatory Report (paragraph 209) indicates that "content data" refers to "the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)." Under Article 20, a Party is required to enable its authorities to collect traffic data with respect to any offense, although under Article 14(3)(a), a Party may take a reservation limiting the types of crimes to which Article 20 must be applied. This reservation would not be needed by the United States as federal law already makes this mechanism generally available for criminal investigations and prosecutions. With regard to Article 21, the Explanatory Report (paragraphs 210 and 212) recognizes that interception of content

data is considered an intrusive measure and, therefore, that Article only requires a Party to provide for such measures in relation to a range of serious offenses to be determined by its domestic law, which is the approach taken by U.S. federal law.

Under both Articles 20 and 21, a Party is generally required to adopt measures enabling its competent authorities: (a) to collect or record data themselves through application of technical means on the territory of that Party, and (b) to compel a service provider, within its existing technical capability, either to collect or record data through the application of technical means or to cooperate and assist competent authorities in the collection or recording of such data. The Explanatory Report (paragraph 224) explains that in certain states, such as Germany, due to "established legal principles", law enforcement is not able to intercept communications directly and must rely on service providers to have the capability to collect content or traffic data in real time on its behalf. Accordingly, pursuant to Article 20(2), Parties may therefore adopt other measures to ensure the collection or recording of data, including by requiring service providers to provide technical facilities. This exception does not apply to the United States as its authorities are empowered to collect and record data directly through technical means. In states, such as the United States, in which this exception would not be invoked, the obligation on a service provider to assist law enforcement under Articles 20 and 21 is subject to "its existing technical capability." As more fully described in the Explanatory Report (paragraph 221), this means there is no obligation to impose a duty on service providers to obtain or deploy new equipment or engage in costly reconfiguration of their systems in order to assist law enforcement.

Jurisdiction (Article 22):

Article 22 requires a Party to establish jurisdiction over the offenses specified in the Convention where committed in the Party's territory, on board a ship flying its flag, on board an aircraft registered under its laws, or, in certain circumstances, by one of its nationals. Except with respect to offenses committed in its territory, Article 22(2) permits a Party to enter a reservation as to these jurisdictional bases. Because U.S. criminal law does not provide for plenary criminal jurisdiction over offenses involving its nationals and selectively provides for maritime or aircraft jurisdiction, I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 22 and 42, 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 United States

law. Accordingly, the United States shall implement paragraphs 1(b), (c) and (d) to the extent provided for under its federal law.

Under Article 22(3), a Party is also required to establish jurisdiction over the criminal offenses established in accordance with Articles 2–11 of the Convention in the event it does not extradite an alleged offender solely on the basis of nationality. As explained in the Explanatory Report (paragraph 237), establishing such jurisdiction is necessary to ensure that such a Party has the ability to undertake investigations and proceedings against the alleged offender domestically. United States law permits extradition of nationals; accordingly, this paragraph does not give rise to a need for implementing legislation.

As indicated in the Explanatory Report (paragraph 239), offenses committed through the use of the Internet may target victims in many states, giving rise to instances in which more than one Party has jurisdiction. Accordingly, Article 22(5) provides that when more than one Party claims jurisdiction over an alleged offense established in accordance with the Convention, they shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

CHAPTER III—INTERNATIONAL CO-OPERATION (ARTICLES 23–35)

Chapter III, Article 23 ("General principles relating to international co-operation") provides that Parties are to provide international cooperation to one another to the "widest extent possible" for investigations and proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. The Chapter contains extradition and mutual legal assistance provisions typical of many multilateral law enforcement conventions to which the United States is already a party, and, as such, is compatible with existing U.S. law. As provided in the Chapter and as recognized in the Explanatory Report (paragraph 244), the general approach is to supplement existing international cooperation agreements and provide a basis for such cooperation where no such framework exists.

Extradition is covered in Article 24 ("Extradition"), which provides that the offenses established in accordance with Articles 2–11 of the Convention shall be deemed to be included as extraditable offenses in extradition treaties between or among the Parties provided the offenses are subject to minimum penalties as described in the Article. The Article provides that extradition is subject to the conditions provided by the law or applicable treaties of the requested Party, including the grounds on which it may refuse extradition. Any Party that refuses an extradition request solely because the person sought is one of its nationals is obliged at the request of the requesting Party to submit the case to its competent authorities for the purpose of prosecution.

Article 24 also provides that a Party that conditions extradition on the existence of a treaty may use the Convention itself as a treaty basis, although it is not obligated to do so. For situations in which there is no separate extradition treaty in existence, Article 24(7) provides that a Party is to notify the COE of the name and address of its authority for receiving requests for extradition or

provisional arrest under the Convention. The United States would not invoke Article 24 as a separate basis for extradition, but, instead, would continue to conduct extradition pursuant to applicable bilateral treaties, supplemented where appropriate by relevant international law enforcement conventions. Thus, the principal legal effect of Article 24 for the United States would be to incorporate by reference the offenses provided for in the Convention as extraditable offenses under U.S. bilateral extradition treaties. Further, because the United States would continue to rely on bilateral extradition treaties, it would notify the COE that it is not designating an authority under Article 24(7) and that the authority responsible for making or receiving extradition requests on behalf of the United States is set forth in the applicable bilateral extradition treaties.

The provisions relating to mutual legal assistance are set forth in Articles 25–35. Article 25 sets forth "General principles relating to mutual assistance," where the duty to provide cooperation is not limited to the offenses to be established pursuant to Articles 2–11 of the Convention. As the Explanatory Report (paragraph 253) notes, the need for "streamlined mechanisms of international co-operation" extends beyond such offenses and, thus, Article 25 obliges the Parties to afford mutual assistance "to the widest extent possible for the purposes 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." Article 25 provides that in urgent circumstances a Party may make a request for assistance by expedited means of communication (e.g., fax or e-mail) and that the requested Party shall be obliged to respond to the request by expedited means of communication as well. Article 25(4) sets forth the general rule that, except as otherwise specifically provided for in Chapter III, mutual assistance shall be subject to conditions provided for by applicable mutual legal assistance treaties or by the law of the requested Party. Article 25(4) itself provides for an exception to this general rule in that it precludes a Party from denying assistance with respect to the offenses set forth in Articles 2–11 on the ground that the request concerns a fiscal (i.e., tax) offense.

Article 26 ("Spontaneous information") provides that, without receiving an assistance request, a Party may forward to another Party information it obtains in one of its own investigations where it believes such information might assist the other Party in initiating or carrying out an investigation or proceeding. Per the Explanatory Report (paragraph 260), such a provision was thought useful because some states require a positive grant of legal authority to provide such assistance, which would be satisfied by inclusion of this provision in the Convention. Before providing such information, a Party may require that it be used subject to conditions, such as that it be kept confidential.

Article 27 ("Procedures pertaining to mutual assistance requests in the absence of applicable international agreements") and Article 28 ("Confidentiality and limitations on use") provide a framework for assistance where there is no mutual legal assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting Party and the requested Party. Arti-

cle 27 provides procedures for handling assistance requests as well as grounds for refusal, which include where the request concerns a political offence or is "likely to prejudice [a requested Party's] sovereignty, security, ordre public or other essential interests." The Article also provides for the designation by each Party of a central authority or authorities, which is to be responsible for handling requests for mutual assistance. In the event of urgency, Article 27(9) allows for requests to be sent directly to judicial authorities. A Party may declare, however, that for reasons of efficiency, such requests are to be addressed to its designated central authority. In this regard, I recommend that the following declaration be included in the U.S. instrument of ratification:

> The Government of the United States of America declares, pursuant to Articles 27 and 40, that requests made to the United States of America 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.

Article 28 provides that the requested Party may condition the provision of information on confidentiality and certain use limitations. The Article only applies, however, where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force as between the requested and requesting Parties, unless the Parties concerned agree to its application in whole or in part.

Articles 29–35 contain specific provisions on mutual assistance that apply regardless of whether assistance is being requested or provided pursuant to an existing mutual legal assistance treaty or arrangement.

Article 29 ("Expedited preservation of stored computer data") and Article 30 ("Expedited disclosure of preserved traffic data") address the preservation and disclosure of data. As indicated in the Explanatory Report (paragraphs 282 and 290), these articles make available for the purposes of international cooperation the mechanisms provided for use at the domestic level in Articles 16 and 17. Under Article 29, a requesting Party may obtain advance, expedited preservation of stored data that is located in the territory of the requested Party provided it intends to submit a subsequent, formal mutual assistance request for disclosure of the data. Upon preservation, the requesting Party shall then have at least sixty days to submit its mutual assistance request. A requested Party may refuse preservation on the ground that the request concerns a political offense or that its execution would be "likely to prejudice its sovereignty, security, ordre public, or other essential interests." For the purposes of obtaining the initial preservation, Article 29 does not as a rule require dual criminality. As explained in the Explanatory Report (paragraph 285), once preserved, the data is generally not subject to disclosure to government officials until the formal mutual assistance request is executed. A determination with respect to any dual criminality requirement can be made in the context of that request. However, a requested Party that requires dual criminality as a condition under its applicable mutual legal assistance framework may enter a reservation that would enable it to refuse a preservation request if it has reason to believe that at the

time of the disclosure dual criminality would not be met. Because the United States generally seeks, as a policy matter, to minimize the application of dual criminality as a ground for refusing international mutual assistance, and, especially since preservation in and of itself does not result in disclosure of data to government officials, the United States would not exercise this reservation. Under Article 30, if the requested Party determines in executing an Article 29 request for expedited preservation concerning a specific communication that a service provider in another state was involved in that communication, then it is under an obligation to disclose to the requesting Party such traffic data as necessary to identify the foreign service provider and the communication path. As in Article 29, such disclosure may only be withheld by the requested Party on political offense grounds or on the grounds that it "is likely to prejudice its sovereignty, security, ordre public or other essential interests."

Article 31 ("Mutual assistance regarding accessing of stored computer data") is the international cooperation counterpart to Article 19 ("Search and seizure of stored computer data") in the procedural law chapter. It requires a requested Party to be able to "search or similarly access, seize or similarly secure, and disclose" stored data in response to a request for mutual assistance. Where the data is "particularly vulnerable to loss or modification," the requested Party is required to expedite its response.

Article 32 ("Trans-border access to stored computer data with consent or where publicly available") is not a mutual assistance provision per se. Rather, as discussed in the Explanatory Report (paragraphs 293 and 294), it reflects the general agreement that an accessing Party need not seek the prior authorization of another Party to access data stored in that other Party's territory where the data is publicly available or obtained through a computer system located in the accessing Party's territory with the lawful and voluntary consent of a person who has lawful authority to disclose that data through that system.

Article 33 ("Mutual assistance in the real-time collection of traffic data") and Article 34 ("Mutual assistance regarding the interception of content data") are the counterparts in the international cooperation chapter to Articles 20 and 21. Under Article 33, a Party is required to provide mutual assistance in the real-time collection of traffic data at least with respect to offences for which such real-time collection would be permitted under its domestic law. Similarly, Article 34 obligates a Party to provide mutual assistance in the interception of content data, but only to the extent permitted under its applicable treaties and domestic law.

Article 35 ("24/7 Network") requires each Party to designate a point of contact that will be available 24 hours a day, seven days a week to ensure the provision of immediate assistance for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form. This shall include an obligation to facilitate or, if permitted by its domestic law and practice, direct the carrying out of immediate assistance in the provision of technical advice, the expedited preservation of stored computer data, the expedited disclosure of preserved traffic data, the collection of evi-

dence, the provision of legal information, and the locating of suspects. As indicated in the Explanatory Report (paragraph 298), this channel draws its inspiration from a network created by the G8 countries in 1998. The 24/7 point of contact for the United States would be the same point of contact used for the G8 network: the Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section.

Chapter IV—Final provisions (Articles 36–48):

As indicated in the Explanatory Report (paragraph 303), the provisions contained in Chapter IV ("Final provisions") are generally based on standard model clauses used by the COE. Article 36 ("Signature and entry into force") provides that the Convention is open for signature by COE member states and by non-member states that have participated in its elaboration, i.e., the United States, Canada, Japan, and South Africa. Five states, including at least three COE member states, must express their consent to be bound by the Convention for it to enter into force. After entry into force, states subsequently expressing their consent to be bound shall become party to it on the first day of the month following a three month period from the date of that state's expression of consent. Article 37 ("Accession to the Convention") details a procedure for accession by other states after the Convention enters into force. Reflecting past practice in this area within the COE, accession by a state requires the unanimous consent of the Parties to the Convention. Article 38 ("Territorial application") enables states to specify the extent of their territory to which the Convention will apply.

Article 39 ("Effects of the Convention") addresses the relationship of the Cybercrime Convention to other international instruments. It makes clear that the Convention is intended to supplement applicable treaties or arrangements between the Parties in the area of international cooperation. As set forth in the Article and as explained in the Explanatory Report (paragraph 312), Parties are free to enter into new agreements with one another regarding matters dealt with in the Convention provided they do not undermine its objectives and principles. Article 39 also contains a "savings" clause to the effect that the Convention does not affect other rights and obligations that are not addressed in the Convention.

Article 40 ("Declarations"), Article 41 ("Federal clause") and Article 42 ("Reservations") permit Parties to modify or derogate from specified Convention obligations. Under Article 40, a Party may declare that it avails itself of various additional elements provided for in specified articles at the time it consents to be bound by the Convention. As set forth above, in order to meet its Convention obligations without having to seek new implementing legislation, the United States would make declarations under Articles 2, 6(1)(b), 7, and 27(9)(e).

Article 41 ("Federal clause") permits a federal state to enter a reservation allowing for minor variations in coverage of its Chapter II obligations ("Measures to be taken at the national level"). As stated in the Explanatory Report (paragraph 316), this reservation takes into account that variations in coverage may occur due to "well-established domestic law and practice" of a federal state based on the federal state's "Constitution or other fundamental

principles concerning the division of powers in criminal justice matters" between its central government and its constituent entities. The reservation was inserted to make clear that the United States could meet its Convention obligations through application of existing federal law and would not be obligated to criminalize activity that does not implicate a foreign, interstate or other federal interest meriting the exercise of federal jurisdiction. In the absence of the reservation, there would be a narrow category of conduct regulated by U.S. State, but not federal, law that the United States would be obligated to criminalize under the Convention (e.g., an attack on a stand-alone personal computer that does not take place through the Internet). Article 41 makes clear that this reservation is available only where the federal state is still able to meet its international cooperation obligations and where application of the reservation would not be so broad as to exclude entirely or substantially diminish its obligations to criminalize conduct and provide for procedural measures. Such a restriction is not an obstacle for the United States because the Convention's international cooperation provisions are implemented at the federal level and because federal substantive criminal law provides for broad overall coverage of the illegal conduct addressed by the Convention. In invoking the reservation, the U.S. Government would be obliged to bring the Convention's provisions to the attention of its constituent States and entities, with a "favourable opinion" encouraging them to take appropriate action to give effect to such provisions, even though, as a result of the reservation, there would be no obligation for them to do so. This step would be accomplished through an outreach effort on the part of the federal government. Accordingly, I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 41 and 42, reserves the right to assume obligations under Chapter II of the Convention in a manner consistent with its fundamental principles of federalism. Furthermore, in connection with this reservation, I recommend that the Senate include the following understanding in its resolution of advice and consent:

The United States understands that, in view of its reservation pursuant to Article 41, Chapter II of the Convention does not warrant the enactment of any legislative or other measures; instead, the United States will rely on existing federal law to meet its obligations under Chapter II of the Convention.

Article 42 ("Reservations") enumerates those provisions by which a Party can exclude or modify its obligations with respect to specified articles at the time it consents to be bound by the Convention. Consistent with COE treaty practice, the Article provides that no other reservations may be made. Article 43 ("Status and withdrawal of reservations") provides a mechanism for Parties to withdraw their reservations as soon as circumstances permit. As set forth above, to meet its obligations without the need for additional implementing legislation, the United States would make permitted reservations under Articles 4(2), 6(3), 9(4), 10(3), 22(2), and 41.

The procedure for amending the Convention is set forth in Article 44 ("Amendments") and provides that amendments do not come

into force until they have been accepted by all Parties to the Convention. Article 45 ("Settlement of disputes") obligates Parties to seek to settle disputes as to the interpretation or application of the Convention through peaceful means of their choosing. Resort to binding arbitration or to the International Court of Justice is possible if the Parties concerned agree. Article 46 ("Consultations of the Parties") establishes a flexible framework for Parties to consult regarding implementation of the Convention, including the effect on implementation of significant legal, policy or technological developments. As appropriate, such consultations are to be facilitated by the COE, including specifically by the European Committee on Crime Problems. The Explanatory Report (paragraph 328) encourages Parties, in the context of these consultations, to seek the views of non-governmental and private sector organizations on privacy, business and other related issues.

Article 47 ("Denunciation") sets out the procedure for a Party to denounce the Convention with three months advance notice, and Article 48 ("Notification") empowers the COE's Secretary General to act as the notifying authority in relation to the Convention.

It is my belief that the Convention would be advantageous to the United States and, subject to the reservations and declarations proposed in this Report, would be consistent with existing United States legislation. The Departments of Justice and Commerce join me in recommending that the Convention be transmitted to the Senate at an early date for its advice and consent to ratification, subject to the reservations and declarations described above.

Respectfully submitted.

COLIN L. POWELL.