Background and Process

Q: What is the Council of Europe? [Top]

A: The Council of Europe ("CoE") (website: www.coe.int) consists of 47 member States, including all of the members of the European Union. It was established in 1949 primarily as a forum to uphold and strengthen human rights, and to promote democracy and the rule of law in Europe. Over the years, the CoE has been the negotiating forum for a number of conventions on criminal matters in which the United States has participated.

Q: What is the history of the Convention on Cybercrime? [Top]

A: Since the late 1980s, the CoE has been working to address the growing international concern over the threats posed by hacking and other computer-related crimes. In 1989, it published a study and recommendations addressing the need for new substantive laws criminalizing certain conduct committed through computer networks. See Recommendation No. R. (89) 9. This was followed by a second study, published in 1995, which contained principles concerning the adequacy of criminal procedural laws in this area. See Recommendation No. R. (95) 13. (Both the 1989 and 1995 Recommendations are available at www.coe.int and www.cybercrime.gov.) Building on the principles developed in the 1989 and 1995 reports, in 1997 the CoE established a Committee of Experts on Crime in Cyberspace (PC-CY) to begin drafting a binding convention to facilitate international cooperation in the investigation and prosecution of computer crimes.

Q: What role did the United States play in drafting the Council of Europe Convention? [Top]

A: The United States was invited to participate as an "observer" in both the 1989 and 1995 Recommendations, as well as in the development of the Convention on Cybercrime. Because of the vulnerability of the United States to Cybercrime, the benefits to be gained from a well-crafted instrument focused on increasing international cooperation in this area, the U.S. desire to help shape such an important instrument, and the importance of the information technology sector, the United States accepted the CoE's invitation to participate in the Convention negotiations. Among other non-CoE States participating in the negotiations were Canada, Japan, and South Africa. By virtue of their having participated in the Convention's elaboration, the United States and other non-CoE States have the right to become Parties to the Convention, and all have in fact signed it. The United States, represented by the Departments of Justice, State and Commerce, in close consultation with other U.S. government agencies and interested private parties, actively participated in the negotiations in both the drafting and plenary sessions, working closely with both CoE and non-CoE member States. Because the provisions in the Convention were generally adopted by consensus both in the drafting and plenary groups, rather than by member State vote, the United States had a real voice in the drafting process.

Q: How open was the drafting process? [Top]

A: During the drafting and negotiation process, the United States sought comments and other input from a variety of groups representing U.S. interests. In an extensive series of meetings held primarily from 2000 through 2001, representatives of the Departments of Justice, State and

Commerce met with representatives of the U.S. technology and communications industry and a variety of public interest groups to hear comments on draft provisions and to share information on the status of the Convention. As a result of these consultations, the United States sought and obtained several important revisions to the Convention's text and Explanatory Report. In addition, the United States and other countries urged the Council of Europe to make drafts available to the public for comment. The Council of Europe made numerous successive drafts publicly available.

Q: What benefits is this Convention expected to bring for the United States? [Top]

A: The United States is heavily dependent on computers that are networked, and it offers many targets across every sector of society. Attacks on computer systems supporting the military, satellite networks, transportation and communications systems, and large utilities pose a constant threat to our critical infrastructures and hence our national security. Criminals in foreign countries also have penetrated computer systems of major U.S. financial institutions and stolen large sums. Numerous cases of credit, debit and ATM card fraud, telemarketing fraud, and copyright piracy have caused significant losses for U.S. individual and corporate victims. Finally, the Internet has greatly facilitated communications among criminal and terrorist organizations and physical-world crimes such as murder, stalking, bomb threats, extortion, and narcotics trafficking. In short, if left unchallenged, computer crime poses a serious threat to the health and safety of our citizens, and may stifle the Internet's power as a tool to communicate, engage in commerce, and expand people's educational opportunities around the globe. Thus, the United States has much to gain from a strong, well-crafted multilateral instrument that removes or minimizes the many procedural and jurisdictional obstacles that can delay or endanger international investigations and prosecutions of computer-related crimes.
The Convention breaks new ground by being the first multilateral agreement drafted specifically to address the problems posed by the international nature of computer crime. Although we believe that the obligations and powers that the Convention requires the U.S. to undertake are already provided for under United States law, the Convention makes progress in this area by (1) requiring signatory countries to establish certain substantive offenses in the area of computer crime, (2) requiring Parties to adopt domestic procedural laws to investigate computer crimes, and (3) providing a solid basis for international law enforcement cooperation in combating crime committed through computer systems.

Q: What is the current status of the Convention? [Top]

A: The working group assigned to draft the Convention concluded its activities in May, 2001. The Convention was opened for signature at a signing ceremony in Budapest, Hungary on November 23, 2001, during which 30 countries signed the Convention (including 26 member States of the Council of Europe, and the four observer States that participated in the negotiations). Since that time, additional States have signed.
Further information about the Convention, including the text of the instrument itself, the text of its lengthy Explanatory Report, and a current list of signatories and ratifying States, may be found on the Council of Europe web site:
http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185.

Q: What further conditions are necessary for the Convention to enter into force? [Top]

A: The terms of the Convention require that it will enter into force only once it has been ratified by five countries, at least three of which are member States of the Council of Europe. As of October 2003, the Convention has been ratified by three countries (Albania, Croatia, and Estonia) all of which are members of the Council of Europe.

Q: Has the United States signed the Convention? [Top]

A: Yes. The United States was one of 30 countries (including 26 member States and three other observers) that signed the Convention on November 23, 2001 in Budapest. On November 17, 2003, President Bush transmitted the Convention to the Senate with a view to receiving its advice and consent to ratification. See the President's Message to the Senate on the Council of Europe Convention on Cybercrime (November 17, 2003).

Q: Will implementing legislation be required for the U.S. to join the Convention? [Top]

A: In order for the U.S. to join the Convention, it would have to be ratified by the United States with the advice and consent of the U.S. Senate (see previous question). However, should the United States ratify the Convention, further implementing legislation would not be required for it to become a Party.
First, the U.S. delegation has worked hard to balance attentiveness to the suggestions of other countries with respect for the strengths of current U.S. law. As a result, the central provisions of the Convention are consistent with the existing framework of U.S. law and procedure. Second, the terms of the Convention do permit us some flexibility to the extent that our laws do not conform to certain provisions. This is because, in accordance with traditional CoE practice, Parties to the Convention are permitted to take reservations or enter declarations modifying their obligations on a limited number of specified articles, or parts thereof. For example, we have taken a partial reservation to the Jurisdiction article (Article 22) because the U.S. does not as a general matter assert jurisdiction over crimes committed by U.S. citizens broad.

Q: Will there be any limits on when the United States must assist another country's investigation or prosecution? [Top]

A: Yes. The Convention provides for limitations on assistance to other countries. This enables the United States to deny assistance in a variety of circumstances - for example, if it would violate our First Amendment guarantees.

Q: Will the Convention be open for participation by other non-members of the Council of Europe? [Top]

A: Once the Convention enters into force, the Committee of Ministers of the Council of Europe, with agreement from all of the Contracting States, may invite other non-member States to become Parties by accession.

Structure of the Convention [Top]

Q: Why are the crimes to be established by Parties to the Convention drafted so generally? [Top]

A: The Convention does not itself create substantive criminal law offenses or detailed legal procedures. Parties agree to ensure that their domestic laws criminalize several categories of conduct and establish the procedural tools necessary to investigate such crimes under their own national laws.
By their nature, multilateral conventions must take into account many different legal systems, and the text of such conventions is often more general than would be a domestic statute. The level of specificity in this convention is consistent with other multilateral law enforcement conventions. Under Council of Europe practice, an Explanatory Report ("ER") describing the Convention's requirements has also been prepared. This ER describes in more detail the kind of conduct to be criminalized under the Convention to ensure that Parties implement the Convention consistently.

Q: How is legitimate activity by businesses and individuals excluded from criminalization under the Convention? Is the term "without right" in Articles 2-11 intended to address this issue? [Top]

A: The crimes established in the Convention must, by their terms, be committed "without right." While ER para. 38 explains that national law will determine precisely how to exempt legitimate activity, para. 41 makes clear that offenses must be drafted with sufficient clarity and specificity to provide foreseeability as to the conduct that will be criminalized. Moreover, ER paras. 38, 46-48, 58, 62, 68-69, 77 and 89-90 specifically provide that legitimate and common operating or commercial practices should not be criminalized. For example, the Convention does not purport to exhaustively define the line between what sorts of "interception" are lawful and which are not under Article 3 ("Illegal Interception"). Therefore, nothing in this Convention would change the U.S. wiretap statute (18 U.S.C. 2511(2)(a)(I)), which specifically allows monitoring by a service provider of traffic on its own network undertaken to protect its rights and property.

Questions relating to Substantive Offense Provisions [Top]

Q: What kind of mens rea requirement is contemplated for the crimes in Articles 2-11? [Top]

A: The Parties agree to criminalize the conduct described in articles 2-11 when it has been committed "intentionally" or "wilfully." While there is no prohibition on application of other standards if required under a particular Party's legal system, nothing in the Convention encourages such an approach.

Q: Does the Convention outlaw legitimate security testing or research? [Top]

A: Nothing in the Convention suggests that States should criminalize the legitimate use of network security and diagnostic tools. On the contrary, Article 6 obligates Parties to criminalize the trafficking and possession of "hacker" tools only where such conduct is (i) intentional, (ii) "without right", and (iii) done with the intent to commit an offense of the type described in Articles 2-5 of the Convention. Because of the criminal intent element, fears that such laws

would criminalize legitimate computer security, research, or education practices are unfounded. Moreover, paragraph 2 of Article 6 makes clear that legitimate scientific research and system security practices, for example, are not criminal under the Article. ER paragraphs 47-48, 58, 62, 68 and 77 also make clear that the use of such tools for the purpose of security testing authorized by the system owner is not a crime.

Finally, in practice, the existing U.S. laws that already criminalize use of, possession of, or trafficking in "access" or "interception" tools have not led to investigations of network security personnel.

Q: Because there are no exemptions from liability for service providers, will they be subject to criminal liability for failing to monitor customer or user content, or for the criminal actions of their employees? [Top]

A: Nothing in the Convention requires service providers to monitor content to avoid liability. The provisions of the Convention governing aiding and abetting or corporate liability are based upon well established principles of criminal law.
Aiding and abetting liability under Article 11 arises if the accomplice has specific intent that the object crime be committed. ER para. 119 also provides that the aider and abettor must share the mental state required for the commission of the crime, and that a service provider is under no duty to monitor its system in order to avoid criminal liability.
In addition, Article 12, governing corporate liability, restates the traditional corporate liability principle that if a person with significant authority within a corporation intentionally undertakes or, through a lack of supervision of an agent of the corporation, makes possible the intentional undertaking of criminal activity for the corporation's benefit, the corporation may face criminal, civil or administrative liability. Liability cannot result from actions of mere users of an Internet service provider or other service under Article 12. (See also ER paragraphs 124-125). This Article is based upon similar provisions in other multilateral law enforcement treaties and does not go beyond current U.S. law governing the vicarious liability of corporations. In fact, the Convention's liability requirements would apply to a more limited group of persons than under U.S. federal law.

Questions relating to Domestic Procedure Provisions [Top]

Q: What kind of safeguards does the Convention contain to protect the rights of individuals under the Convention? [Top]

A: Article 15 requires Parties to establish conditions and safeguards to be applied to the powers established in articles 16-21. Those conditions and safeguards must adequately protect human rights and liberties, such as privacy. Article 15 lists some specific safeguards, such as requiring judicial supervision, which should be applied where appropriate in light of the power or procedure concerned. The Article also requires Parties to consider (to the extent consistent with the public interest and sound administration of justice) the impact on third parties (such as service providers) of the powers and procedures listed in the section. ER paras. 146 and 214 list further safeguards that national laws should contain.

Q: Are costs incurred by service providers in the course of providing assistance to law enforcement reimbursed? [Top]

A: Article 15, paragraph 3, provides for consideration of interests of third parties to the extent consistent with the public interest. ER para. 147 clarifies that this includes the impact of a procedure on service providers and whether means can be taken to mitigate such impact. A reimbursement obligation was inconsistent with existing legal regimes in some States participating in the negotiations, and was also viewed as unworkable for small countries. The current U.S. law and practice of providing reimbursement in many instances would not be affected.

Q: I've read news reports that state that the Council of Europe Convention will require Internet service providers to collect and retain data, adopt mandatory business practices, and build certain technical capabilities into their infrastructures. Is this accurate? [Top]

A: The Convention does not contain any mandatory retention provisions or requirements that service providers collect or maintain categories of data generally, nor does it require certain technical capabilities.
There is no data retention obligation in the Convention; there is, however, a data preservation provision. It is important to distinguish between data retention requirements, which would require providers to collect and keep all or a large portion of a provider's traffic as a routine matter, and preservation requirements, which enable law enforcement authorities, during the course of a criminal investigation, to instruct a service provider to set aside specified data that is already in the service provider's possession until law enforcement procures the proper documents to require the data's disclosure. The Convention requires preservation, not retention. Thus, service providers are obligated only to preserve (i.e., not delete or disclose) data that they are currently storing, if requested to do so by law enforcement with respect to specified data in a particular case. (See articles 14(1), 16(1), ER paras. 149-154, 157-158, 160). The ER makes clear that the Convention does not require, or even recommend, a general obligation to retain data not needed for business purposes. (See ER paras.151-152).
Preservation is not a new idea; it has been the law in the United States since April 1996. 18 U.S.C. 2703(f) requires an electronic communications service provider to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process" upon "the request of a governmental entity." This applies in practice only to reasonably small amounts of specified data identified as relevant to a particular case where the service provider already has control over that data. Similarly, as with traditional subpoena powers, issuance of an order to an individual or corporation to produce specified data during the course of an investigation carries with it an obligation not to delete or destroy information falling within the scope of that order when that information is in the person's possession or control.
Finally, the Convention does not require any particular architecture or capability; nothing in the Convention states that a service provider must be able to obtain evidence that it is not technically capable of collecting. Indeed, Articles 20 and 21 explicitly state that a service provider need only collect data "within its existing technical capability" when ordered to compel data through proper legal process. (See also ER para. 220). There is a limited exception for countries like Germany whose established systems require ISPs to have technical capability to gather such data (see articles 20(2), 21(2)).

Q: What are the trap and trace and interception provisions of the Council of Europe Cybercrime Convention? Is this an attempt by the United States to legalize or provide for an international "Carnivore"? [Top]

A: No. The Council of Europe Cybercrime Convention requires that countries have an ability to implement interception of data either with the assistance of service providers or, in circumstances where there is no service provider or where the service provider is not able to provide assistance, to be able to exercise these powers themselves. The latter power is necessary because the Convention only requires providers to provide assistance "within their technical ability." In a serious case where law enforcement has obtained an interception or trap and trace order, but a service provider lacks the technical ability to assist them, law enforcement requires the ability to effectuate the terms of the order themselves; otherwise, critical evidence may be lost.
The Department of Justice does not view the Convention as differing from or requiring change to current U.S. law, which provides for each such possibility. Most importantly, however, the Convention does not change or weaken in any way the requirements of United States law that there be judicial supervision and approval of any exercise of these powers by law enforcement. Similarly, the Convention is absolutely silent on the technical mechanism for implementing interceptions - it does not require or even suggest the use of any particular technology to intercept data. The United States intends to carry out interception and trap and trace orders by its current means of doing so, which is by working cooperatively with service providers to effectuate lawful orders with a minimum of disruption to legitimate users. The Convention would not affect or limit our ability to do this in any way.

Information on Other Issues [Top]

Protocol on the Criminalization of Act of a Racist and Xenophobic Nature Committed Through Computer Systems [Top]

An additional protocol to the Council of Europe Cybercrime Convention, addressing materials and "acts of racist or xenophobic nature committed through computer networks," was proposed by some member States. This additional protocol was the subject of negotiations in late 2001 and early 2002. Final text of this protocol was adopted by the Committee of Ministers on November 7, 2002, and is available at http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm. The protocol opened for signature in late January 2003. A current list of signatories and ratifying States is available on the Council of Europe web site at http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=189&CM=&DF=.

The protocol requires participating States to criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults, and denial of the Holocaust and other genocides.
The United States participated in the negotiations of this protocol despite its concern that the final product would not comport with the U.S. Constitution.

As with the main Convention, during the drafting and negotiation process, the United States sought comments and other input from a variety of groups representing U.S. interests. In a series

of meetings held in 2001 and 2002, representatives of the Departments of Justice, State and Commerce met with representatives of the U.S. technology and communications industry and a variety of public interest groups to hear comments on draft provisions and to share information on the status of the protocol. As with the main Convention, the Council of Europe made numerous successive drafts publicly available.

The United States does not believe that the final version of the protocol is consistent with its Constitutional guarantees. For that reason, the U.S. has informed the Council of Europe that it will not become a Party to the protocol.

It is important to note that the protocol is separate from the main Convention. That is, a country that signed and ratified the main Convention, but not the protocol, would not be bound by the terms of the protocol. Thus, its authorities would not be required to assist other countries in investigating activity prohibited by the protocol.