Prepared Statement of Mark M Richard
Counselor for Justice Affairs
U.S. Mission to the European Union

Presented at the Meeting of EU's Article 29 Working Group
Brussels, 14 April 2005

Thank you, Mr. Chairman, for the opportunity to address this Committee. It is a pleasure to be here today. My name is Mark Richard. I work for the Criminal Division of the United States Department of Justice, presently as Counselor for Justice Affairs at the U.S. Mission to the European Union. Prior to accepting my current position, I supervised for twenty years at the U.S. Justice Department all international criminal matters, including extradition and mutual legal assistance, and investigations and prosecutions of international terrorism. My statement, however, reflects the position of the United States Government and not merely that of the Department of Justice.

Today I want to speak on the important and related topics of data retention and data protection, because EU Member States and the Commission are now considering EU legislation that would mandate EU-wide data retention for communications providers, for public safety and law enforcement purposes. Terrorism and Internet-related crime are now borderless crimes in many respects. Because any agreed EU legislation in this area will impact law enforcement in the EU and the United States, I would like to present the following views on behalf of the United States Government.

At the outset, let me emphasize that the EU needs to address the consequences that broad data protection requirements have on law enforcement investigations, in order to ensure that data critical to terrorism and criminal investigations exists at the time that the data is sought by investigators. Any actions the EU takes with regard to data

protection and/or data retention should balance the needs of public safety with the needs of industry and with concerns for civil liberties.

Data availability is essential for effective terrorist and criminal investigations

With the globalization of communications networks, public safety is increasingly dependent on effective law enforcement cooperation across borders. As we saw in the 2001 attacks in the U.S. and again in Madrid in 2004, terrorists and cybercriminals acting in one country communicate with and are supported by individuals in other countries. For this reason, access to historic computer traffic data, such as connection logs, in conformity with accepted due process protections, is particularly critical for investigators to identify terrorists and criminals who commit offenses on or through the use of computer networks. Analysis of traffic data may in some cases be the only way to connect the terrorists with their co-conspirators. Additionally, without the freedom to voluntarily retain traffic data as they deem appropriate, service providers lose their ability to effectively protect their own networks from fraud, hacking, computer viruses, and other malicious activity.

We note that the recent Data Protection Directive explicitly acknowledged that Member States could derogate from the Directive for law enforcement and national security needs. However, effective law enforcement cooperation may not be possible, or at a minimum is significantly complicated, when public safety authorities are confronted with a variety of non-uniform exceptions to data protection requirements to immediately destroy communications data. In such cases, the failure of a <u>single</u> country to enact an exception to the default data destruction requirements can hamper efforts to prevent and investigate criminal or terrorist activity.

The U.S. System

Let me describe the U.S. system for preserving Internet communications data. The United States believes that investigators and prosecutors need the ability to have service providers preserve (without disclosing) for a limited period of time, data which already exists within their network architecture and which relates to a specific investigation. We have a specific law for this purpose.[1] Public safety officials therefore rely on providers to preserve specified log files, electronic mail, and other records quickly, upon notification that such information is necessary for a specific investigation, before such information is altered or deleted. The law requires preservation for 90 days and preservation is renewable for another 90 days. Later access to these historical records is obtained by court order or other statutory processes in conformity with accepted due process protections. Data preservation, however, does not require a service provider to collect data prospectively, nor does it permit the government to preserve everything in a provider's system – only what relates to a particular investigation. The Council of Europe Cybercrime Convention, which the United States strongly supports, contains a similar scheme, reflecting general agreement that, for now, this preservation regime strikes the proper balance between competing policy interests.

Under this system, U.S. law enforcement may issue preservation requests for any type of data, not merely traffic data. Data such as connection logs, subscriber information, Internet protocol addresses, and billing information may be relevant to an ongoing investigation. In addition, it may be important to preserve the content of stored

[1] This law can be found at Title 18, United States Code, Section 2703(f) and states as follows: "A provider of wire or electronic communications services or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other records in its possession pending the issuance of a court order or other process."

Internet communications – for example, the text of an e-mail message between two criminal co-conspirators.

With respect to the routine destruction of stored communications data (European-styled "data protection") or the routine retention of such data, the United States does not require either from its Internet service providers: providers are free to destroy or retain communications data they receive or generate as they each choose, based upon individual assessments of resources, architectural limitations, network security, fraud risks, and other business needs.

Data preservation could be much less effective in the European context

In EU Member States, data protection laws preclude communications providers from storing any communications traffic data that is not necessary for billing and limited other business purposes. Thus, all providers are required to delete traffic data as soon as practical after they no longer have one of these limited business purpose to keep it. This affirmative obligation to destroy traffic data may seriously undercut the effectiveness of a data preservation model because, with European data protection requirements, much less data will exist when law enforcement requests preservation of data relating to a specific investigation.

The Council of Europe's Convention on Cybercrime

For many computer crime investigations, data covered by the Commission's Data Protection Directive is often the only evidence with which to begin an investigation. While immediately erasing communications data impedes criminal investigations and diminishes public safety, such an approach also undercuts critical provisions of the Council of Europe's Cybercrime Convention. The Convention seeks to ensure a prompt

and broad exchange of information among law enforcement agencies to facilitate the investigation and prevention of criminal acts. A mandatory data destruction regime stands in tension with the Convention's provisions. Allowing service providers the ability to retain data for billing purposes does not solve the problem, because the type of data kept for such purposes is limited in scope and the amount of billing data retained continues to shrink throughout the industry in light of flat-rate pricing models and free Internet and e-mail services.

Communications providers should be free to choose longer retention periods

We would like to emphasize that the U.S. Government position on the handling of data has been and remains in opposition to mandatory data destruction requirements because of the inherent conflict between broad data destruction requirements and the needs to protect public safety and for providers to protect their networks from fraud and network abuse. We remain supportive of communications providers determining their own retention needs as appropriate to their individual business models. If a resolution is reached that includes mandatory data retention for a set period of time, we hope that the resolution will permit service providers to voluntarily choose to retain data to protect their computer networks for lengthier periods than permitted by a mandatory retention regime.

Conclusion

Because the impact of legislation in this field so clearly extends beyond the borders of any one country, the United States hopes to continue working closely with the EU on this issue so that unintended extraterritorial effects are minimized. Our goal is to ensure compatible and complementary approaches, which will advance our shared goals

of protecting the privacy of citizens, giving service providers the flexibility to protect their networks as they see fit, and ensuring that public safety officials will have access to information of critical importance to the success of terrorist and cybercrime investigations. The need to address the issue of mandatory data destruction exists in every place where there is access to the Internet or mobile communications.

The United States Government appreciates this opportunity to speak to the Committee on the issue of mandatory data retention. The United States Government remains available to meet with the Committee on these and other issues, as the need arises. Thank you for your time and your attention.