Deputy Assistant Attorney General Laura H. Parsky Remarks before the 'The Major Challenges of Intellectual Property Protection' Conference in Rome, Italy

Introduction

Thank you for inviting me to speak before you today on a topic of central importance to the United States Department of Justice. Intellectual property theft – whether counterfeit car parts or pirated software – endangers public health and safety and threatens the foundation and integrity of our economies. That is why the United States Justice Department has made the protection of intellectual property rights a law enforcement priority.

Background

Given the challenges of new technologies and the rapid growth of the problems of piracy and counterfeiting, an effective response to these problems requires specialized expertise and can no longer rely on traditional approaches to law enforcement. Federal investigative agencies, such as the Federal Bureau of Investigation, the Bureau of Immigration and Customs Enforcement, and the United States Secret Service, work hand-in-hand with state and local police in investigations of intellectual property violations. The vast majority of federal prosecutions are brought by the 94 United States Attorney's Offices that are located in each judicial district throughout the United States. Each of these offices is part of the Department of Justice and represents the front line of our national prosecutorial efforts.

In addition, since the beginning of his tenure at the Department of Justice, Attorney General John Ashcroft has supported the development of two highly specialized groups of criminal prosecutors at the Department of Justice that are devoted to the unique challenges of intellectual property enforcement. The first is the Computer Crime and Intellectual Property Section, which I supervise. This unit of the Justice Department is a highly specialized team of thirty-five lawyers who focus exclusively on computer and intellectual property crime. These prosecutors continually develop and implement the Department of Justice's overall anti-piracy strategy, assisting our front-line criminal prosecutors in the United States Attorney's Offices throughout the country in the prosecution of intellectual property crimes and reaching out to our international counterparts to ensure a more effective world-wide response to intellectual property theft. Additionally, Attorney General Ashcroft has established specialized units within each United States Attorney's Office – called "Computer Hacking and Intellectual Property" units -- which also consist of specially-trained prosecutors, at the local level, who have specific expertise in both computer crime and intellectual property offenses.

Further, as part of the Bush Administration's initiative to crack down on piracy and counterfeiting, Attorney General Ashcroft announced in March of this year the formation of the Justice Department's Intellectual Property Task Force. The Task Force, of which I am a member, consists of senior-level Department of Justice officials who have closely examined all aspects of how the Department of Justice enforces intellectual property rights and have made recommendations to the Attorney General for how we can improve and more effectively protect these precious rights. This includes criminal enforcement, as well as civil enforcement, international treaties and obligations, legislative and regulatory work, and public awareness. Just yesterday, the Attorney General released the Task Force report to the public and launched the most aggressive and comprehensive crackdown on intellectual property crime in the history of our Justice Department. I am looking forward to working closely with my colleagues at the Department of Justice in the coming months, as we implement the Task Force's recommendations and bring the force of our law enforcement powers to bear on this pernicious crime.

International Cooperation

One of the most critical elements in protecting intellectual property is international cooperation, and Italy has been one of our key partners in combating international computer and intellectual property crimes. The cooperation and responsiveness that we have received from Italian law enforcement has been exemplary, and we look forward to continuing this productive and valuable working relationship. Such relationships are critical in a world where we must confront multinational criminal organizations who seek to profit from intellectual property theft.

Our Approach

In the United States, we have targeted two areas of intellectual property enforcement in particular, which I believe will resonate with your own experiences. These areas are on-line piracy and organized crime.

ONLINE PIRACY

In the Criminal Division, we have focused our efforts on the investigation and prosecution of complex, multi-defendant, international intellectual property cases. This strategy enables us to most efficiently and effectively dismantle the most damaging criminal operations and send the strongest deterrent message to the public.

In particular, we have targeted the largest, most organized groups involved in the theft and distribution of copyrighted works over the Internet. These so-called "warez" ("wares") groups saturate the Internet with pirated digital products, creating an unauthorized supply of software, games, movies, and music, seriously damaging the economic viability of the intellectual property rights holders. These groups include highly sophisticated and technologically savvy members whose goals are to obtain the latest and most coveted products—sometimes prior to commercial release; to then remove or "crack" any security and copyright protection measures installed on these products; and then to disseminate the stolen works over the Internet to as many people as possible and as quickly as possible. The pirated works distributed by these groups quickly circulate over the Internet and are available world-wide within a matter of minutes. These warez groups are often the original source of pirated works that filter down to more pervasive distribution channels such as peer-to-peer networks.

Because the distribution mechanism for this sort of piracy – the Internet – knows no borders or geographical limitations, members of these groups are located throughout the world. As a result, reliance on the traditional single-district prosecution strategy is simply not effective. Intellectual property crime is now undeniably global in nature and so too must be our response. The digital age has brought us into a borderless world, with large criminal conspiracies consisting of people spread around the globe – many of whom have never met each other in person. Because of the dispersed nature of these criminal organizations, as recently as three or four years ago many engaged in online piracy held the common belief that they were engaging in a consequence-free endeavor, and that they were safely hidden from the reach of law enforcement, either by the technology they used to shield their illegal activity or by geographic boundaries or both.

To deal more effectively with digital piracy, we understood that we had to change this perception, and that the only way to do that was to develop and prosecute international piracy cases. The central tenet of this strategy is to build global enforcement relationships that will allow us to work with our foreign counterparts to effectively attack this global problem.

The most recent and far-reaching example of our international efforts occurred just a few months ago. On April 21st of this year, the Department of Justice led the single largest international enforcement effort ever undertaken against online piracy - Operation Fastlink. Operation Fastlink involved the simultaneous execution of search warrants in the United States and ten foreign countries. As a result of the coordination by the Department of Justice and the FBI, in one 24-hour period, over 120 searches were simultaneously executed in eleven different countries, across multiple time zones. In addition to the United States, searches were executed in Belgium, Denmark, France, Germany, Hungary, Israel, the

Netherlands, Singapore, and Sweden as well as Great Britain and Northern Ireland. A few days later, a twelfth country, Spain, moved successfully against targets located in that country as well.

Through this operation, over 100 individuals believed to be engaged in online piracy have been identified, many of them high-level members or leaders of online piracy release groups that specialize in distributing high-quality pirated movies, music, games, and software over the Internet. More than 200 computers were seized worldwide, including over 30 computer servers which function as storage and distribution hubs for many of the online piracy groups targeted by Fastlink. Singapore has already successfully prosecuted one of the individual targets of this investigation, and many more prosecutions are expected worldwide in the coming months.

Simply put, Operation Fastlink was the largest global enforcement action ever undertaken against online piracy. Efforts such as Operation Fastlink are, of course, extremely resource and time-intensive, requiring close coordination among law enforcement around the world for sustained periods of time. But such efforts pay substantial dividends by reducing access to pirated works early in the chain of distribution – at the source -- and thereby ensure the greatest protection for the reproduction and distribution of copyrighted materials by the rightful owners.

Large scale operations like Operation Fastlink, targeting online piracy, have struck at the heart of the highly-organized online piracy world. Geographic boundaries cannot be allowed to insulate pirates and counterfeiters from the reach of law enforcement. The Department of Justice's substantial and largely successful efforts have made significant inroads in the fight against global piracy. This progress must continue, and we stand ready to work with our foreign counterparts to address this serious, ever-growing problem.

ORGANIZED CRIME

In addition to online piracy, there is another significant area of international intellectual property crime that I want to mention today. That is the growing role of organized crime in piracy and counterfeiting. As I mentioned, in the past few years, the Department of Justice has increased its focus on organized criminal organizations engaged in intellectual property theft.

In the context of optical disc piracy and counterfeiting, for example, highly organized criminal groups are emerging as the principal producers, shippers, and distributors of pirated goods. Organized crime syndicates have begun to use piracy and counterfeiting as a means to diversify their illicit activities. It is not surprising that organized crime has begun to step into this arena, given the potential for large profits and the perceived low-risk of prosecution for such crimes.

The nature of piracy has undergone a dramatic transformation over the past several years. Traditionally, piracy operations were small, often run by individuals or a loose collection of people trying to make a "quick buck" in what has been largely perceived to be a "risk-free" criminal endeavor. Today, with low overhead and the possibility of substantial financial reward, piracy is big business. It has become a world-wide, multi-billion-dollar, illicit enterprise which robs legitimate industries and creators of income, while driving up costs for consumers. It is against this backdrop that criminal organizations are playing a more prominent - and dangerous - role in piracy around the globe.

Organized crime syndicates have substantial resources to devote to their illegal operations. This has allowed them to increase the scope and sophistication of their criminal activity. Further, by nature, these syndicates control international distribution channels which allow them to move massive quantities of pirated goods, along with other illegal products, throughout the world with relative ease. In fact, we have learned that organized crime syndicates, which are traditionally competitive, now partner with one another across borders to expand their operations at home. Small factories overseas are able to churn out hundreds of thousands of illicit products annually, ranging from software, to movies, to games, which find their way into the black market both overseas and in the United States.

It is a lucrative endeavor for these criminals, and, as one might expect, these groups do not hesitate to threaten or injure those who attempt to interfere with their illegal operations. We have received numerous reports from overseas that industry representatives have been threatened and attacked and their property vandalized, when their anti-piracy efforts struck too near these illegal operations. Information from overseas indicates that this problem similarly impacts foreign government officials fighting piracy. Some reports from abroad show that raids of factories (producing pirated goods) can often turn into full blown shoot-outs. These world-wide criminal syndicates are formidable foes. The very involvement of organized criminal syndicates, and their apparent willingness to resort to violent means to protect their piracy operations, underscores the critical need for tough enforcement. We are committed to working closely with our foreign counterparts to address this real and emerging threat.

Italy

In our relationship with the Italian government, we have already seen what international cooperation in organized crime cases can accomplish. The Neopolitan Camorra, a notorious organized crime syndicate which I know has been investigated here in Italy, also has a significant presence in the United States. According to law enforcement, the Camorra engage in the distribution of pirated and counterfeit goods in the New York/Newark metropolitan area, as well as Chicago, Los Angeles, and San Diego. These intellectual property crimes are committed in coordination with the Camorra clans operating in Naples. The Office of the Attorney General for Naples reports that there are more than 100 Camorra criminal syndicates active in the Naples vicinity, trafficking in drugs and committing extortion and counterfeiting. The Camorra clans have invested a considerable amount of capital in the purchase of industrial CD-R burners, enabling them to produce more than 2,000 units per day, and they have developed business relationships with Eurasian organized crime groups, permitting them to import large quantities of counterfeit optical media products from such countries as Ukraine and Bulgaria.

In July of this year, approximately 72 arrest warrants were issued in Italy for members of a Camorra ring that trafficked in tens of millions of dollars in counterfeit goods, including designer clothing, electronic camera equipment, and power tools. The ring conducted activities in many countries other than Italy, including the United States, Canada, Great Britain, Australia, Germany, Switzerland, and Spain. The arrests came after a lengthy investigation led by the Naples Prosecutor's Office and the Italian National Anti-Mafia Prosecutor's Office, working with the Italian National Police and with assistance from the Guardia di Finanza. The FBI here in Rome provided substantial assistance to the Italian investigation, coordinating with FBI offices in various parts of the United States. There were related United States investigations, which resulted in dozens of coordinated arrests in the United States at the federal and state level. At the time of the arrests, approximately 300 million Euros worth of real property, bank accounts, and businesses were seized. Two important fugitives in the Italian case were arrested in New York in September, and just a few weeks ago they agreed to waive extradition and be returned to the custody of Italian authorities. This successful crackdown on intellectual property crime demonstrates the efficacy and necessity of different nations working cooperatively to investigate and prosecute these offenses – offenses which threaten the creativity and innovation critical to our economies. The United States Department of Justice has made building cooperative relationships with our foreign law enforcement partners a key priority in our enforcement strategy, and we will continue to support our foreign colleagues as investigations continue and ultimately as successful prosecutions are undertaken. By building these types of law enforcement relationships -- case by case if necessary -- we will begin to effect real change and develop a stronger international regime for the criminal enforcement of intellectual property rights.

Conclusion

Clearly in today's world of global communication and advanced technologies, there are many challenges to effective enforcement of intellectual property rights; however, there are also many opportunities. There are opportunities to develop new tools and strategies to more effectively prevent and punish this destructive and potentially dangerous crime, and there are opportunities to enhance our global partnerships in this common endeavor. The United States Department of Justice is strongly committed to

continuing this vital effort, and we look forward to working closely with you and other law enforcement entities all over the world.

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.