# EUROPEAN INSTITUTE

## Intellectual Property Protection in the Digital Age

**November 17, 1998**

**REMARKS BY ROSLYN A. MAZER**
**SPECIAL COUNSEL FOR INTELLECTUAL PROPERTY**
**U.S. DEPARTMENT OF JUSTICE, CRIMINAL DIVISION**

---

With the approach of the year 2000, our trading partners in the World Trade Organization are shifting focus from enacting substantive intellectual property legislation to developing and implementing effective enforcement mechanisms. The U.S. and Europe, as leaders in the production of intellectual property, have a lot at stake, and must lead the world in providing technical assistance to our trading partners who lack experience and resources to combat IP crime. Developing countries have a large stake in this challenge as well, because economic deprivation and economic downturns provide a ready breeding ground for rampant piracy, discouraging the very conditions that are necessary to encourage economic growth and investment.

The European Institute's recognition of the unique challenges posed by digital piracy could not be more timely. I would like to share four key observations on this subject from our perspective at the Department of Justice.

First, piracy and counterfeiting are attractive areas for criminal organizations, given the absence of strong laws, the potential for high profits, and law enforcement's low priority in enforcing these laws. Second, piracy and counterfeiting operations are now providing organized criminal syndicates with a steady source of income, a product that can move across physical and virtual borders with relative ease, and a high-volume source of funds to support other illicit activities, including sometimes violent criminal and terrorist activities. Third, transborder activities involving computer usage are carried out with meticulous organization: the copyright and trademark industries have been seeing for some time now optical media and counterfeit computer chips being manufactured, transshipped, and imported across three or four continents. And we know that the open borders of the Newly Independent States present special challenges for Europe and the U.S. These countries are frequently manufacturing, distribution, and consumption points for IP-infringing merchandise. Fourth, until quite recently, U.S. law enforcement agencies have been organized to combat 20th century crimes. Their bureaucracies have become increasingly anachronistic and will be easily out-maneuvered, especially in the online world, whether we are talking about hacking into our critical infrastructure or in the commercial IP environment.

I want to mention some the unique challenges law enforcement faces in combating digital piracy.

- First, there are jurisdictional issues. IP pirates can have contact with your economy but have no physical presence. So how do we reach them? And what happens in the case of multiple jurisdictions where the activity is crossing borders in seconds? The communications travel through multiple countries, and information-sharing capabilities between and among those countries may be non-existent or very limited.

- It is also difficult, sometimes impossible, to quantify the losses from piracy and counterfeiting. Such estimates are necessary in order to make the appropriate applications for mutual legal assistance. We know of one web site that displayed over 100,000 downloads of copyrighted software made in a single month. The copies are made instantaneously, they are identical to the original, and there is no deterioration after multiple copying. How does law enforcement quantify these losses?

- Internet piracy requires a very low overhead; anybody can start a website and put up a bulletin board. It is sometimes difficult to detect the perpetrators because, first of all, they have no physical presence, say in a manufacturing facility or a warehouse. Once found, a web site easily is taken down and moves on. If the web site is located in another country, how do we identify the perpetrators?

- Current technology is not yet adequate to protect right holders. As soon as anti-copying and anti-circumvention devices are created, they are quickly cracked. We therefore were pleased to support provisions in the Digital Millennium Copyright Act that will deter and punish those who circumvent such protections.

Unlike the environment in the physical world of infringement, right owners in the digital world for the most part do not have the expertise or the legal authority to conduct online investigations. Law enforcement must be the primary line of defense. It is therefore vital that we foster more significant public and private sector partnerships and find new venues to meet the challenge.

I would like to tell you what the Department of Justice is doing to meet these challenges. In 1996, the Department established the Computer Crime & Intellectual Property Section of the Criminal Division. Its mission is to enforce criminal copyright and trademark statutes and other offenses accomplished over computer terminals, including crimes affecting critical infrastructures. In January, 1998, the Criminal Division established the position of Special Counsel for Intellectual Property whose mission is fourfold: to assist in the development of inter-agency strategic plan for domestic and international enforcement of laws protecting intellectual property, including mobilization of investigative and prosecutorial resources; strengthening of our relationships with our trading partners; fostering closer alliances with the copyright and trademark industries; and assisting our trading partners in enforcing the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement through better training and international cooperation.

The Department of Justice also has designated in every U.S. Attorney's Office around the country an Assistant U.S. Attorney, who serves as the District's Computer and Telecommunications Coordinator, or "CTC." These coordinators are trained to deal with

computer crime and online investigations. Through this network, we are able to build expertise, and have a point-of-contact 24 hours per day, 7 days per week, whether it is needed in the area of critical infrastructure protection of other computer crime areas. This cadre of attorneys will build the type of esprit de corps that will raise consciousness about computer-assisted crime. Coincidentally, this week, CTCs are meeting for a four-day seminar on the latest trends and investigative techniques, as well as legislative changes affecting investigation and prosecution of computer-related and intellectual property crimes.

The Department strongly supported passage of the No Electronic Theft ("NET") Act in December 1997. This legislation amended the Copyright Laws to provide for criminal liability in the case of online/electronic infringements, regardless of whether the infringer acted for financial gain. This legislation was enacted to close a loophole in the criminal Copyright Law that allowed persons who illegally offered copyrighted materials over the Internet for free to escape prosecution. The NET Act also contained a directive from Congress to our Sentencing Commission (the Congressionally-nominated, Presidentially-approved Commission that issues Guidelines for standardizing sentencing in federal criminal cases). The Commission is currently in a state of some disarray, and has thus far failed to act in dealing with one of the most serious challenges in bringing sentencing into the real world of online digital piracy. The current guidelines calculation is based on number of infringing copies multiplied by the price of the infringing copy. We believe this formula under-represents the harm to right owners and society in most cases. We are working very hard with the Commission staff to remedy this flaw in IP sentencing architecture and, more generally, to provide for increased penalties in IP crimes.

Another area where the Department of Justice is engaged is the international arena. Most recently, the President's International Crime Control Strategy has spawned a number of working groups and interagency activities which I think present great potential for greater collaboration in the IP area. I am also very hopeful that there will be an opportunity within the G8 to promote an IP enforcement agenda, though I regret to say that some members of the G8 are not as enthusiastic as the U.S. There is a subgroup within the G8, known as the Lyon Group, for short, which is focusing on international organized crime. Under the auspices of the Lyon Group, the U.S. distributed an Intellectual Property Enforcement Survey to all members of The Eight, responses to which will be very helpful in assessing the potential for joint cooperation within The Eight.

On a bilateral basis, there also have been some fairly dramatic changes, and we hope that we will begin to see results. We think it is fair to say that the alliance between the USTR and the Department of Justice in the area of IP enforcement is closer than ever, and the Attorney General has used the occasion of bilateral meetings with heads of state, ministers of justice, interior, and other foreign visitors, to put IP on the agenda. We work very closely with Joe Papovich of USTR, so that the Justice Department can take advantage of such opportunities to reinforce USTR's important agenda.

As you may know, the Department is also a key player in the training of prosecutors and investigators and judges who may need specialized IP training. We are now trying to make less random the U.S. Government's response to requests for training, and to be more pro-active in identifying target countries and law enforcement agencies that need specialized assistance.

There are legislative changes that are needed to assist in the investigative process. I will just mention one of them today. We are proposing an amendment to the Trap and Trace Pen Register Legislation that would provide for foreign court orders demanding subscriber and communications routing information from the Internet and other communication service providers operating in the U.S. This is motivated by the following typical scenario: a group of citizens in country X are engaged in committing IP crime on the Internet. All of the members of this group were citizens of country X, the activity physically occurred in country X, but the service provider stored all of the relevant e-mail in Virginia. What happens when a court in country X files a request for mutual legal assistance? This is the new environment we are in, and we are going to be seeing it again and again. Trying to harmonize mutual legal assistance treaties to deal with online piracy is a very special challenge. If treaties have been negotiated within the last 15-20 years, they usually have dual criminality provisions so that mutual legal assistance will be provided if the requesting country also criminalizes the activity. But increasingly we are seeing foreign courts resisting using the general basket of crimes -- for example, fraud crimes -- as a predicate for providing mutual legal assistance.

The other area that I also am encouraged about is the opportunity to multiply our international training efforts. Congress has appropriated funds for the establishment of international law enforcement academies ("ILEAs"). The first one was created in Budapest several years ago, and another academy was established in Bangkok. The principal mission of the ILEAs is to strengthen international cooperation against crime by buttressing rule of law programs and improving legislative and law enforcement efforts. One of the modalities that ILEAs are to utilize is to foster cooperation among foreign police authorities, including those who are engaged in organized crime investigations. This week, another coincidence, there is a Key Leaders meeting in ILEA-Bangkok. The Department of Justice and FBI will be addressing intellectual property issues, and IP has been added to the standard curriculum. We believe the ILEAs can be a real force multiplier and can augment the FBI's legal attaches, the customs attaches, and the others who are on the ground in many countries around the world.

So I will conclude by saying that the proliferation of IP crime in the digital environment, and generally, presents a host of legal, public policy, and technical challenges. It is therefore ever more vital for our government to join forces with our counterparts in other governments, and with our corporate citizens, to protect and promote the vitality of our IP industries, and the prosperity and prestige they justifiably should earn. To do this, the architecture of 21st century law enforcement needs to adjust, and I thank the European Institute for its leadership and vision in hosting this continuing dialogue.