U.S. Department of Justice
Office of the Attorney General

REPORT OF THE DEPARTMENT OF JUSTICE'S TASK FORCE ON INTELLECTUAL PROPERTY

October 2004

United States Department of Justice

REPORT OF THE DEPARTMENT OF JUSTICE'S TASK FORCE ON INTELLECTUAL PROPERTY

October 2004

TASK FORCE MEMBERS

David M. Israelite, Chair
Deputy Chief of Staff and Counselor
Office of the Attorney General

Daniel J. Bryant, Vice Chair
Assistant Attorney General
Office of Legal Policy

Brian D. Boyle
Principal Deputy Associate Attorney General
Office of the Associate Attorney General

Valerie Caproni
General Counsel
Federal Bureau of Investigation

Paul D. Clement
Acting Solicitor General
Office of the Solicitor General

Peter D. Keisler
Assistant Attorney General
Civil Division

William E. Moschella
Assistant Attorney General
Office of Legislative Affairs

Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division

R. Hewitt Pate
Assistant Attorney General
Antitrust Division

Kevin V. Ryan
United States Attorney
Northern District of California

Christopher A. Wray
Assistant Attorney General
Criminal Division

Debra Wong Yang
United States Attorney
Central District of California

TASK FORCE STAFF

Arif Alikhan
Executive Director and Chief Counsel

Trent William Luckinbill
Associate Counsel

Sujean Song Lee
Special Assistant

Edward S. McFadden
Publication Editor

Contributors

Carl Alexandre
Ryan W. Bounds
Rachel L. Brand
P. Kevin Carwile
Steven Chabinsky
Stuart M. Chemtob
Matthew B. Devlin
Uttam Dhillon
Jennifer M. Dixton
Kenneth L. Doroshow
Elena J. Duarte
Berkley M. Etheridge
Andrew C. Finch
Scott L. Garland
Jason Gull
Paul W. Hahn
Brian M. Hoffstadt
Patrick Kelley
Eric Klumb
Marie-Flore Kouame
Richard P. Larm
Frances Marshall
Christopher S. Merriam
Thos. Gregory Motta
Ross W. Nadel
John A. Nowacki
Michael P. O'Leary
Matthew Parrella
Robert A. Potter
Jay V. Prabhu
Anne Purcell-White
Crystal Roberts
Andrea Sharrin
Thomas G. Snow
Luke A. Sobota
Christopher P. Sonderby
Martha Stansell-Gamm
Beth L. Truebell
Jeffrey A. Wadwsorth
Roger G. Weiner
Corbin A. Weiss
Hill B. Wellford

TABLE OF CONTENTS

I. PREFACE

In response to the growing threat of intellectual property crime, on March 31, 2004, the Attorney General of the United States announced the creation of the Department of Justice's Task Force on Intellectual Property.

The Task Force was entrusted with a timely and important mission: to examine all of the Department of Justice's intellectual property enforcement efforts and to explore methods for the Justice Department to strengthen its protection of the nation's valuable intellectual resources. A team of legal experts, with a diverse range of expertise and experience, was assembled to tackle this undertaking.

The Task Force formed five working groups, or subcommittees, to explore important areas of intellectual property. These working groups, each comprised of relevant Task Force members and expert staff, were designed to ensure that the results would be thorough, comprehensive, and accurate. The working groups analyzed existing resources and proposed meaningful improvements in the following areas: (1) Criminal Enforcement, (2) International Cooperation, (3) Civil and Antitrust Enforcement, (4) Legislation, and (5) Prevention.

The Task Force also consulted other government agencies and gathered information from multiple sources outside the government, including victims of intellectual property theft, creators of intellectual property, community groups, and academia.

After six months of work, the Task Force submits this final report of recommendations to the Attorney General. These recommendations outline both substantive and tangible methods for the Department of Justice to expand and enhance its efforts in protecting the nation's creative and intellectual resources.

* * * * *

A Message from the Chair

There are many people who deserve the credit for this report.

I thank the President and the Attorney General for their leadership in recognizing the importance of intellectual property and their vision for investing the resources necessary to fight the threat posed by the theft of intellectual property.

This report reflects the hard work and insight of a truly remarkable team. I thank my fellow task force members for their significant contributions and wise counsel. Each member contributed considerable time and effort to this project. And I extend my sincere appreciation to the Task Force Staff. Their Herculean effort and tireless commitment made this report possible.

Finally, I thank the career men and women of the Department of Justice whose job it is everyday to protect the institutions that make America strong and prosperous.

David M. Israelite
Chair

II. INTRODUCTION

A teenage boy living in New York underwent a lifesaving liver transplant in March 2002. He and his family were elated with the success of the procedure, and he diligently followed the medical team's instructions to make a strong recovery. The doctors had prescribed a number of medications including a weekly injection to treat the boy's anemia, a blood condition that occurs when the number of red blood cells falls below normal. The body gets less oxygen, putting excessive pressure on a person's heart. Untreated anemia is life-threatening, so for weeks following the transplant, the 16-year-old regularly received his anemia treatment.

The World Health Organization estimates counterfeit drugs account for eight to ten percent of all pharmaceuticals worldwide.

While the boy's transplant appeared to be successful, his anemia was not getting any better; in fact, complications were developing. Soon after receiving his weekly shot of medicine, the teenager began feeling excruciatingly painful spasms in his leg and the pain often lasted into the following day. The cause of the spasms, however, was a mystery and bewildered the boy's doctor. Muscles spasms were not a known side-effect of the medicine the boy was receiving. Eight weeks into the anemia treatment – in early May 2002 – the boy and his family learned what had caused the mysterious, painful episodes: the medicine injected into the boy's body was counterfeit and did not contain the necessary dosage to treat his condition.

In September 2004, a Connecticut teenager placed his cell phone in its desk cradle to charge overnight while he slept. In the early morning hours, the boy awoke when an explosion ripped through his room. Through the smoke, he could see that his carpet, desk, and computer monitor were in flames. After he safely escaped the fire in his bedroom, investigators began assessing the damage and the cause of the fire. Initially, the cause of the explosion and ensuing fire was a mystery, but after further investigation, the fire department determined the culprit: the cell phone's battery was counterfeit and had exploded while it was charging on the boy's desk.

The Consumer Product Safety Commission reports counterfeit cell phone batteries caused fires and injuries across the United States, and that more than 50,000 batteries were recalled.

A well-known Nashville-based songwriter wrote a track on Jessica Simpson's best-selling album, "Sweet Kisses." By the time Simpson's album was released in 1999, this songwriter had used his talent and hard work to build a major song-writing firm in Nashville that employed eight additional songwriters and an office assistant. As with many song-writing businesses in New York or Los Angeles, the Nashville firm depended on royalties to pay salaries and cover expenses. "Sweet Kisses" was a commercial success for them and sold more than three million copies. But during a three-week period after its release, the album was illegally downloaded more than 1.2 million times, according to a Nashville-based firm that tracked the online theft of the album. As more and more of the firm's songs were illegally downloaded, the firm saw less and less income from royalties. The Nashville songwriter was forced to downsize, ultimately laying off all nine of his employees. Today, he is a one-man song-writing operation.

Counterfeit products and the theft of intellectual property have real-world consequences. Not only are they threats to the nation's economy, but certain types of intellectual property crimes also endanger our citizens. To understand why intellectual property is such a critical component to the lives and industries of America, it is important to understand what intellectual property is, why intellectual property protection is important, and how the United States Department of Justice can further address the global threat of intellectual property crime through criminal prosecutions, international cooperation, civil enforcement, antitrust enforcement, legislative action, and prevention programs.

III. WHAT IS INTELLECTUAL PROPERTY?

America builds upon human innovation and creativity. People, inspired by new ideas or artistic visions, create books for us to read, music for us to listen to, and products that improve our lives. Whether they produce movies, design fashion, or develop chemical compounds, these individuals all contribute the creations of their intellect for the nation's benefit.

Just as the law grants ownership rights over material possessions, such as a home or a bicycle, it similarly grants individuals legal rights over intangible property, such as an idea or an invention. When a person creates something that is novel and unique, the law recognizes its value and grants the creator the respect and integrity of ownership for this intellectual property.

Intellectual property permeates everything we do, and its diversity is reflected in the four distinct areas of law that protect it: copyrights, trademarks, trade secrets, and patents.

Copyrights

Written works form the first broad category of protected intellectual property. Books, music, movies, artwork, and plays, for example, are all protected by copyrights, which ensure that the creator of the work can claim authorship and financially benefit from his or her work (for a limited term, usually until 70 years after the author's death). Copyright protection ensures that no one else can claim credit for the work, and the creator is therefore granted the exclusive rights to his or her creation.

Copyrights protect works of creative expression that are (1) original and (2) tangibly expressed. In other words, while the physical expression of an idea is protected, the actual idea is not. For example, facts presented in a work are freely available, as long as the exact manner of expression is not copied. This allows society to benefit from the accessibility of ideas themselves while still protecting the original creative work. Copyright law applies to literary, musical, and dramatic works; motion pictures and sound recordings; and pictorial, graphic, sculptural, and architectural works.

Copyright protection applies as soon as the work is expressed in a concrete form, without any need for the creator to apply for a copyright. This prevents the scenario in which an artist devotes time and energy to creating a new work, only to have it copied by others without any compensation or acknowledgment. Copyright therefore encourages artists to continue creating, and allows society to continue to benefit from their works.

Copyright law also grants the creator exclusive rights to reproduce, distribute, display, perform, rent, record, translate, or adapt the work. For example, except in certain defined situations – such as teaching, research, or scholarship – the law generally prohibits copying a copyrighted document without the author's permission.

Since Congress enacted the first criminal law protecting intellectual property in 1909, federal law enforcement's role has evolved to reflect the changing technologies and media of expression and distribution. The Internet has greatly revolutionized the ability to share information, but at the same time it offers copyright offenders a vast resource for illegally copying and distributing creative works to which they have no rights. In addition, intellectual property enforcement has become a global problem reaching countries all over the world. Consequently, several international agreements exist to coordinate copyright and other intellectual property protections.

Trademarks

In addition to protecting creative works, intellectual property law also protects trademarks. A trademark is any trait used to identify and distinguish products, services, or their producers. McDonald's golden arches and the Nike "swoosh," for example, are commonly recognized trademarks that immediately identify the companies they represent. Trademarks protect the integrity and uniqueness of a product by allowing a consumer to distinguish one product from another. The trademark may be part of the item or its packaging, and may include a distinctive symbol, word, name, sign, shape, or color; even sounds and smells may be part of a trademark. Generic terms, like "soap," however, do not qualify as trademarks.

Manufacturers who have developed a good brand image and a reputation of high quality can rely on their trademark to prevent others from capitalizing on their successes, and to ensure that customers can continue to purchase those same manufacturers' products. Trademarks therefore contribute to fair competition in the marketplace. Consumers, on the other hand, rely on trademarks to differentiate between products, and to select those whose reputations they most trust. Trademark protection is therefore the most widely applied intellectual property system both by small businesses and in developing economies.

Registering a trademark with the United States Patent and Trademark Office confers important advantages to the trademark owner. For example, the owner is granted the exclusive right to use the mark in the United States, and can exclude others from using the trademark, or a comparable mark, in a way that would cause confusion in the marketplace. Trademarks are also protected by anti-dilution laws, which ensure that a trademark's distinctiveness cannot be blurred or tarnished through identical or nearly identical marks. Federal trademark registration is necessary for federal criminal prosecutions, particularly in prosecutions for trafficking in counterfeit goods.

In order to register a trademark, the applicant must demonstrate that (1) the mark is distinctive and (2) the mark will be used, or is intended for use, in interstate or foreign commerce. A trademark never expires.

Trade Secrets

A trade secret is any information used by a business that has some independent economic value which motivates those who possess the information to keep it secret. The recipes for Coca-Cola and Pepsi, for example, are trade secrets that are protected. Trade secrets are far broader in scope than patents, and include scientific or technological information, business information, such as marketing strategies, and even information on "what-not-to-do," such as failed or defective inventions. When the information is obtained through legitimate means, however, it can be freely used. For example, a scientist who reverse-engineers a product and discovers how it is assembled can legally use that information to re-create the product. Furthermore, trade secret protection applies only while secrecy is maintained. Once the secret is publicly disclosed, it loses its legal protection.

Patents

The final major category of intellectual property protection is the patent. From the composition of a new drug to the latest time-saving gadget, patents protect the world of inventions. Laws of nature and natural phenomena, such as gravity and acceleration, however, are not eligible for patent protection, as they are not human creations.

While there are no federal criminal laws that protect patents, there are federal civil laws that protect against patent infringement, and the United States government has numerous international agreements with foreign countries to protect patents.

Misuse of Intellectual Property

Misusing copyrighted material, stealing trade secrets, or counterfeiting trademarked products is a crime. Just as intellectual property has become more and more important for the economy and security of the United States, misuse of intellectual property has become easier and easier, and the consequences are devastating: people are deceived, property is stolen, and businesses are harmed. Consequently, federal laws that criminalize violations of intellectual property rights are fundamentally consistent with other criminal laws, which aim to protect property, deter fraud, and encourage market stability.

IV. WHAT LAWS PROTECT INTELLECTUAL PROPERTY?

The laws of the United States protect the four major categories of intellectual property through (1) protection of copyrighted works, (2) protection of trademarks, (3) protection of trade secrets, and (4) protection of patents.[1] The following is a summary of how existing federal laws protect these intellectual property resources.

Protection of Copyrighted Works

The federal criminal copyright laws prohibit the unauthorized reproduction, distribution, or performance of a copyrighted work, such as a book, motion picture, audio recording, or software program. Once an author creates the work, others generally may not copy and distribute the work without the author's permission. For example, a business that does not pay for software but instead downloads from an Internet software site copyrighted software without authorization in most situations is committing a federal crime.

According to federal law, it is also illegal to design or traffic in technology which is intended to bypass technological measures that copyright owners use to protect their works. Many copyrighted works are encrypted with standard technological or programming protections that limit the ability of others to replicate the copyrighted works easily. Federal law makes it illegal to design and distribute a code that would circumvent this defense. Providing free access to subscription digital cable television programming, for example, is a criminal offense.

Federal law provides additional protection for copyrighted works that fall outside of criminal copyright law. Specifically, trafficking (trade or sale) in counterfeit labels that are attached to copyrighted works is not permitted. This law prevents a situation in which someone creates a counterfeit computer label to attach to a computer disk with the intent to sell the computer disk as if it were an authentic brand.

Protection of Trademarks

Federal law protects trademarks by prohibiting the trafficking of goods or services that bear a counterfeit trademark that has been registered by its rightful owner. This law safeguards consumers, who rely on a trademark to identify products they trust and prefer, from being deceived by a fake label. Furthermore, in certain cases consumers can avoid exposure to serious public health and safety dangers. For example, the manufacture and sale of counterfeit automotive parts marked with a counterfeit manufacturer's label is illegal.

Protection of Trade Secrets

Federal laws that protect trade secrets criminalize the unauthorized disclosure of information that has an independent economic value and that the owner has taken reasonable measures to keep secret. The law categorizes two types of disclosures: those that are intended to benefit a foreign government and those that are motivated by economic gain. For example,

[1] The protection of patents is exclusively addressed by the civil laws of the United States. Consequently, the enforcement of patents was not an area examined by the Task Force.

federal law prohibits an employee from providing the secret ingredient of an employer's famous fried chicken recipe to a competitor. Likewise, a scientist may be committing a crime if he or she provides a company's confidential research results to a foreign government.

Other Laws

Finally, many additional laws provide further intellectual property protection in specific areas of technological innovation. To protect performers who entertain audiences in a live setting, federal laws prohibit recording live performances and then financially benefitting from subsequent copying and distribution of the recording. Federal law also prohibits the manufacture and distribution of devices designed to intercept cable or satellite television signals, and devices used to de-scramble satellite television signals, which would enable viewers to receive programming without authorization.

Federal Criminal Laws Protecting Intellectual Property

Copyright

17 U.S.C. § 506 & 18 U.S.C. § 2319
Criminal Infringement of a Copyright. Statutory maximum penalty of 5 years in prison and a $250,000 fine for a first-time offender and 10 years in prison for a repeat offender.

18 U.S.C. § 2318
Trafficking in Counterfeit Labels for Phonograph Records, Copies of Computer Programs, and Similar Materials. Maximum penalty of 5 years in prison and a $250,000 fine.

18 U.S.C. § 2319A
Unauthorized Fixation of and Trafficking in Sound Recordings and Music Videos of Live Musical Performances. Maximum penalty of 5 years in prison and a $250,000 fine for a first-time offender and 10 years in prison for a repeat offender.

17 U.S.C. § 1201-1205
Circumvention of Copyright Protection Systems. Maximum penalty of 5 years in prison and a $500,000 fine for a first-time offender and 10 years in prison and a $1 million fine for a repeat offender.

47 U.S.C. § 553
Unauthorized Reception of Cable Services. Maximum penalty of 6 months in prison and $1,000 fine for individual use and 2 years in prison and $50,000 fine for commercial/financial gain for a first-time offender; 5 years in prison and a $100,000 fine for a repeat offender.

47 U.S.C. § 605
Unauthorized Publication or Use of Communications. Maximum penalty of 6 months in prison and a $2,000 fine for individual use and 2 years in prison and $50,000 fine for commercial/financial gain for a first-time offender; 5 years in prison and a $100,000 fine for a repeat offender.

Trademark

18 U.S.C. § 2320
Trafficking in Counterfeit Goods of Services. Maximum penalty of 10 years in prison and $2,000,000 fine for a first-time offender, and 20 years in prison and a $5 million fine for a repeat offender. A corporate offender is subject to a maximum fine of $15 million.

Trade Secrets

18 U.S.C. § 1831
Economic Espionage. Maximum penalty of 15 years in prison and a $500,000 fine for an individual and a $10 million fine for a corporate offender.

18 U.S.C. § 1832
Theft of Trade Secrets. Maximum penalty of 10 years in prison and a $250,000 fine. A corporate offender is subject to a maximum fine of $5 million.

V. WHY IS INTELLECTUAL PROPERTY PROTECTION IMPORTANT?

Ideas and the people who generate them serve as critical resources both in our daily lives and in the stability and growth of America's economy. The creation of intellectual property – from designs for new products to artistic creations – unleashes our nation's potential, brings ideas from concept to commerce, and drives future economic and productivity gains. In the increasingly knowledge-driven, information-age economy, intellectual property is the new coin of the realm, and a key consideration in day-to-day business decisions.

The Economic Impact of the Copyright Industry

The International Intellectual Property Alliance - an association of 1,300 United States companies that produce and distribute books, newspapers, periodicals, motion pictures, music, television shows, and computer software - commissioned a recently-released study by economist Stephen E. Siwek on the value of copyright industries in the nation's economy. The value of all intellectual property in the American economy is actually much higher because the Siwek study did not include industries that produce trademarked goods or generate revenue from valuable trade secrets. The study, which used data published by the United States government and the methodologies of the World Intellectual Property Organization, found that:

- In 2002, American copyright industries accounted for an estimated 6% of the nation's Gross Domestic Product ("GDP"). Their $626.6 billion contribution to the United States economy exceeded the total GDP of such countries as Australia, Argentina, The Netherlands, and Taiwan.
- Copyright industries employed 5.48 million workers, or 4% of America's work force.
- Between 1997 and 2002, copyright industries added workers at an annual rate of 1.33%, exceeding that of the national economy as a whole (1.05%) by 27%.
- Copyright industries in the United States sold and exported an estimated $89.26 billion in 2002 to foreign nations. Copyright industries exceeded other major industries including the chemical, food and live animal, motor vehicle, and aircraft sectors.

When intellectual property is misappropriated, the consequences are far more devastating than one might imagine. First, intellectual property theft threatens the very foundation of a dynamic, competitive and stable economy. Second, intellectual property theft can physically endanger our health and safety. As the examples that open this report illustrate, illegal products are often destructive products. Finally, those who benefit most from intellectual property theft are criminals, and alarmingly, criminal organizations with possible ties to terrorism. This is why an effective legal system that defines and protects intellectual property in all its diversity is essential. Intellectual property theft is dangerous and harmful, and we must protect ourselves from the criminals of the new millennium who steal the ideas and hard work of others.

Intellectual property thieves profit – not at the expense of a narrow segment of our society – but at the expense of a wide spectrum of artists, manufacturers, distributors, retailers, company employees, and consumers, as well as the government. The statistics are staggering. According to the Office of the United States Trade Representative, intellectual property theft worldwide costs American companies $250 billion a year. Moreover, as a direct result of counterfeit products and Internet theft of intellectual property, the American economy is losing hundreds of millions of dollars in tax revenues, wages, investment dollars, as well as hundreds of thousands of jobs.

Unfortunately, the harmful consequences of these crimes become even more tangible when we examine cases of counterfeit merchandise. Many people assume that the world of counterfeit and stolen intellectual property is limited to fake "designer" purses, bootleg DVDs for sale on a street corner, or music available for download on the Internet. In reality, counterfeit luxury goods and entertainment products are only a small part of the problem. Intellectual property thieves target highly identifiable, commonly used, and respected trademarked items, such as prescription drugs, automobile and airplane parts, batteries, insecticides, and food products. Criminals falsely duplicate these everyday objects, often substituting cheap filler for a product's real ingredients, to mislead the public into using potentially harmful items. As a result, counterfeiting has jeopardized the lives and health of Americans in cases such as these:

- In the past few years, counterfeit versions of prescription drugs that claim to treat infection, HIV-AIDS, heart disease, and Parkinson's disease have been released to the American public. One pharmaceutical company discovered a counterfeit version of its pills that was made with a combination of floor wax and yellow lead-based paint normally used to mark roads.

- Counterfeit automotive parts, such as headlights, brake pads, fan belts, and car batteries, have been discovered in American retail stores, and were pulled from the shelves. In one Asian country, counterfeit brake pads made of compressed sawdust resulted in the death of seven children.

- Hundreds of thousands of counterfeit batteries bearing a trusted brand name were discovered by law enforcement agents. The batteries were intended for sale in bargain or "dollar" stores, which would eventually land them in everyday products like children's toys or CD players. It was quickly determined, however, that the batteries contained unsafe levels of mercury and were so poorly manufactured that exposure to sunlight could cause the batteries to explode. In fact, the batteries posed such a serious threat that federal authorities needed several months to destroy them safely.

- Hundreds of doctors and medical students have allegedly taken advantage of stolen medical textbooks and information posted by an online medical user group. Some of the most critical data, however, is listed incorrectly, including a prescription drug dosage table that in several cases indicates dosage amounts that could be fatal if prescribed.

Finally, while the harmful consequences of intellectual property theft may seem frightening, it is also disturbing to learn who is benefitting from many of these crimes. The anonymity allowed by the Internet, the use of technology which enables flawless and rapid counterfeiting, and the immense profit margins available are just some of the reasons why intellectual property crime is a lucrative venture for many different types of criminals. Intellectual property theft has been linked to organized crime and, potentially, may fund terrorist organizations attracted by the profitability of these offenses.

The Department of Justice is dedicated to protecting the American people. Because intellectual property theft is a clear danger not only to the nation's national economic security but the health and safety of the public, the Justice Department remains strongly committed to the enforcement of intellectual property rights, safeguarding the public, and punishing those who violate the law.

VI. WHAT PRINCIPLES SHOULD APPLY TO INTELLECTUAL PROPERTY ENFORCEMENT?

The Department of Justice has developed a comprehensive, multi-dimensional strategy against intellectual property crime. This strategy addresses the many different yet essential aspects of intellectual property enforcement: criminal enforcement, international cooperation, civil and antitrust enforcement, and prevention. While the perspective and focus of each of these areas differs, they are nonetheless all united by underlying values that form the foundation of the Justice Department's intellectual property efforts. The Task Force has identified these key principles that drive and shape the Department of Justice's intellectual property enforcement efforts, and which provide a basis for recommending further actions. These principles are set forth below:

- **The laws protecting intellectual property rights must be enforced.**
  The nation's economic security depends on the protection of valuable intellectual resources. The Department of Justice has a responsibility to enforce the criminal laws of the nation that are designed to protect its economic security and the creativity and innovation of entrepreneurs.

- **The federal government and intellectual property owners have a collective responsibility to take action against violations of federal intellectual property laws.**
  The federal government has the primary responsibility for prosecuting violations of federal criminal laws involving intellectual property. Likewise, the owners of intellectual property have the primary responsibility of protecting their creative works, trademarks, and business secrets, and pursuing civil enforcement actions.

- **The Department of Justice should take a leading role in the prosecution of the most serious violations of the laws protecting copyrights, trademarks, and trade secrets.**
  The Department of Justice has historically placed – and should continue to place – the highest priority on the prosecution of intellectual property crimes that are complex and large in scale, and threaten our economic national security or involve a threat to the public health and welfare. The Department of Justice should continue to focus on these areas and enforce federal intellectual property laws as vigorously as resources will allow.

- **The federal government should punish those who misuse innovative technologies rather than innovation itself.**
  The Department of Justice should enforce federal intellectual property laws in a manner that respects the rights of consumers, technological innovators, and content providers.

- **Intellectual property enforcement must include the coordinated and cooperative efforts of foreign governments.**
  Violations of intellectual property laws are increasingly global in scope and involve

offenders in foreign nations. Enforcement measures must therefore confront and deter foreign as well as domestic criminal enterprises. This requires the informal assistance of foreign governments and their law enforcement agencies, active enforcement of their own intellectual property laws, and formal international cooperation through treaties and international agreements.

VII. HOW HAS THE DEPARTMENT OF JUSTICE ATTACKED THE GLOBAL THREAT OF INTELLECTUAL PROPERTY CRIME?

In recent years, the Justice Department has made the enforcement of intellectual property laws a high priority, and in turn has developed a team of specially-trained prosecutors who focus specifically on intellectual property crimes.

The Department of Justice's intellectual property enforcement team includes prosecutors in the Criminal Division's Computer Crime and Intellectual Property Section ("CCIPS"). Based in Washington, D.C., this team of specialists serves as a coordinating hub for national and international efforts against intellectual property theft.

Additionally, to combat the widespread nature of intellectual property crime, the Justice Department has assigned specialized prosecutors, called "Computer and Telecommunications Coordinators" ("CTCs"), to all 94 United States Attorney's Offices located in geographic subdivisions throughout the nation. These front-line federal prosecutors are directly responsible for handling intellectual property prosecutions in the field.

Finally, the Justice Department has concentrated additional intellectual property theft prosecutors in regions of the country where intellectual property enforcement is especially critical. In these cities, specialized "Computer Hacking and Intellectual Property" ("CHIP") Units have been created to concentrate the number of prosecutors to reflect the intellectual property theft problem in the region.

Computer Crime and Intellectual Property Section ("CCIPS")

With the support of Congress, the Computer Crime and Intellectual Property Section has grown from 22 attorneys to more than 35 attorneys over the past two years. Created in 1991, CCIPS attorneys prosecute intellectual property cases and provide guidance and training to prosecutors in the field. CCIPS also advises Congress on the development and drafting of intellectual property legislation and provides other policy guidance. Finally, CCIPS prosecutors develop relationships with international law enforcement agencies and foreign prosecutors to strengthen the global response to intellectual property theft.

Computer and Telecommunications Coordinators ("CTCs")

A national network of high-tech federal prosecutors, designated "Computer and Telecommunications Coordinators," exists in all 94 United States Attorney's Offices. These federal prosecutors are responsible for prosecuting computer crime and intellectual property cases, training agents and prosecutors, and promoting public awareness programs in their geographic region. Today, there are about 190 CTCs in the field, as many offices have two or more prosecutors dedicated to intellectual property prosecutions. Each prosecutor receives specialized training at an annual conference, and many attend additional seminars at the Department of Justice's National Advocacy Center in Columbia, South Carolina.

Computer Hacking and Intellectual Property Units ("CHIP Units")

Because certain areas of the country have high concentrations of computer crime and intellectual property cases, the Justice Department created "Computer Hacking and Intellectual Property" ("CHIP") Units in those regions. The first of these was launched in February 2000 in the United States Attorney's Office in San Jose, California, which is responsible for handling cases in the high-tech region of Silicon Valley. In July 2001, the Attorney General expanded the program by creating 12 new CHIP Units in Los Angeles; San Diego; Atlanta; Boston; New York (Brooklyn and Manhattan); Dallas; Seattle; Alexandria, Virginia; Miami; Chicago; and Kansas City, Missouri. In addition to prosecuting computer crime and intellectual property cases, the CHIP teams work closely with local intellectual property industries to prevent computer crime and intellectual property offenses, and also train federal, state, and local prosecutors and investigators. There are currently 60 prosecutors assigned to 13 existing CHIP Units. In total, the Department of Justice has dedicated more than 250 federal prosecutors around the country to prosecute computer crime and intellectual property theft.

Investigative Resources

Successful criminal prosecutions require reliable investigative resources. Within the Department of Justice, Special Agents of the Federal Bureau of Investigation ("FBI") serve as the primary, and largest, group of investigators working with federal prosecutors. To address the increasing importance of computer crime and intellectual property, in June 2002 the FBI created a new Cyber Division and Intellectual Property Rights Unit that specifically investigates intellectual property theft and fraud. In addition, trained teams of computer forensic experts analyze digital evidence in FBI computer labs and field offices throughout the country. The FBI also has an extensive network of international partnerships with foreign countries and assigns special agents as legal attachés in United States embassies throughout the world.

The Department of Justice also works closely with numerous local and state police officers and other federal law enforcement agencies, including the United States Secret Service, the Bureau of Immigration and Customs Enforcement, and the United States Postal Inspection Service.

The Secret Service seeks to protect America's financial and telecommunications infrastructure, which is increasingly exploited by intellectual property criminals. The Secret Service's Criminal Investigative Division has an Electronic Crimes Section that supports 13 Electronic Crimes Task Forces in select cities where local, state, and federal law enforcement officers investigate numerous types of high-tech crimes.

The Bureau of Immigration and Customs Enforcement is an investigative arm of the Department of Homeland Security, and assists federal prosecutors with the seizure of counterfeit goods at the nation's borders and ports-of-entry.

Finally, as the primary law enforcement arm of the United States Postal Service, the Postal Inspection Service performs postal investigative and security functions, which become especially important in the investigation of trafficking in counterfeit goods.

Intellectual Property Prosecutions

Working together, the specially-trained federal prosecutors of the Department of Justice and the dedicated agents of federal, state, and local law enforcement agencies have formed a formidable team against intellectual property criminals. Over the past several years, the Department of Justice and its law enforcement partners have prosecuted numerous intellectual property thieves and dismantled criminal networks that presented a serious threat to the nation's economic security and the personal well-being of Americans. Some of these cases include the following:

- **Counterfeit Baby Formula:** In August 2002, a California man was sentenced to over three years in prison for selling thousands of cases of counterfeit infant formula to wholesale grocers.

- **Counterfeit Pharmaceuticals:** In January 2004, two California men were prosecuted for manufacturing 700,000 fake Viagra tablets valued at $5.6 million, and for attempting to sell the fake drugs in the United States. One defendant has pleaded guilty and is awaiting sentencing, while the other defendant is awaiting trial for his alleged role in the scheme.

- **Counterfeit Pesticides:** In January 2004, an Alabama man was sentenced to over three years in prison and ordered to pay $45,000 in restitution for selling mislabeled and adulterated pesticides to city governments and private businesses, which used the pesticides to try to control mosquitos harboring the deadly West Nile virus in a number of southern and mid-western states.

- **Counterfeit Designer Clothing:** In 2003, a South Carolina man was sentenced to seven years in prison and ordered to pay $3.5 million in restitution for selling fake Nike shoes and Tommy Hilfiger apparel.

- **Counterfeit Software:** In December 2003, a Virginia man was sentenced to over five years in prison and ordered to pay $1.7 million in restitution for distributing more than $7 million in counterfeit software over the Internet. In a separate prosecution in April 2004, a Ukranian man was charged with illegally distributing millions of dollars of unauthorized copies of software from Microsoft, Adobe, Autodesk, Borland, and Macromedia. The government of Thailand recently extradited the defendant to the United States to face criminal charges.

- **Bootleg Recordings:** In July 2004, a Pittsburgh man was sentenced to over a year in prison and fined $120,000 for illegally copying and selling 11,000 video and audio recordings of live musical acts by such artists as KISS, Aerosmith, Bob Dylan, and Bruce Springsteen.

- **Counterfeit DVDs:** In April 2004, an Illinois man pleaded guilty and faces up to three years in prison for reproducing and distributing more than 200 movie videos sent to Academy Award voters for screening, including "Master and Commander: The Far Side of the World" and "House of Sand and Fog."

- **Illegal Movie Distribution:** In June 2003, a New York man was sentenced to six months of home confinement, fined $2,000, and ordered to pay $5,000 in restitution for illegally distributing a copy of the motion picture, "The Hulk" on the Internet prior to its theatrical release.

- **Stolen Satellite Signals:** From 2003 to 2004, more than 20 computer hackers and hardware distributors were convicted of distributing hardware and software designed to steal copyrighted satellite programming.

- **Theft of Trade Secrets:** In December 2002, two California men were indicted for stealing valuable integrated circuit designs from a company in the United States and attempting to deliver the secrets to the Chinese government.

In addition to these cases, the Department of Justice has also successfully dismantled criminal networks that span the nation and the globe. A few of these efforts include:

- **Operation Buccaneer:** In December 2001, law enforcement authorities executed 70 searches in the United States and foreign countries including Australia, Finland, Sweden, Norway, and the United Kingdom against members of online organizations known as "warez" groups. This operation has resulted in 36 convictions worldwide for illegally distributing thousands of movies, musical recordings, and software programs on the Internet. Ten members of the group received prison sentences ranging from three to four years.

- **Operation FastLink:** In April 2004, more than 200 computers were seized in 11 countries from members of Internet groups that specialize in illegally distributing high-quality movies, music, games, and software over the Internet.

- **Operation Digital Marauder:** In September 2004, over $56 million in counterfeit Microsoft software was seized, and 11 people in California, Texas, and Washington were charged with manufacturing counterfeit software and counterfeit packaging.

- **Operation Digital Gridlock:** In August 2004, more than 40 terabytes of illegally distributed copyrighted materials, the equivalent of 60,000 movies or 10.5 million songs, were seized from computers located in Texas, New York, and Wisconsin in the first federal law enforcement action against a "peer-to-peer" network.

As shown in these cases, the Department of Justice has adopted an aggressive approach to combating intellectual property crime. With the help of other federal agencies and law enforcement officers worldwide, the Justice Department's network of highly-trained prosecutors strikes at intellectual property crimes with coordinated force. While the Department of Justice has prosecuted several important cases, the Task Force recognizes that the Justice Department can adopt concrete strategies to reinforce and improve upon these successes.

VIII. WHAT CAN THE DEPARTMENT OF JUSTICE DO TO EXPAND THE FIGHT AGAINST INTELLECTUAL PROPERTY CRIME?

A. CRIMINAL ENFORCEMENT RECOMMENDATIONS

The United States Department of Justice makes enforcement of the criminal intellectual property laws a high priority. The Justice Department prosecutes criminal cases involving the theft of copyrighted works, trademark counterfeiting, and theft of trade secrets. Many divisions and offices of the Justice Department participate in the enforcement of intellectual property laws, including federal prosecutors located throughout the nation. These prosecutors work closely with local, state, and federal law enforcement agents to identify criminals and prosecute them in accordance with the law.

While the Department of Justice has successfully prosecuted numerous intellectual property cases over the past several years, the Task Force believes additional success is possible. Accordingly, the Task Force recommends that the Department of Justice adopt the following recommendations to further expand and strengthen the fight against intellectual property crime:

(1) **Create five additional CHIP Units in regions of the country where intellectual property producers significantly contribute to the national economy. These areas are (1) the District of Columbia; (2) Sacramento, California; (3) Pittsburgh, Pennsylvania; (4) Nashville, Tennessee; and (5) Orlando, Florida;**

(2) **Reinforce and expand existing CHIP Units located in key regions where intellectual property offenses have increased, and where the CHIP Units have effectively developed programs to prosecute CHIP-related cases, coordinate law enforcement activity, and promote public awareness programs;**

(3) **Designate CHIP Coordinators in every federal prosecutor's office and make the coordinators responsible for intellectual property enforcement in that region;**

(4) **Examine the need to increase resources for the Computer Crime and Intellectual Property Section of the Criminal Division in Washington, D.C., to address additional intellectual property concerns;**

(5) **Recommend that the FBI increase the number of Special Agents assigned to intellectual property investigations, as the Justice Department itself increases the number of prosecutors assigned to intellectual property enforcement concerns;**

(6) **Recommend that the FBI increase the number of personnel assigned to search for digital evidence in intellectual property cases;**

(7) **Dismantle and prosecute more nationwide and international criminal organizations that commit intellectual property crimes;**

(8) **Enhance programs to train prosecutors and law enforcement agents investigating intellectual property offenses;**

(9) **Prosecute aggressively intellectual property offenses that endanger the public's health or safety;**

(10) **Emphasize the importance of charging intellectual property offenses in every type of investigation where such charges are applicable, including organized crime, fraud, and illegal international smuggling;**

(11) **Enhance its program of educating and encouraging victims of intellectual property offenses and industry representatives to cooperate in criminal investigations. Recommended enhancements include:**

- (A) **Encouraging victims to report intellectual property crime to law enforcement agencies;**
- (B) **Distributing the new "Department of Justice Guide to Reporting Intellectual Property Crime" to victims and industry representatives regarding federal intellectual property offenses; and**
- (C) **Hosting a conference with victims and industry representatives to educate participants on how they can assist in law enforcement investigations; and**

(12) **Issue internal guidance to federal prosecutors regarding how victims can assist prosecutors in intellectual property cases.**

Detailed background information and explanations for each of these important recommendations are set forth below.

CRIMINAL ENFORCEMENT RECOMMENDATION #1

Expand the CHIP Program by Adding Five New Units

RECOMMENDATION: ***The Department of Justice should create five additional CHIP Units in regions of the country where intellectual property producers significantly contribute to the national economy. These areas are (1) the District of Columbia; (2) Sacramento, California; (3) Pittsburgh, Pennsylvania; (4) Nashville, Tennessee; and (5) Orlando, Florida.***

BACKGROUND: In July 2001, the Attorney General created the Computer Hacking and Intellectual Property ("CHIP") Program based on the success of the model CHIP Unit existing in the United States Attorney's Office in San Jose, California. The CHIP Program requires prosecutors to focus on copyright and trademark violations, theft of trade secrets, computer intrusions, theft of computer and high-tech components, and Internet fraud. In addition, CHIP Unit prosecutors are expected to develop public awareness programs and provide training to other prosecutors and law enforcement agencies regarding high-tech issues.

The Attorney General expanded the CHIP Program by creating 10 additional units in strategic regions of the country where, similar to San Jose, California, intellectual property offenses and computer crime were most prevalent. Using funds provided by Congress for the 2001 fiscal year, the Justice Department added 28 positions for prosecutors and assigned them to 10 offices to create new CHIP Units. In addition to the new positions, each office assigned existing prosecutors to the CHIP Unit. In total, the 10 CHIP Units created in 2001 consisted of 48 CHIP Unit positions for prosecutors. In 2002, the Attorney General expanded the program once more and created CHIP Units in Chicago, Miami, and Kansas City, Missouri. As a result, the CHIP Program currently consists of Units in 13 offices with approximately 60 prosecutors dedicated to computer crime and intellectual property enforcement.

EXPLANATION: The Task Force has found that the CHIP program has been very successful in increasing the effectiveness of the Justice Department's intellectual property enforcement efforts. During the 2003 fiscal year, the first full year after all 13 of the CHIP Units became operational, the offices with CHIP Units filed charges against 46% more defendants than they had averaged in the four fiscal years prior to the formation of the units.

This increase in intellectual property prosecutions in districts with CHIP Units can be linked to several factors. First, many districts have large populations and strong business sectors that are frequently victimized by intellectual property crime. In addition, the creation of a specialized unit in the area visibly conveys the Department of Justice's commitment to prosecuting intellectual property crime. As a result, more victims have reported intellectual property crimes and cooperated with law enforcement authorities. Moreover, CHIP Units have developed local policies, guidelines, and strategies to address specific intellectual property crime issues in their regions. Consequently, the strategically tailored and focused approach to a particular region in areas with CHIP Units is more likely to result in a higher number of enforcement actions.

The Department of Justice should expand the CHIP Program by adding units in areas of the country where intellectual property resources significantly contribute to the national economy. These areas should have intellectual property concerns that can be addressed with intellectual property enforcement efforts, such as a large population of potential victims and a history of intellectual property offenses in the area. Accordingly, the Task Force recommends the creation of new units in the following five areas: (1) the District of Columbia, home to numerous sensitive government computer systems that contain the nation's intellectual property; (2) Sacramento, California (population 6.8 million), which has significant high-tech sectors; (3) Pittsburgh, Pennsylvania (population almost 4 million), which also has significant high-tech sectors; (4) Nashville, Tennessee, home to one of the largest recording industries in the world, including the country music industry; and (5) Orlando, Florida (population 8.9 million), an expanding region with a history of intellectual property prosecutions.

Each of these areas has business sectors that generate significant intellectual property resources and are often victimized by intellectual property crime. The creation of CHIP

Units in these areas should significantly increase the Justice Department's intellectual property efforts.

CRIMINAL ENFORCEMENT RECOMMENDATION #2

Reinforce and Expand CHIP Units in Key Regions

RECOMMENDATION: ***The Department of Justice should reinforce and expand existing CHIP Units located in key regions where intellectual property offenses have increased, and where the CHIP Units have effectively developed programs to prosecute CHIP-related cases, coordinate law enforcement activity, and promote public awareness programs.***

BACKGROUND: Two regions of the country have had particularly significant intellectual property problems. The Central District of California, consisting of the Los Angeles metropolitan area, is the largest district in the United States and has a population of approximately 18 million. The district includes the largest sea port in the world, is home to the entertainment industry, and includes numerous high-tech businesses and universities. The existing CHIP Unit in Los Angeles has prosecuted 10% of all intellectual property cases in the United States from 1998 through 2003 and 24% of the cases prosecuted by the 13 offices with CHIP Units during the same period.

The Northern District of California, which contains San Jose and San Francisco, ranks second in the number of intellectual property cases prosecuted in the country. The district has approximately 7.5 million people and includes numerous high-tech companies that produce a large amount of intellectual property resources. The existing CHIP unit has also handled several important theft of trade secret cases and recently achieved the unprecedented extradition of a defendant in an international software theft case.

Both the San Jose and Los Angeles regions have a large economic base and numerous actual and potential victims of intellectual property theft. Both offices have extensive public awareness programs, and the economies of both districts are highly dependent on the protection and enforcement of intellectual property rights. Accordingly, the Department of Justice should expand and reinforce the CHIP Units in these two districts with new prosecutors who can respond to the significant intellectual property enforcement needs in these regions.

CRIMINAL ENFORCEMENT RECOMMENDATION #3

Designate CHIP Coordinators in Every Federal Prosecutor's Office in the Nation

RECOMMENDATION: ***The Department of Justice should designate CHIP Coordinators in every federal prosecutor's office and make the coordinators responsible for intellectual property enforcement in that region.***

BACKGROUND: In 1995, the Department of Justice created the Computer and Telecommunications Coordinator ("CTC") Program, which designated at least one federal prosecutor to prosecute cyber crime and intellectual property theft within each district. In addition, CTCs were made responsible for providing technical advice to fellow prosecutors, assisting other CTCs in multi-district investigations, and coordinating public awareness efforts.

CTCs receive special training and participate in an annual CTC conference. During the CTC conference, participants receive training in both computer and intellectual property-related areas and meet with other CTCs to coordinate investigations and exchange ideas. When the Attorney General created the CHIP Units, those 13 offices replaced the CTC positions with CHIP prosecutors. The remaining United States Attorney's Offices without CHIP Units continued to designate prosecutors as CTCs.

EXPLANATION: The re-designation from CTC to CHIP Coordinator will align all 94 U.S. Attorney's Offices with the Attorney General's CHIP program announced in 2001, and the enforcement mission of the Computer Crime and Intellectual Property Section in Washington, D.C. The addition of "Intellectual Property" in the title will further clarify the coordinator's responsibility to prosecute intellectual property offenses and coordinate public awareness and training efforts within the district. A CHIP Coordinator in every office will also provide a designated contact for law enforcement agents and victims of intellectual property crime. Consequently, the Department of Justice should be able to increase intellectual property prosecutions and effectively coordinate enforcement efforts.

CRIMINAL ENFORCEMENT RECOMMENDATION #4

Examine the Need to Increase CCIPS Resources

RECOMMENDATION: ***The Department of Justice should examine the need to increase resources for the Computer Crime and Intellectual Property Section of the Criminal Division in Washington, D.C., to address additional intellectual property enforcement concerns.***

BACKGROUND: The past three years have seen a marked evolution in the development of the Criminal Division's intellectual property rights enforcement efforts. Specifically, the Computer Crime and Intellectual Property Section ("CCIPS") has made the development, investigation, and prosecution of large-scale, multi-national intellectual property cases a singular priority. As a result, CCIPS has pursued several significant intellectual property law enforcement actions. In addition, CCIPS has developed comprehensive programs and policies to address important aspects of intellectual property enforcement, including domestic and international issues, and provided advice to lawmakers.

EXPLANATION: Currently there are 12 prosecutors in CCIPS dedicated to the enforcement of intellectual property rights. Particularly in light of the increasing necessity to focus the Justice Department's efforts on large-scale, multi-national, and multi-district

prosecutions, such as Operations Buccaneer and Fastlink, it is critical to ensure that CCIPS has sufficient resources to prosecute, coordinate, and otherwise provide assistance and expertise to high-priority intellectual property cases. In addition, because of the Department of Justice's increased efforts to enhance international cooperation, additional resources are particularly necessary. Accordingly, the Justice Department should examine the need for additional prosecutors for CCIPS.

CRIMINAL ENFORCEMENT RECOMMENDATION #5

Increase the Number of FBI Agents Assigned to Intellectual Property Investigations

RECOMMENDATION: ***The Department of Justice should recommend that the FBI increase the number of Special Agents assigned to intellectual property investigations, as the Justice Department itself increases the number of prosecutors assigned to intellectual property enforcement.***

BACKGROUND: The Task Force has recommended that the Department of Justice expand the number of CHIP Units and prosecutors who handle intellectual property prosecutions. Additional prosecutions, however, are dependent upon the number of investigative agents assigned to respond to intellectual property crimes.

The FBI has proven its tremendous investigative and technical capabilities in numerous, complex intellectual property cases prosecuted by the Department of Justice, including multi-district investigations and sophisticated enforcement actions. In addition, FBI agents are on the front line of criminal investigations, and they are typically the first responders when trade secret thefts or other intellectual property crimes are reported.

EXPLANATION: The FBI should continue to develop intellectual property cases and increase the number of agents who are dedicated to intellectual property investigations. As the volume of intellectual property crime continues to expand, both the number of prosecutors and the number of investigators must increase. In addition, the FBI should align its investigative resources in the regions where the Justice Department has assigned additional prosecutors to fight intellectual property crime.

CRIMINAL ENFORCEMENT RECOMMENDATION #6

Increase FBI Personnel Assigned to Search for Digital Evidence

RECOMMENDATION: ***The Department of Justice should recommend that the FBI increase the number of personnel assigned to search for digital evidence in intellectual property cases.***

BACKGROUND: Because digital evidence is often the cornerstone of a successful intellectual property prosecution, the government's ability to locate and interpret this

evidence is critical. Information found on computers and other digital devices, such as cell phones and personal digital assistants, can often lead to important evidence in an intellectual property case. For example, organized online groups, known as "warez" groups, distribute stolen software, movies, and other copyrighted works using sophisticated computer networks that contain large storage devices. A timely computer forensic examination is often necessary to identify the offenders, analyze the stolen materials, and determine whether additional evidence is needed before criminal charges can be filed.

EXPLANATION: In response to the evolving technological sophistication of intellectual property theft, the FBI should increase its forensic capabilities to maintain its advantage over high-tech intellectual property criminals, who are increasingly using complex computer systems and massive data storage devices. Consequently, digital evidence examination is becoming especially important in the investigative phase of intellectual property cases and the FBI should increase the number of trained personnel capable of addressing this important issue.

CRIMINAL ENFORCEMENT RECOMMENDATION #7

Target Large, Complex Criminal Organizations That Commit Intellectual Property Crimes

RECOMMENDATION: ***The Department of Justice should dismantle and prosecute more nationwide and international criminal organizations that commit intellectual property crimes.***

BACKGROUND: The Department of Justice divides the United States into geographic districts where federal prosecutors are assigned to prosecute crimes within that particular district. Intellectual property theft, however, is a crime that is not limited by the borders of a district, state, or nation. Intellectual property is routinely stolen from the United States, sent overseas, manufactured in clandestine factories, and shipped around the world. Internet-related intellectual property theft is even more global because intellectual property thieves can use computer networks to steal, store, and distribute stolen software, motion pictures, music, and other copyrighted material. In addition, the Internet and computer technologies have enabled intellectual property thieves to communicate instantly over thousands of miles through e-mail, chat rooms, instant messaging, and a variety of other methods.

The Task Force recognizes that the Department of Justice has been responsive to the threat of intellectual property. For example, as one part of this important effort, the Department of Justice has developed complex, multi-district, and international enforcement efforts designed to attack this problem. Several of these enforcement efforts have included numerous arrests, searches, and seizures of evidence within a short time period. These coordinated efforts send a strong signal that sophisticated, multiple-defendant criminal organizations are not immune from prosecution. Coordinated operations, such as Operations Buccaneer, Fastlink, Digital Gridlock, and Digital Marauder, involved charges against

numerous defendants and required execution of simultaneous searches in dozens of foreign countries. Each of these challenging operations required coordination with several offices within the Department of Justice, law enforcement agencies, and international governments, and in effect, served as a visible deterrent against intellectual property crimes.

EXPLANATION: The Department of Justice should increase the number of complex, multi-district intellectual property enforcement actions to target sophisticated intellectual property thieves and organizations. Because global enforcement is the key to global deterrence, the Department of Justice should continue to work with foreign nations to build on the success of operations involving simultaneous arrests and searches and make them an integral part of future coordinated efforts. These types of challenging, yet important, initiatives should serve as a model for future law enforcement efforts to attack intellectual property crime.

CRIMINAL ENFORCEMENT RECOMMENDATION #8

Enhance Training Programs for Prosecutors and Law Enforcement Agents

RECOMMENDATION: ***The Department of Justice should enhance programs to train prosecutors and law enforcement agents investigating intellectual property offenses.***

BACKGROUND: The nature of intellectual property crime is constantly changing. Counterfeiters quickly change their methods to conceal their illicit activity. Copyright infringers rapidly adapt to security measures placed on music, DVDs, or software that are intended to deter illegal copying. Criminal networks swiftly modify communication techniques, distribution channels, and other methods of advancing their criminal activity.

Law enforcement must constantly adapt to these changing criminal methods. To address this concern, the Department of Justice conducts training on a wide variety of legal and technical intellectual property issues. For example, each year the Justice Department sponsors a conference for all prosecutors involved in intellectual property and computer crime enforcement. During this conference, prosecutors from across the country learn about changes in the law and exchange ideas about enforcement efforts. In addition, the Department of Justice sponsors a course at its National Advocacy Center in Columbia, South Carolina, to educate prosecutors and emphasize that intellectual property enforcement is a federal priority.

Department of Justice prosecutors also provide intellectual property training for local, state, and federal law enforcement agents. This training involves presentations on intellectual property law, investigative approaches, and the changing methods of intellectual property criminals. The FBI also sponsors an annual course at its training academy in Quantico, Virginia, for special agents assigned to investigate intellectual property offenses.

EXPLANATION: Because training and preparation are keys to an effective and swift enforcement plan, the Department of Justice should enhance training opportunities and programs for prosecutors and investigators assigned to intellectual property enforcement. With rapidly changing technology and criminal methods, it is essential that the Justice Department constantly review its training courses, and offer additional training courses to advance the government's ongoing emphasis on intellectual property enforcement.

CRIMINAL ENFORCEMENT RECOMMENDATION #9

Prosecute Intellectual Property Offenses That Endanger the Public's Health or Safety

RECOMMENDATION: ***The Department of Justice should prosecute aggressively intellectual property offenses that endanger the public's health or safety.***

BACKGROUND: It is clear that intellectual property crime can pose a serious health and safety risk to the public, from batteries with dangerously high levels of mercury that can find their way into children's toys, to fake medicines and pesticides that can harm unsuspecting consumers. Accordingly, the criminals who counterfeit these items and place the public at risk must be prosecuted aggressively and to the fullest extent of the law. Federal laws have been enacted to give prosecutors necessary legal tools to hold criminals accountable for such conduct. As the sheer volume of fake goods that are harmful to public health and safety continues to rise, it is important to dedicate the level of resources necessary to deter the intellectual property criminals threatening our public health and safety.

EXPLANATION: The Department of Justice should, through a formalized memorandum to prosecutors throughout the country, emphasize the urgency of aggressively prosecuting intellectual property offenses that endanger the health and safety of the public. The Justice Department should continue to commit itself to ensuring the public good, as well as reinforcing consumer confidence in the products that positively affect the welfare of the country. In addition, the Department of Justice should continue to work closely with federal and local agencies, that encounter these products at the nation's borders and in the marketplace, to prosecute those who seek to endanger the public through intellectual property offenses.

CRIMINAL ENFORCEMENT RECOMMENDATION #10

Emphasize Charging of Intellectual Property Offenses

RECOMMENDATION: ***The Department of Justice should emphasize the importance of charging intellectual property offenses in every type of investigation where such charges are applicable, including organized crime, fraud, and illegal international smuggling.***

BACKGROUND: Many crimes involve intellectual property offenses. When the focus of the investigation centers on another serious offense, however, the intellectual property offenses are often not emphasized. For example, a counterfeit drug investigation may result

in charges under the federal statutes that prohibit the sale of adulterated pharmaceuticals. In addition, defendants who commit organized crime or fraud offenses where counterfeiting is involved are usually charged with racketeering or fraud violations, sometimes without additional intellectual property charges.

EXPLANATION: Consistent with the Department of Justice's policy that prosecutors must charge the most serious, readily provable offenses, the Task Force believes that the Department of Justice should emphasize that intellectual property offenses should always be charged when appropriate. If an intellectual property offense occurs during the course of other types of criminal activity, such as fraud, organized crime, or international smuggling, prosecutors should also charge the intellectual property offense. The Department of Justice should seek to convict defendants involved in intellectual property offenses regardless of whether the focus of the investigation is on another serious offense, in order to send a message that intellectual property offenses will not be tolerated.

CRIMINAL ENFORCEMENT RECOMMENDATION #11

Enhance Victim Education Programs and Increase Cooperation

RECOMMENDATION: ***The Department of Justice should enhance its program of educating and encouraging victims of intellectual property offenses and industry representatives to cooperate in criminal investigations. Recommended enhancements include:***

(1) Encouraging victims to report intellectual property crime to law enforcement agencies;

(2) Distributing the new "Department of Justice Guide to Reporting Intellectual Property Crime" to victims and industry representatives regarding federal intellectual property offenses; and

(3) Hosting a conference with victims and industry representatives to educate participants on how they can assist in law enforcement investigations.

BACKGROUND: Prosecutors in the Department of Justice have made extensive inroads through public awareness programs to educate victims, consumers, and the law enforcement community that intellectual property enforcement is a priority of the Department of Justice. The Task Force recognizes that combating intellectual property crime requires cooperation among law enforcement, prosecutors, and victims of intellectual property theft, including those who have unwittingly purchased counterfeit or stolen goods.

EXPLANATION: The Department of Justice should enhance its programs to encourage victims of intellectual property offenses and industry representatives to cooperate in criminal

investigations. This can be accomplished in three ways. First, Department of Justice prosecutors should continue to develop regional public awareness programs that encourage intellectual property victims to report offenses to federal authorities at the earliest stage possible.

Effective prosecution of intellectual property crime requires substantial assistance from its victims. Because the holders of intellectual property rights are often in the best position to detect a theft, law enforcement authorities cannot act in many cases unless the crimes are promptly reported to them. Once these crimes are reported, federal law enforcement authorities need to identify quickly the facts that establish jurisdiction for the potential offenses, such as federal copyright and trademark registration information, the extent of the victim's potential loss, the nature of the theft, and the identity of possible suspects. In a digital world where evidence can disappear at the click of a mouse, swift investigation is often essential to a successful prosecution.

Second, the Justice Department should extensively distribute the new "Department of Justice Guide to Reporting Intellectual Property Crime," found in the appendix of this report. This guide will further educate individuals and industry representatives on how to report intellectual property crime. The accompanying checklist should streamline the process, and assist prosecutors and law enforcement agents in the rapid response to reports of intellectual property crimes.

Finally, the Department of Justice should sponsor a conference to explore how victims and industry representatives can assist law enforcement in fighting intellectual property crime. Victim assistance is a critical factor in the success or failure of an intellectual property investigation. Intellectual property enforcement, however, is a complex and sometimes technically challenging area. The conference should be designed to educate participants, and to exchange ideas on the best methods for attacking the problem of intellectual property theft.

CRIMINAL ENFORCEMENT RECOMMENDATION #12

Issue Internal Guidance to Federal Prosecutors Regarding How Victims Can Assist Prosecutors in Intellectual Property Cases

RECOMMENDATION: ***The Department of Justice should issue internal guidance to federal prosecutors regarding how victims can assist prosecutors in intellectual property cases.***

BACKGROUND: Prosecutions of intellectual property crime often depend on cooperation between victims and law enforcement. Without information-sharing from victims, prosecutors cannot enforce the intellectual property laws. Many industry groups and victims of intellectual property theft are eager to assist law enforcement in finding intellectual property offenders and to bring them to justice. Certain types of assistance, however, such as the donation of funds, property, or services by outside sources to federal law enforcement authorities, can raise potential

legal and ethical issues. In general, federal rules and regulations place limitations on the types of assistance victims and outside sources can provide to law enforcement authorities.

EXPLANATION: The Department of Justice should issue internal guidance to Department of Justice prosecutors regarding permissible assistance of victims in intellectual property prosecutions. Victim assistance is a critical factor in the success of an investigation and prosecution of an intellectual property crime. Nevertheless, the Department of Justice must continue its ongoing efforts to educate federal prosecutors about potential legal and ethical issues, in an effort to maintain the Department of Justice's independence and unassailable integrity.

B. INTERNATIONAL COOPERATION RECOMMENDATIONS

The Task Force believes that international cooperation is a critical component in stemming the tide of global intellectual property theft. Intellectual property thieves in foreign countries must be subject to prosecution by foreign governments. In addition, foreign governments must assist the United States in its efforts to gather evidence and prosecute intellectual property criminals who violate the laws of the United States. Accordingly, the Task Force recommends that the Department of Justice adopt the following recommendations to increase cooperation with foreign countries regarding intellectual property enforcement:

(1) **Deploy federal prosecutors to the United States embassies in Hong Kong and Budapest, Hungary, and designate them as "Intellectual Property Law Enforcement Coordinators" ("IPLECs") to coordinate intellectual property enforcement efforts in those regions;**

(2) **Recommend that the FBI co-locate Legal Attachés with intellectual property expertise to Hong Kong and Budapest, Hungary, to assist the newly assigned IPLECs in investigative efforts;**

(3) **Direct prosecutors and agents to increase the use of alternative channels of communication, such as "law enforcement-to-law enforcment" contacts, to collect information and evidence quickly in foreign investigations;**

(4) **Enhance its intellectual property training programs for foreign prosecutors and law enforcement investigators in coordination with the Department of State;**

(5) **Prioritize treaty negotiations for legal assistance agreements with foreign governments where intellectual property enforcement is a significant problem;**

(6) **Ensure that intellectual property crimes are included in all extradition treaties and prioritize negotiations with foreign countries according to intellectual property enforcement concerns; and**

(7) **Emphasize intellectual property enforcement issues during discussions with foreign governments.**

INTERNATIONAL COOPERATION RECOMMENDATION #1

Deploy Intellectual Property Law Enforcement Coordinators to Asia and Eastern Europe

RECOMMENDATION: ***The Department of Justice should deploy federal prosecutors to the United States embassies in Hong Kong and Budapest, Hungary, and designate them as "Intellectual Property Law Enforcement Coordinators" ("IPLECs") to coordinate intellectual property enforcement efforts in those regions.***

BACKGROUND: International cooperation is a major component of a comprehensive intellectual property enforcement program. Many intellectual property offenders operate in countries where the laws are not effective or the relevant expertise of law enforcement is inadequate. Asia and Eastern Europe are areas of particular importance to the creators of intellectual property because of the increasing amount of counterfeiting in the regions.

While developing nations in Asia have increased their manufacturing capacity for legitimate goods, the region has also become a major manufacturer of counterfeit products. Factories in China, Taiwan, and Hong Kong produce numerous counterfeit designer goods and other products protected by United States trademarks. Factories in Singapore and Thailand produce large amounts of counterfeit software and movies that are exported to the United States, sometimes before the films are released to the general public. Consequently, many intellectual property offenses in the United States are traced to manufacturing plants and bank accounts in Asia. In fact, the United States Trade Representative has identified several Southeast Asian countries, such as China, Malaysia, Thailand, Taiwan, Indonesia, and the Philippines, as countries that do not adequately or effectively protect intellectual property rights.

Fortunately, many of these nations are trying to improve the situation and are increasingly cooperative with the United States in its international law enforcement efforts. For example, China has hosted international training programs on intellectual property enforcement and invited Department of Justice officials to participate. In another example, Thailand has extradited to the United States a fugitive accused of intellectual property crimes, and through a joint United States-Hungarian task force on organized crime, Hungary has also cooperated with the Department of Justice and the FBI in attacking international intellectual property offenses.

EXPLANATION: The Department of Justice should encourage the continued cooperation of the governments in Asia and Eastern Europe by assigning a federal prosecutor to the United States embassies in Hong Kong and Budapest, Hungary. The federal prosecutor should have the specific task of coordinating investigations and prosecutions of intellectual property criminals located in the region. The prosecutor should be designated as an "Intellectual Property Law Enforcement Coordinator," or "IPLEC," and should develop relationships with

the foreign law enforcement agencies in the region. The IPLEC should also provide legal and technical assistance and develop training programs on intellectual property enforcement. In addition, the IPLEC should assist prosecutors based in the United States by providing direct contact with foreign law enforcement agencies, and assist in intellectual property investigations.

The Department of Justice should recruit federal prosecutors who are experienced in prosecuting intellectual property crimes for placement as the IPLECs in Hong Kong and Budapest, Hungary. In addition, the IPLECs should be a valuable resource in examining intellectual property crime trends in the region.

INTERNATIONAL COOPERATION RECOMMENDATION #2

Co-Locate FBI Intellectual Property Legal Attachés to Asia and Eastern Europe

RECOMMENDATION: ***The Department of Justice should recommend that the FBI co-locate Legal Attachés with intellectual property expertise to Hong Kong and Budapest, Hungary, to assist the newly assigned IPLECs in investigative efforts.***

BACKGROUND: The Federal Bureau of Investigation currently assigns special agents to United States embassies throughout the world. The agents, known as "Legal Attachés," communicate regularly with foreign law enforcement agencies, assist in joint investigations, and provide expertise when requested by the foreign government. Legal Attachés are responsible for assisting in all types of international investigations, from terrorism to computer crime.

Intellectual property investigations are often complex and involve unique technical issues. For example, investigations that target online intellectual property theft often require specialized computer expertise to track down the offenders and locate important evidence. In addition, the schemes and methods used by intellectual property smugglers are often sophisticated and involve complex financial transactions. Consequently, specially-trained investigators are needed to pursue intellectual property offenders who operate in foreign countries.

EXPLANATION: The Department of Justice should recommend that the FBI assign an Intellectual Property Legal Attaché in Hong Kong and Budapest, Hungary, to assist the federal prosecutor assigned as the Intellectual Property Law Enforcement Coordinator for the region. An effective enforcement program requires close coordination between prosecutors and the skilled investigators who gather evidence, interview witnesses, and develop investigative strategies. An FBI agent assigned as an Intellectual Property Legal Attaché will

significantly increase the effectiveness of international enforcement efforts by providing an experienced United States investigator to support international assistance requests, develop relationships with foreign law enforcement agents, and provide investigative expertise to foreign nations. The Intellectual Property Legal Attaché should receive special training in intellectual property investigations and should work closely with the IPLEC to create international partnerships and task forces in the region.

INTERNATIONAL COOPERATION RECOMMENDATION #3

Increase the Use of Informal Contacts to Gather Evidence from Foreign Countries

RECOMMENDATION: ***Direct prosecutors and agents to increase the use of alternative channels of communication, such as "law enforcement-to-law enforcement" contacts to collect information and evidence quickly in foreign investigations.***

BACKGROUND: International enforcement requires international cooperation in identifying criminal suspects, gathering information from victims, and collecting other types of evidence. The United States has negotiated numerous "Mutual Legal Assistance Treaties" with foreign governments to provide a method to share information and to assist other nations in international criminal investigations. These treaties usually include procedures to interview witnesses and perform other investigative functions. Evidence obtained through formal legal assistance is processed by government agencies in both countries and is typically admissible in United States District Courts. Often, however, investigators need to gather information quickly to determine whether a crime has been committed or to identify criminal suspects before they flee. At that stage of the investigation, it is often unclear whether the case will be prosecuted in the United States or referred to the foreign country where the American rules of evidence do not apply. In addition, evidence that may exist on computers, whether on personal computers or the large networks of foreign Internet Service Providers, is not always preserved and could disappear if immediate action is not taken.

EXPLANATION: While legal assistance treaties provide a reliable mechanism for contacting foreign nations, making information requests, and gathering evidence that is admissible in United States courts, the Department of Justice should explore the use of alternative measures when formal requests are unnecessary, or when the need to gather evidence is time-sensitive. In these situations, law enforcement-to-law enforcement contact should be used to gather information quickly. For example, FBI Legal Attachés assigned to United States embassies often have close working relationships with foreign law enforcement representatives, including national and local police officers. Many times, these "police-to-police" contacts are a much more efficient method to obtain information in criminal investigations, especially when timing is critical. In addition, the police-to-police contacts may open up opportunities for the FBI Legal Attachés to develop relationships with foreign Internet Service Providers, industry representatives, and other commercial contacts where the foreign nation allows such contacts. In many international

investigations, Department of Justice prosecutors have also used "prosecutor-to-prosecutor" and "prosecutor-to-police" contacts with their foreign counterparts to gather information and coordinate international enforcement efforts. The Department of Justice should continue to use these important methods of communication with foreign law enforcement, especially in cases where a legal assistance treaty does not exist between the United States and the foreign government. Consequently, a police-to-police, prosecutor-to-prosecutor, or prosecutor-to-police contact can sometimes be the only method to gather evidence quickly in a criminal investigation.

INTERNATIONAL COOPERATION RECOMMENDATION #4

Enhance Intellectual Property Training Programs for Foreign Prosecutors and Law Enforcement

RECOMMENDATION: ***The Department of Justice should enhance its intellectual property training programs for foreign prosecutors and law enforcement investigators in coordination with the Department of State.***

BACKGROUND: Intellectual property crime is a global problem, but many countries lack the necessary laws, resources, or expertise to enforce intellectual property rights. Numerous foreign countries have yet to develop a legal system to handle intellectual property cases, and many countries that have such laws lack the experience or expertise to prosecute sophisticated offenders. Consequently, foreign prosecutors and investigators are often unable to enforce copyright laws or prosecute large-scale counterfeiters who have stolen the intellectual property of Americans.

EXPLANATION: For the purposes of providing the requisite expertise and enabling the development of critical law enforcement-to-law enforcement relationships, it is essential that the Department of Justice provide additional training and assistance programs to foreign nations focused on intellectual property crimes.

The Department of Justice should identify countries where: (1) intellectual property enforcement would have a significant impact, (2) the foreign governments are willing to create new laws, or modify old ones, to fight intellectual property crimes, and (3) the foreign governments are willing to dedicate resources to fighting intellectual property crime, but lack the expertise to do so.

The Department of Justice should invite these countries to participate in a training program, or series of training programs, to learn about enforcement strategies, receive assistance on drafting new laws, and receive valuable guidance on methods to track down intellectual property criminals. The Justice Department should then further develop the relationships with the participating foreign governments by sending federal prosecutors and investigators to the foreign countries to further assist in the countries' intellectual property enforcement efforts.

INTERNATIONAL COOPERATION RECOMMENDATION #5

Prioritize Negotiations for Legal Assistance Treaties

RECOMMENDATION: ***The Department of Justice should prioritize treaty negotiations for legal assistance agreements with foreign governments where intellectual property enforcement is a significant problem.***

BACKGROUND: Working in close coordination with the Department of State, the Justice Department is actively involved in negotiating treaties with foreign countries to increase cooperation in criminal investigations. For example, the United States negotiates "Mutual Legal Assistance Treaties" with many nations to create a formal method for exchanging evidence and information. These formal international agreements are useful to prosecutors and law enforcement agents because they provide a method for the Department of Justice to request a foreign government to gather evidence, interview witnesses, and to provide other forms of legal assistance. In addition, a legal assistance treaty imposes an important obligation on the foreign country to assist in criminal investigations in accordance with the international agreement.

EXPLANATION: The Department of Justice should prioritize the negotiation of legal assistance treaties with foreign governments where intellectual property enforcement is a significant problem. For example, the Department of Justice should ensure that it has effective legal assistance treaties with the nations in Asia, where counterfeiting has become a significant problem. Many intellectual property investigations in the United States lead to evidence located in Asian and South Asian countries where American law enforcement agents do not have jurisdiction. Therefore, it is vital that the Department of Justice and other government agencies negotiate legal assistance treaties with these countries to increase international cooperation.

INTERNATIONAL COOPERATION RECOMMENDATION #6

Prioritize Negotiations and Include Intellectual Property Crimes in Extradition Treaties

RECOMMENDATION: ***The Department of Justice should ensure that intellectual property crimes are included in all extradition treaties and prioritize negotiations with foreign countries according to intellectual property enforcement concerns.***

BACKGROUND: In addition to legal assistance treaties, the Department of Justice is actively involved in negotiating extradition treaties with foreign countries. Extradition treaties provide a formal process for the Department of Justice to bring an alleged criminal to the United States to face criminal charges. The United States currently has extradition treaties with more than 100 countries, and some of these treaties have been in place for decades. In some of the older extradition treaties, the United States is allowed to seek the extradition of an alleged criminal only if the crime charged is one of the crimes listed in the treaty. In newer treaties, however, the United States may generally seek extradition when the crime charged is

an offense in both countries. For example, if trafficking in counterfeit goods is a crime in both the United States and the foreign country, an alleged criminal in the foreign country could be extradited to the United States to face those charges.

EXPLANATION: The Department of Justice should work to ensure that intellectual property crimes are included in extradition treaties with foreign countries. The United States should seek to negotiate new extradition treaties with countries where intellectual property enforcement is critical and should seek to re-negotiate treaties when intellectual property offenses are not included in existing agreements. The ability of governments to apprehend intellectual property criminals in foreign nations is a critical factor in whether intellectual property laws can be enforced. Consequently, it is important to have effective international extradition treaties that include intellectual property offenses in order to promote global cooperative efforts.

INTERNATIONAL COOPERATION RECOMMENDATION #7

Emphasize Intellectual Property Enforcement During Discussions with Foreign Governments

RECOMMENDATION: ***The Department of Justice should emphasize intellectual property enforcement issues during discussions with foreign governments.***

BACKGROUND: The Attorney General and other Department of Justice officials routinely meet and correspond with foreign law enforcement officials to discuss international cooperation on a wide variety of criminal justice issues. For example, the Attorney General frequently meets and corresponds with Justice Ministers in Asia, Europe, and South America.

EXPLANATION: The Department of Justice should, with increased emphasis, raise the issue of intellectual property enforcement with foreign officials, especially in such regions as Asia and Eastern Europe, where enforcement is of concern to the United States. As set forth in other recommendations in this report, the Department of Justice should offer its expertise and assistance in developing robust intellectual property enforcement programs in foreign nations, developing effective legal assistance treaties, and continuing an open dialogue about emerging intellectual property issues.

C. CIVIL ENFORCEMENT RECOMMENDATION

The Department of Justice's approach to combating the theft of intellectual property is most visible in its enforcement of criminal laws, because the Justice Department is aggressively investigating and prosecuting intellectual property crimes. Success in the fight against intellectual property theft, however, also requires aggressive enforcement of civil laws by the owners of intellectual property. Accordingly, the Task Force recommends that the Department of Justice adopt the following recommendation to increase the effectiveness of civil intellectual property enforcement.

CIVIL ENFORCEMENT RECOMMENDATION

Support Civil Enforcement of Intellectual Property Laws by Owners of Intellectual Property Rights

RECOMMENDATION: ***The Department of Justice should assist private parties in enforcing civil laws that protect intellectual property owners against theft by supporting an effective statutory framework for such enforcement. When a court decision or lawsuit threatens the civil remedies available under federal law, the Justice Department should defend in court all appropriate intellectual property protections and vigorously defend Congress's authority in protecting intellectual property rights.***

BACKGROUND: The owners of intellectual property often use civil lawsuits effectively to protect their intellectual property rights. In recent years, private owners have obtained numerous judgments and settlements against those who steal their intellectual property. Civil lawsuits have proven to be an effective enforcement method in many types of intellectual property cases.

Over the last several years, one of the greatest emerging threats to intellectual property ownership has been the use of peer-to-peer ("P2P") networks. P2P networks are freely accessible on the Internet and allow users to access and copy data files directly from each others' computers. The use of these networks is widespread, and digital copies of audio and video recordings are the most transferred items. It is estimated that millions of users access P2P networks and that the vast majority of users illegally distribute copyrighted material through the networks. In most instances, these violators are difficult to prosecute criminally for a variety of reasons, including the general lack of a profit motive and the relatively low dollar value often involved. Enforcement is thus generally left to owners of the intellectual property to locate offenders and file civil lawsuits against them.

Private civil enforcement, however, is not always effective. Although illegal P2P file sharing is rampant, the Internet has made tracking illegal file sharing very difficult. For example, users of the Internet must gain access through an Internet Service Provider that assigns an "Internet Protocol Address" to the user. The Internet Protocol Address is a unique number that can be

later used to identify the person who used the address. The Internet Service Provider, however, is the sole holder of the information that links the Internet Protocol Address with the identity of the user. Consequently, owners of intellectual property cannot identify users of file sharing programs without the information from the Internet Service Providers.

For years, one of the few legal options available to an owner of a copyright who believed an unknown file sharing user was illegally transmitting copyrighted material was to file a "John Doe" lawsuit against the violator. "John Doe" lawsuits allow the copyright owner, or industry association, to file a lawsuit and start the legal process without knowing the name of the violator. Because Internet Service Providers are not required to maintain records for any length of time, plaintiffs in "John Doe" lawsuits are not always able to obtain a court order in time to identify the violator.

In 1998, Congress provided an alternative to the "John Doe" lawsuits when it enacted the Digital Millennium Copyright Act ("DMCA"). The DMCA allows copyright owners to compel Internet Service Providers to identify alleged infringers by serving a subpoena without having to first file a lawsuit. This legal tool is an improvement in the civil enforcement scheme because it enables copyright owners to move quickly in identifying the name of a suspected violator before any relevant records are erased. Armed with a subpoena, copyright owners can determine who is unlawfully downloading their copyrighted material using P2P networks and then work to resolve the dispute by taking legal action.

Some Internet Service Providers have resisted DMCA subpoenas by contending that the subpoena provision does not apply to their service because they do not store the copyrighted material, but instead only transmit the data. The Justice Department has filed briefs opposing the Internet Service Providers' challenges to the use of the DMCA to identify suspected violators of intellectual property rights and has also defended the constitutionality of the statute.

EXPLANATION: In civil cases where the constitutionality or viability of important civil enforcement tools are at issue, the Department of Justice should intervene by submitting a written brief to the court hearing the case, to protect the use of civil enforcement methods in accordance with federal law. In addition to defending the validity of the DMCA's subpoena provision, the Justice Department has shown its commitment to intervene in cases when other intellectual property laws have come under constitutional attack. Therefore, the Department of Justice should closely monitor civil enforcement developments in the law that may reduce the effectiveness of the private, civil enforcement scheme. When such court decisions arise, the Justice Department must identify them and take affirmative steps to correct them.

D. ANTITRUST ENFORCEMENT RECOMMENDATIONS

The core mission of the Antitrust Division of the Department of Justice is to promote and protect the competitive process and the American economy through enforcement of antitrust laws. These laws prohibit a variety of practices that restrain trade, such as price-fixing conspiracies, corporate mergers likely to reduce competition, and predatory acts designed to achieve or maintain monopoly power. When these practices involve intellectual property, they can raise complex questions about the proper application of antitrust to intellectual property rights. The Department of Justice recognizes that intellectual property rights can promote competition by creating incentives to innovate and commercialize new ideas that enhance consumer welfare. The Department of Justice is also aware that enforcing the antitrust laws in a way that condemns the beneficial use of intellectual property rights could undermine the incentive to create and disseminate intellectual property. The Task Force therefore recommends that the Department of Justice adopt the following recommendations to help ensure that the antitrust laws are appropriately applied to intellectual property in a way that does not chill the exercise of legitimate intellectual property rights.

(1) **Support the rights of intellectual property owners to decide independently whether to license their technology to others;**

(2) **Encourage trade associations and other business organizations seeking to establish industry standards for the prevention of intellectual property theft, to use the Justice Department's business review procedure for guidance regarding antitrust enforcement concerns;**

(3) **Continue to promote international cooperation and principled agreement between nations on the proper application of antitrust lawa to intellectual property rights.**

ANTITRUST ENFORCEMENT RECOMMENDATION #1

Support the Rights of Intellectual Property Owners to Determine Independently Whether to License Their Technology

RECOMMENDATION: ***The Department of Justice should support the rights of intellectual property owners to decide independently whether to license their technology to others.***

BACKGROUND: It is well established under United States law that an intellectual property owner's decision not to license its technology to others cannot violate the antitrust laws. Nonetheless, some critics of robust intellectual property rights have suggested that antitrust laws should be used to force owners of intellectual property rights to share "essential" technology with others, even when that would require them to assist their competitors.

EXPLANATION: Owners of intellectual property rights should be free to decide

independently whether to license their technology to others, without fear of violating the antitrust laws. This was confirmed by a recent legal ruling that expressed great skepticism about applying the antitrust laws in ways that would force companies to share the source of their competitive advantage with others. Although an intellectual property owner has the right to decide not to license its technology, the owner does not have the right to impose conditions on licensees that would effectively extend an intellectual property right beyond its legal limits. The Department of Justice should continue to oppose efforts in the United States and abroad to promote the notion that an independent decision not to license technology is an antitrust violation.

ANTITRUST ENFORCEMENT RECOMMENDATION #2

Encourage Use of the Justice Department's Business Review Procedure

RECOMMENDATION: ***The Department of Justice should encourage trade associations and other business organizations seeking to establish industry standards for the prevention of intellectual property theft, to use the Justice Department's business review procedure for guidance regarding antitrust enforcement concerns.***

BACKGROUND: Trade associations and other organizations often take steps to develop and adopt uniform standards that will better enable industry participants to protect their intellectual property rights and discourage theft of their intellectual property. Digital rights management software, anti-theft software, and other content protection schemes could, for example, be the subject of such standard-setting activities. However, the process of negotiating standards can raise antitrust concerns. For example, competitors involved in the standard-setting process may use such negotiations as a forum for price fixing and other forms of collusion.

EXPLANATION: The Department of Justice's business review procedure provides trade associations and other business organizations seeking to establish industry standards a valuable opportunity to receive guidance from the Department of Justice with respect to the scope, interpretation, and application of the antitrust laws to proposed standard-setting activities. Under that procedure, persons concerned about whether a particular proposed standard-setting activity is legal under the antitrust laws may ask the Department of Justice for a statement of its current enforcement intentions with respect to that conduct. When sufficient information and documents are submitted to the Department of Justice, the Department will make its best effort to resolve the business review request within 60 to 90 days. In this way, the Department of Justice can protect competition while at the same time

facilitate efficient business arrangements that enable intellectual property owners to protect their rights.

ANTITRUST ENFORCEMENT RECOMMENDATION #3

Promote International Cooperation on the Application of Antitrust Laws to Intellectual Property Rights

RECOMMENDATION: ***The Department of Justice should continue to promote international cooperation and principled agreement between nations on the proper application of antitrust laws to intellectual property rights.***

BACKGROUND: While antitrust and intellectual property laws are often national in scope, competition occurs on an increasingly global scale. Differing application of antitrust and intellectual property law principles in different countries can create inefficiencies for global business, result in antitrust violations in some countries for the use of intellectual property that is legal in others, and even lead to the loss of intellectual property rights in certain nations. If nations can reduce such discrepancies in applying antitrust law to intellectual property, they can reduce inefficiencies and promote vigorous cross-border competition.

EXPLANATION: The Department of Justice should continue to promote principled agreement among nations on the proper application of antitrust law to intellectual property. It should continue its efforts to engage in multinational meetings, formal conferences, and informal outreach with foreign antitrust agencies. Through these efforts, the Department of Justice can ensure that the United States and its trading partners have the benefit of each other's experience in dealing with issues at the intersection of antitrust and intellectual property law. Through the establishment of intellectual property working groups with the European Union, Japan, and Korea, the Department of Justice has discussed a wide variety of intellectual property topics vital to the efficient functioning of the global marketplace of ideas. These working groups foster candid communications between the Department of Justice and foreign antitrust enforcers. The Department of Justice should continue these efforts and expand them to include more United States trading partners, and should also closely monitor developments concerning the application of antitrust to intellectual property.

IX. WHAT PRINCIPLES SHOULD APPLY TO PENDING AND FUTURE INTELLECTUAL PROPERTY LEGISLATION?

The Task Force examined a number of pending bills in Congress and developed a set of general principles that should guide pending and future legislation regarding the enforcement of intellectual property rights. This survey does not attempt to identify every principle underlying intellectual property protection or enforcement. Instead, it focuses on principles related to pending legislation, or general proposals for future legislation, that will increase the effectiveness of intellectual property enforcement. Unless noted, the Task Force does not formally endorse or oppose any specific bill, specific provision of a bill, or any of the legislative proposals.

Principles for Pending Legislation

The circumvention of technological safeguards protecting copyrighted works should be subject to prosecution. The owners of intellectual property have the primary responsibility for protecting their creative works from unauthorized duplication. Technological safeguards such as digital rights management software and other forms of copy-protection provide means of doing so. Federal law should reinforce the use of these technological safeguards by preventing their deliberate and unauthorized circumvention.

The Digital Media Consumers' Rights Act of 2003 (H.R. 107) would allow the sale of tools and equipment that could be used to circumvent technological safeguards designed to protect copyrighted works.

The distribution of counterfeit products should be thwarted by seizing, when possible, the materials and equipment used in making them. The distribution of counterfeit products (both goods and creative works) represents not only a theft of intellectual property and a potential source of consumer fraud, but a significant threat to public health and safety. In order to prevent the distribution of counterfeit products, the government should take reasonable steps to prevent their production. When law enforcement officials find materials and equipment that are used to create counterfeit products, the materials and equipment should be seized. Legal loopholes should not allow trafficking in counterfeit labels simply because they have not yet been attached to counterfeit goods.

The Anti-Counterfeiting Amendments of 2003 (H.R. 3632) would expand the prohibition of trafficking in counterfeit labels for copyrighted works to include trafficking in genuine but unauthorized labels and packaging. The bill would also allow the government to seize and impound the equipment used in producing the counterfeit and unauthorized labels.

The Stop Counterfeiting in Manufactured Goods Act (H.R. 4358) would require the destruction of equipment used to manufacture and package counterfeit goods and the forfeiture of any proceeds from the manufacture or sale of such goods. The bill would also prohibit the sale of counterfeit labels that are not attached to any goods and the sale of labels that incorporate an unauthorized reproduction of a trademark.

The passive sharing of copyrighted works for unlawful duplication should be treated as the distribution of those works and should, where appropriate, be subject to prosecution. Distributing unauthorized copies of copyrighted works is a criminal violation if the total retail value of the original work, multiplied by the number of unauthorized copies, reaches a certain monetary threshold. Given the minimal cost of distributing copyrighted works over the Internet, making such files available for others to copy is equivalent to distributing them. The criminal copyright statute should therefore prohibit people from knowingly making available to the public a threshold number of infringing copies or exceeding a threshold value.

The Piracy Deterrence and Education Act (H.R. 4077) would amend the criminal copyright statute to clarify that it may be a violation merely to offer copyrighted works in a digital format for others to copy.

Copyright law should recognize the premium value of a copyrighted work before the work is released for sale to the general public. A copy of a copyrighted work is more valuable before it can be legitimately obtained by anyone else. In such situations, not only is this "pre-release" copy rarer, but it can also permit the holder to distribute copies as early as – or before – the copyrighted work's legitimate owner. As a result, although pre-release copies of a copyrighted work have no legitimate retail value, they can be the most valuable copies of all and their distribution can damage the rights holder. The copyright laws should reflect the premium value of pre-release copies, particularly at the stage of sentencing defendants for criminal violations.

The Piracy Deterrence and Education Act (H.R. 4077) and the Artists' Right and Theft Prevention Act of 2003 (S. 1932) would declare the camcording of films in movie theaters to be a federal felony without proof of the value of a copy of the particular film at issue. These bills also take additional steps to recognize the damage caused by copyright infringement of pre-release works.

The law should provide a remedy against those who intentionally induce infringement. Owners of intellectual property have the primary responsibility for protecting their intellectual property through civil enforcement actions if necessary. Computer networks that facilitate the unauthorized sharing and copying of copyrighted works by users are some of the most dangerous threats to copyright ownership today. A copyright owner should have some express remedy against such networks and other businesses, to the extent that they depend upon and intend for their customers to violate the owner's copyright.

The Inducing Infringement of Copyrights Act (Induce) Act of 2004 (S. 2560) would allow copyright holders to bring a civil suit against individuals and businesses who intentionally induce the infringement of their copyright.

Principles for Future Legislation

The law should prohibit not only the sale of counterfeit goods, but also the possession of counterfeit goods with the intent to sell them. Under current law, it is illegal to sell counterfeit goods (or to attempt to do so), but it is not illegal to possess even large quantities of counterfeit goods with the intention of selling them. As a result, someone who is caught with a warehouse full of counterfeit handbags may escape prosecution for trademark violations if there is no evidence that he has already sold or attempted to sell them.

The Task Force recommends further consideration of a proposal to criminalize the possession of counterfeit goods with the intention of selling or otherwise trafficking in them.

The law should not distinguish between selling counterfeit goods for cash and giving them away with the general expectation of receiving any other type of benefit in the future. Under current trademark law, it is a criminal violation to sell or traffic in counterfeit goods. At least one court has held, however, that it is not illegal to give away such goods where there is no agreement to get something of value from the recipient in return. Under that standard, the distribution of counterfeit goods as samples or as gifts to cultivate a customer's goodwill might not be illegal.

The Task Force recommends further consideration of a proposal to broaden the definition of the word "traffic" in the federal trademark law so that it would explicitly include any distribution of counterfeit goods from which the distributor hopes to gain something of value from any source.

As with other laws involving intellectual property, an attempt to violate the criminal copyright statute should be a violation without regard to whether it is successful. Unlike the federal criminal trademark statute, the criminal copyright statute does not criminalize attempted violations. It is a general tenet of criminal law, however, that those who attempt to commit a crime are as morally culpable as those who succeed in doing so. As a practical matter, individuals who attempt to commit copyright crimes are disproportionately likely to have committed them in the past and to commit them again in the future (unless they have been caught and punished).

The Task Force recommends further consideration of a proposal to amend the criminal copyright statute to outlaw attempted violations.

Law enforcement officers should have access to the full range of accepted law enforcement tools when they investigate intellectual property crimes that pose a serious threat to public health or safety. A federal court may issue an order authorizing the use of a voice intercept, otherwise known as a "wiretap," in the investigation of many federal crimes, including the theft of interstate shipments, but not for intellectual property crimes. Although

there are good reasons to restrict the use of wiretaps in deference to individual privacy rights, some intellectual property crimes present a more serious danger to public health or safety. Trademark violations, for instance, may involve the distribution of counterfeit goods that are defective and prone to causing widespread consumer injuries.

The Task Force recommends further consideration of a proposal to amend the Federal Wiretap Act to provide for the use of voice intercepts in investigating intellectual property crimes specifically when they threaten public health or safety.

Counterfeit and stolen intellectual property should not be permitted to flow into or out of the United States. Under current law, it is not a violation of intellectual property laws simply to import or export unauthorized copies of copyrighted works or counterfeit goods. Given the central role that international distribution plays in intellectual property crimes and the importance of not contributing in any way to intellectual property violations in other countries, the shipping of infringing products across the nation's borders should be expressly prohibited.

The Task Force recommends further consideration of a proposal to criminalize the importation and exportation of counterfeit goods and unauthorized copies of copyrighted works into and out of the United States.

Copyright law should recognize that copies of a copyrighted work are more valuable before copies of the work are released for sale to the general public. The criminal copyright statute often requires federal prosecutors to prove the retail value of the copyrighted work that has been stolen, both to establish that a criminal violation has occurred and to assess the appropriate penalty upon conviction. As explained above, however, copyrighted works that are stolen before they are released for sale lack an established retail value and yet are extraordinarily valuable. The copyright law should recognize and eliminate this tension.

The Task Force recommends a proposal to assign a presumed retail value to copies of copyrighted works that have not yet been released for sale to the public.

The United States should facilitate the prosecution of individuals who are accused of intellectual property violations in another country if the violations would have been crimes under American law. Given the ease and frequency with which perpetrators of intellectual property crimes cross international borders, it is important for the United States and other nations to cooperate whenever necessary in the prosecution of these criminals. Nevertheless, under current law, the United States will not extradite an individual accused of intellectual property crimes unless (1) the United States has a treaty with the nation seeking extradition and (2) that treaty lists intellectual property crimes as a basis for extradition. This presents a significant obstacle to international cooperation because the United States has not finalized extradition treaties with many nations, and many of the treaties that the United States has concluded do not list intellectual property crimes. Therefore, the United States is often precluded from extraditing, and thus securing the extradition of, individuals accused of even the most egregious intellectual property violations.

The Task Force recommends further consideration of a proposal to permit the extradition of individuals who are accused of intellectual property violations that are criminalized under the laws both of the United States and of the other nation, even in the absence of a formal extradition treaty between them.

The United States should support enhanced international enforcement of intellectual property laws. With the globalization of the economy and the rise of digital commerce, intellectual property crimes have crossed international borders with increasing frequency. The United States has signed two treaties that would facilitate international cooperation in halting some of the most egregious of these crimes: the United Nations Convention Against Transnational Organized Crime and the Council of Europe Convention on Cybercrime. The Department of Justice supports the ratification of these treaties, but the Senate has not yet voted on them.

The Task Force recommends the expeditious ratification of both treaties.

X. HOW CAN THE DEPARTMENT OF JUSTICE PREVENT INTELLECTUAL PROPERTY CRIME?

While prosecuting intellectual property crime forms the crux of the Department of Justice's strategy, the Task Force also recognizes that preventing crimes from occurring in the first place is a critical component to any crime-fighting program. Publicizing successful prosecutions is an important way to deter future crimes. In addition, educational initiatives that make clear the consequences of choices made must play a key role in any solution to such a pervasive and complex problem. Accordingly, the Task Force examined several public awareness and prevention issues and recommends that the Department of Justice:

(1) Develop a national program to educate students about the value of intellectual property and the consequences of committing intellectual property crimes by:

(A) Developing materials for student educational programs;

(B) Creating partnerships with non-profit educational organizations to promote public awareness regarding intellectual property crime;

(C) Developing a video to teach students about the negative consequences of intellectual property theft; and

(D) Encouraging federal prosecutors handling intellectual property crime cases throughout the nation to promote the Department of Justice's public awareness programs.

(2) Educate the public about its policy prohibiting the use of peer-to-peer software on Justice Department computer systems; and

(3) Promote authorized use of the FBI's new Anti-Piracy Seal and Warning.

PREVENTION RECOMMENDATION #1

Develop a National Education Program to Prevent Intellectual Property Crime

RECOMMENDATION: ***The Department of Justice should develop a national program to educate students about the value of intellectual property and the consequences of committing intellectual property crimes by: (A) Developing materials for student educational programs, (B) Creating partnerships with non-profit educational organizations to promote public awareness regarding intellectual property crime, (C) Developing a video to teach students about the negative consequences of intellectual property theft, and (D) Encouraging federal prosecutors handling intellectual property crime cases throughout the nation to promote the Department of Justice's public awareness programs.***

BACKGROUND: Prosecuting criminals, civil enforcement, and international cooperation are only some of the methods that can be used to address the problem of intellectual property

theft. As in other areas of the law, public awareness and prevention is a necessary dimension in addressing the growing problem of intellectual property theft. Educating the public, and especially the youth of the nation, about intellectual property rights and responsibilities can be an effective method of deterring crime before it happens. In addition, such educational efforts can generate a better understanding of the value of creative works in the nation's economy and the need to protect these valuable economic resources.

EXPLANATION: The Task Force recommends that the Department of Justice develop a national education campaign on intellectual property. This effort would be aimed at teaching students about the value of creativity and innovation, and would send a clear message that intellectual property theft is both illegal and sometimes dangerous. The education campaign, which will be set in motion by the Task Force's launch event, will be expanded nationwide through the United States Attorney's Offices and through interagency partnerships, as well as cooperation with both non-profit organizations and industry.

The Task Force has developed a proposal to launch the national education campaign with a full-day conference for high school students in October 2004. The Justice Department is currently organizing the event. In partnership with Court TV,[2] and with the help and support of Street Law[3] and i-Safe,[4] the Task Force will bring together about 100 students from high schools in the District of Columbia, Virginia, and Maryland along with teachers, legal experts, and artists, to learn about and discuss intellectual property issues. The conference will feature discussions with diverse speakers representing government, industry, and entertainment; creative presentations by popular artists; workshops aimed at educating the students on the alternatives to illegal downloading and other violations of intellectual property rights; and an opportunity for the students to share their own views and ask questions of the Attorney General and Task Force members.

Such an event can serve as a model for similar conferences nationwide, and may be recorded by Court TV to produce television programming on intellectual property issues. An authorized recording of the program can be distributed throughout the country for use in public awareness events.

The Task Force also recommends that the Department of Justice work with non-profit

[2] Court TV is a cable network that specializes in investigative and forensics programming.

[3] Street Law is a non-profit education provider based in Washington, D.C. It develops programs and written materials to promote awareness of legal rights and responsibilities and to engage youth and adults in the democratic process.

[4] i-Safe America, Inc., is a non-profit foundation dedicated to ensuring the safe and responsible use of the Internet by the nation's youth. It offers a series of interactive classroom lessons (for all grades, K-12) A curriculum section on intellectual property is first offered in fifth grade, and continues through the twelfth grade.

organizations to help develop a set of classroom materials regarding intellectual property. By developing partnerships with organizations that promote youth education on intellectual property, the Department of Justice can build upon existing materials and expand educational opportunities throughout the United States.

The Task Force recommends a new private/public education initiative aimed at teaching fifth and sixth graders about the dangers of intellectual property theft. Working in concert with private industry representatives, the Justice Department's Offices of Public Affairs and Intergovernmental and Public Liaison should develop an educational video to teach students about the value of intellectual property and the dangers and consequences of online theft. The initiative should also foster in students an appreciation for genuine and legal works of creativity. This group should explore launching an initiative in the 2005-2006 school year.

Finally, the Task Force recommends that the Department of Justice use the existing network of talented federal prosecutors to promote the Justice Department's public awareness program. Because federal prosecutors are located in particular regions of the country, they can identify crime problems within their region and tailor public awareness efforts to address those problems. Accordingly, the Department of Justice should encourage every CHIP Coordinator to initiate local educational campaigns on intellectual property, using the materials developed by the Justice Department and its education partners. The program may consist of presentations at local schools, one-day student conferences modeled after the launch event mentioned earlier, or other methods that may appeal to students in the particular region.

PREVENTION RECOMMENDATION #2

Educate the Public Regarding the Department of Justice's Policy on Peer-to-Peer Networks

RECOMMENDATION: ***The Department of Justice should educate the public regarding its policy prohibiting the use of peer-to-peer file sharing networks on Justice Department computer systems.***

BACKGROUND: The Department of Justice has recognized that peer-to-peer networks may pose a danger to computer systems and are often used to distribute copyrighted materials without authorization. On September 17, 2004, the Chief Information Officer for the Justice Department issued a memorandum to every employee discussing the Department of Justice's policy prohibiting the use of peer-to-peer software on its computer systems. A copy of the memorandum is included in the appendix.

EXPLANATION: The Department of Justice should educate the public about its analysis of

peer-to-peer software as a vehicle for distributing unauthorized copies of copyrighted software and the negative effects it can have on computer networks.

PREVENTION RECOMMENDATION #3

Promote Authorized Use and Awareness of The FBI's New Anti-Piracy Seal and Warning.

RECOMMENDATION: ***The Department of Justice should promote authorized use and awareness of the FBI's new Anti-Piracy Seal to deter copyright infringement and trademark offenses.***

BACKGROUND: The FBI is expanding the use of its warning message and seal to address intellectual property rights violations. Last year, the FBI together with the Justice Department collaborated to develop a new FBI Seal for intellectual property enforcement purposes. On November 17, 2003, the Attorney General approved the "Anti-Piracy Seal and Warning." The purpose of the new seal is to warn the public that unauthorized duplication of copyrighted works is a federal crime. The FBI has entered into agreements with record and movie associations to include the seal on copyrighted works as part of a pilot program, and is developing additional agreements with the software and video game industry. The program will serve as a model for future widespread application of the seal. A copy of the seal is included in the appendix.

EXPLANATION: The Department of Justice should promote awareness of the FBI's Anti-Piracy Seal and support its continued use on copyrighted works. The Department of Justice should encourage industry associations to use the seal, in accordance with written agreements with the FBI, on copyrighted works to serve as a visible warning of the consequences of committing intellectual property crimes.

XI. CONCLUSION

This report is not an ending, but a beginning. Under the leadership of the Attorney General, the Task Force looks forward to implementing these recommendations and continuing to improve the performance of the Department of Justice to protect intellectual property.

While technology is constantly advancing, so must the tools and techniques of law enforcement to prevent theft. And as the nation's economy becomes increasingly dependent on intellectual property, law enforcement must work harder to protect that which makes America prosperous.

* * * * *

XII. APPENDICES

The Federal Bureau of Investigation's Anti-Piracy Warning Seal The Department of Justice

APPENDIX B

Memorandum on the Use of Peer-to-Peer File Sharing Technology

U.S. Department of Justice

Washington, D.C. 20530

September 17, 2004

MEMORANDUM FOR HEADS OF COMPONENTS
COMPONENT CHIEF INFORMATION OFFICERS
ALL DEPARTMENT OF JUSTICE EMPOLYEES

FROM: Paul R. Corts
Assistant Attorney General for Administration

SUBJECT: Information Technology Security Awareness Training
Use of Peer-to-Peer File Sharing Technology

Peer-to-Peer (P2P) file sharing is a capability that allows individual users of the Internet to connect to each other and share files. These systems tend to be highly decentralized and tailored to persons seeking to exchange certain types of files. While there may be appropriate uses of this technology, research shows that the vast majority of files exchanged on P2P networks are copyrighted music, motion pictures, and pornography. P2P file exchanges are also a common distribution avenue for viruses and other types of malicious code.

Department computer systems, as well as those operated by contractors on the Government's behalf, may not be used for the sharing of illegal material or unauthorized copyrighted material. There are very rare occasions when employees need to use P2P capabilities within the Department. Such uses can only be authorized after consultation with the CIO. Use of the P2P file sharing using the Internet is expressly forbidden. Technical controls on such use are already in place and they will be strengthened as appropriate.

Every component in the Department of Justice is anxious to use new information technology (IT) to service our mission. At the same time, we must continuously monitor our systems and networks and the use of new technology to ensure the integrity, confidentiality, and availability of IT services.

This memo is intended to augment IT security training for all users by increasing your awareness of the vulnerabilities and policies associated with P2P. Training material on P2P file sharing will be included in online security awareness training programs used in the Department. If you have any questions or require additional information on P2P, please contact Martin Burkhouse on (202) 616-4574, or by email at martin.t.burkhouse@usdoj.gov.

Reporting Intellectual Property Crime:

A Guide for Victims of Counterfeiting, Copyright Infringement, and Theft of Trade Secrets

The United States Department of Justice's Task Force on Intellectual Property Enforcement

Reporting Intellectual Property Crime: A Guide for Victims of Counterfeiting, Copyright Infringement, and Theft of Trade Secrets

Contents

What are Copyrights, Trademarks and Trade Secrets?

The United States has created enforceable rights in "intangibles" that are known as intellectual property, including copyrights, trademarks and trade secrets. ***Copyright law*** provides federal protection against infringement of certain exclusive rights, such as reproduction and distribution, of "original works of authorship," including computer software, literary works, musical works, and motion pictures. The use of a commercial brand to identify a product is protected by ***trademark law***, which prohibits the unauthorized use of "any word, name, symbol, or device" used by a person "to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods." Finally, trade secret law provides legal protection for any formula, device, or compilation of information used in a business from being disclosed without the owner's permission. However, legal protection is only afforded to those trade secrets that possess independent economic value and which the owner has taken reasonable measures to keep secret.

How Can Intellectual Property Be Stolen?

Intellectual property may be stolen or misappropriated in many ways. A copyrighted work may be illegally infringed by making and selling an unauthorized copy, as with infringing computer software. A trademark may be infringed by selling a good with a counterfeit mark. A trade secret may be stolen from its owner and used to benefit a competitor.

What Types of Intellectual Property Theft Constitute a Federal Crime?

Although civil remedies may provide compensation to wronged intellectual property rights holders, criminal sanctions are often warranted to ensure sufficient punishment and deterrence of wrongful activity. Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business for defendants. Among the most significant provisions are the following:

Counterfeit Trademarks: The Trademark Counterfeiting Act, 18 U.S.C. § 2320(a), provides penalties of up to ten years imprisonment and a $2 million fine for a defendant who "intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services."

Counterfeit Labeling: The counterfeit labeling provisions of 18 U.S.C. § 2318 prohibit trafficking in counterfeit labels designed to be affixed to phono records, copies of computer programs, motion pictures and audiovisual works, as well as trafficking in counterfeit documentation or packaging for computer programs. Violations are punishable by up to 5 years imprisonment and a $250,000 fine.

Criminal Copyright Infringement: Copyright infringement is a felony punishable by up to 3 years imprisonment and a $250,000 fine under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319 where a defendant willfully reproduces or distributes at least 10 copies of one or more copyrighted works with a total retail value of more than $2,500 within a 180_day period. The maximum penalty rises to 5 years imprisonment if defendant acted "for purposes of commercial advantage or private financial gain." Misdemeanor copyright infringement occurs where the value exceeds $1,000.

Theft of Trade Secrets: The Economic Espionage Act contains two separate provisions that criminalize the theft of trade secrets. The first provision, 18 U.S.C. § 1831(a), prohibits thefts of the trade secrets for the benefit of a foreign government or agent, and is punishable by up to 15 years imprisonment and a $500,000 fine. The second, 18 U.S.C. § 1832, prohibits thefts of commercial trade secrets, and is punishable by up to 10 years imprisonment and a $250,000 fine. The statute broadly defines the term "trade secret" to include all types of information which the owner has taken reasonable measures to keep secret and which has independent economic value.

Confidentiality: Federal law also provides special protections to victims in trade secret cases to preserve the confidentiality of the information during criminal proceedings. The statute provides that courts "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835.

Why Should You Report Intellectual Property Crime?

Intellectual property is an increasingly important part of the United States' economy, representing its fastest growing sector. For example, in 2002 copyright industries alone contributed approximately 6%, or $626 billion, to America's gross domestic product, and employed 4% of America's workforce, according to an economic study commissioned by the International Intellectual Property Alliance. As the nation continues to shift from an industrial economy to an information-based economy, the assets of the country are increasingly based in intellectual property.

In recognition of this trend, the Department of Justice is waging the most aggressive campaign against the theft and counterfeiting of intellectual property in its history. The priority of criminal intellectual property investigations and prosecutions nationwide has been increased, and additional resources on both the prosecutive and investigative levels have been brought to bear on the growing problem of intellectual property theft.

Effective prosecution of intellectual property crime, however, also requires substantial assistance from its victims. Because the holders of intellectual property rights are often in the

best position to detect a theft, law enforcement authorities cannot act in many cases unless the crimes are reported in the first place. Once these crimes are reported, federal law enforcement authorities need to quickly identify the facts that establish jurisdiction for the potential intellectual property offenses, such as federal copyright and trademark registration information, as well as facts concerning the extent of victim's potential loss, the nature of the theft and possible suspects. In a digital world where evidence can disappear at the click of a mouse, swift investigation is often essential to successful intellectual property prosecutions.

Accordingly, the Department of Justice has created this handbook to facilitate the flow of critical information from victims of intellectual property crimes to law enforcement authorities. The Department of Justice's aim is to make it as easy as possible to report incidents of intellectual property crime to law enforcement authorities, including whom to call and what to tell them.

Note: The guidelines set forth below seek information that, in the experience of Department of Justice prosecutors and investigators, is useful or even critical to the successful prosecution of the most common intellectual property crimes. These guidelines are not intended to be exhaustive, nor does the presence or absence of responsive information from the victim necessarily determine the outcome of an investigation.

What Should You Do if You are Victimized?

Victims of intellectual property crime such as counterfeiting and theft of trade secrets often conduct internal investigations before referring matters to law enforcement. These investigations can encompass a variety of investigative steps, including interviews of witnesses, acquisition of counterfeit goods, surveillance of suspects, and examination of computers and other evidence. Victims can maximize the benefit of these independent investigative activities as follows:

1. Document All Investigative Steps: To avoid duplication of effort and retracing of steps, internal investigations should seek to create a record of all investigative steps that can later be presented to law enforcement, if necessary. If a victim company observes counterfeit goods for sale online and makes a purchase, for example, investigators should record the name of the Web site, the date and time of the purchase, the method of payment, and the date and manner of delivery of the goods. Any subsequent examination of the goods should then be recorded in a document that identifies the telltale characteristics of theft or counterfeiting, such as lack of a security seal, poor quality or the like.

Similarly, in the case of a suspected theft of trade secrets, any internal investigation or surveillance of the suspect, or a competitor believed to be using the stolen information, should be recorded in writing. A record of any interviews with suspects or witnesses should be made by tape or in writing. The pertinent confidentiality agreements, security policies and access logs should also be gathered and maintained to facilitate review and reduce the risk of deletion or destruction.

2. Preserve the Evidence: Any physical, documentary or digital evidence acquired in the course of an internal investigation should be preserved for later use in a legal proceeding. In the online theft example identified above, victims should print-out or obtain a digital copy of the offending Web site and safely store any infringing goods and their packaging, which may contain valuable details of their origin. If the computer of an employee suspected of stealing trade secrets has been seized, any forensic analysis should be performed on a copy of the data, or "digital image," to undermine claims that the evidence has been altered or corrupted.

3. Contact Law Enforcement Right Away: Victims can maximize their legal remedies for intellectual property crime by making contact with law enforcement soon after its detection. Early referral is the best way to ensure that evidence of an intellectual property crime is properly secured and that all investigative avenues are fully explored, such as the execution of search warrants and possible undercover law enforcement activities. Communication with law enforcement authorities at the onset of suspected violations also allows a victim to coordinate civil proceedings with possible criminal enforcement. Use the reporting guides set forth later in this document to organize the information you gather and provide the necessary information to your law enforcement contact.

How Can You Assist Law Enforcement?

Prosecutions of intellectual property crime often depend on cooperation between victims and law enforcement. Indeed, without information sharing from intellectual property rights holders, prosecutors can neither discern the trends that suggest the most effective overall enforcement strategies, nor meet the burden of proving the theft of intellectual property in a specific case. The following seeks to provide guidance concerning the types of assistance that may be offered by victims of intellectual property theft to law enforcement authorities.

Identify Stolen Intellectual Property: Just as in cases involving traditional theft, such as a burglary or shoplifting, victims of intellectual property theft may – and often must – assist law enforcement in the identification of stolen property. Thus, law enforcement may call upon a victim representative or expert to examine items obtained during an investigation to determine their origin or authenticity. In a copyright infringement or trademark investigation, for example, an author or software company may be called upon to analyze CDs or other media that appear to be counterfeit, while a victim representative in a theft of trade secret case may be asked to review documents or computer source code. Prosecutors may later the seek expert testimony from the victims at trial.

In certain investigations, law enforcement agents also may request a victim's presence during the execution of a search warrant to help the agents identify specific items to be seized. In those circumstances, the victim's activities will be strictly limited to those directed by supervising law enforcement agents.

Share the Results of Internal Investigations or Civil Lawsuits: As with any suspected crime, victims may provide law enforcement with information gathered as a result of internal investigations into instances of intellectual property theft. This handbook contains a section on "Gathering Information on Suspected Intellectual Property Crime" to provide guidance on how a victim can maximize the benefit of any internal investigations it chooses to conduct. In addition, unless the proceedings or information has been ordered sealed by a court, victims may generally provide law enforcement with any evidence or materials developed in civil intellectual property enforcement actions, including court pleadings, deposition testimony, documents and written discovery responses.

Participate in Law Enforcement Task Forces: Federal, state and local law enforcement agencies and prosecutors all over the country have formed task forces to combat computer and intellectual property crime and to promote information sharing between government and industry. The United States Secret Service, for example, has created Electronic Crimes Task Forces in 13 cities, and the Federal Bureau of Investigation has founded more than 60 "Infragard" chapters around the country. In addition, many areas have "high-tech crime" task forces that investigate intellectual property theft. Members of the intellectual property industry are encouraged to participate in these organizations to establish law enforcement contacts that will enable these members to quickly respond to incidents of intellectual property and other crime. (Information on joining these organizations is available on the Web at *www.ectaskforce.org* and *www.infragard.net*).

Contributions of Funds, Property, or Services: Donating funds, property, or services to federal law enforcement authorities can raise potential legal and ethical issues that must be addressed on a case-by-case basis. In general, federal law places limitations on contributions to law enforcement authorities.

Checklist for Reporting a Copyright Infringement or Counterfeit Trademark Offense

If you or your company have become the victim of a copyright infringement or counterfeit trademark offense, please fill out the information as indicated below and contact a federal law enforcement official to report the offense. An insert with contact information for law enforcement officials in your area should be included at the end of this guide.

Background and Contact Information:

1. Victim's Name:

2. Primary Address:

3. Nature of Business:

4. Contact:

Phone: Fax:

Email: Pager/Mobile:

Description of the Intellectual Property

5. Describe the copyrighted material or trademark (e.g., title of copyrighted work, identity of logo):

6. Is the copyrighted work or trademark registered with the U.S. Copyright Office or the Federal Patent and Trademark Office? ___ YES ___NO

   a. If so, please provide the following:

      i. Registration Date:

      ii. Registration Number:

      iii. Do you have a copy of the certificate of registration?

      iv. Has the work or mark been the subject of a previous civil or criminal enforcement action? If so, please provide a general description.

b. If not, state if and when you intend to register:

7. What is the approximate retail value of the copyrighted work or trademarked good?

Description of the Intellectual Property Crime

8. Describe how the theft or counterfeiting was discovered:

9. Do you have any examination reports of the infringing or counterfeit goods? ___YES ___NO.
(If so, please provide those reports to the law enforcement official).

10. Describe the scope of the theft or counterfeiting operation, including the following information:

a. Estimated quantity of illegal distribution:

b. Estimated time period of illegal distribution:

c. Is the illegal distribution national or international? Which states or countries?

11. Identify where the theft or counterfeiting occurred, and describe the location:

12. Identify the name(s) or location(s) of possible suspects, including the following information:

Name (Suspect #1):

Phone number:

Email address:

Physical address:

Current employer, if known:

Reason for suspicion:

Name (Suspect #2):

Phone number:

Email address:

Physical address:

Current employer, if known:

Reason for suspicion:

13. If the distribution of infringing or counterfeit goods involves the Internet (e.g., World Wide Web, FTP, email, chat rooms), identify the following:

    a. The type of Internet theft:

    b. Internet address, including linking sites (domain name, URL, IP address, email):

    c. Login or password for site:

    d. Operators of site, if known:

14. If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired:

Civil Enforcement Proceedings

15. Has a civil enforcement action been filed against the suspects identified above? ___YES ___NO

    a. If so, identify the following:

        i. Name of court and case number:

        ii.Date of filing:

        iii. Names of attorneys:

        iv. Status of case:

    b. If not, is a civil action contemplated? What type and when?

16. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Checklist for Reporting a Theft of Trade Secrets Offense

If you or your company have become the victim of a theft of trade secrets offense, please fill out the information indicated below and contact a federal law enforcement official to report the offense. An insert with contact information for law enforcement officials in your area should be included at the end of this guide.

NOTE ON CONFIDENTIALITY: Federal law provides that courts "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835. Prosecutors utilizing any of the information set forth below will generally request the court to enter an order to preserve the status of the information as a trade secret and prevent its unnecessary and harmful disclosure.

Background and Contact Information

1. Victim's Name:

2. Primary Location and Address:

3. Nature of Primary Business:

4. Law Enforcement Contact:

Phone: Fax:

Email: Pager/Mobile:

Description of the Trade Secret

5. Generally describe the trade secret (e.g., source code, formula):

Provide an estimated value of the trade secret identifying ONE of the methods and indicating ONE of the ranges listed below:

Method

___Cost to Develop the Trade Secret;

___Acquisition Cost (identify date and source of acquisition); or

___Fair Market Value if sold.

Estimated Value:

___Under $50,000;

___Between $50,000 and $100,000;

___Between $100,000 and $1 million;

___Between $1 million and $5 million; or

___Over $5 million

Identify a person knowledgeable about valuation, including that person's contact information:

General Physical Measures Taken to Protect the Trade Secret

6. Describe the general physical security precautions taken by the company, such as fencing the perimeter of the premises, visitor control systems, using alarming or self-locking doors or hiring security personnel.

7. Has the company established physical barriers to prevent unauthorized viewing or access to the trade secret, such as "Authorized Personnel Only" signs at access points? (See below if computer stored trade secret.) ___YES ___NO

8. Does the company require sign in/out procedures for access to and return of trade secret materials? ___YES ___NO

9. Are employees required to wear identification badges? ___YES ___ NO

10. Does the company have a written security policy? ___YES ___NO

    a. How are employees advised of the security policy?

    b. Are employees required to sign a written acknowledgment of the security policy? ___YES ___NO

    c. Identify the person most knowledgeable about matters relating to the security policy, including title and contact information.

11. How many employees have access to the trade secret?

12. Was access to the trade secret limited to a “need to know” basis? ___YES ___NO

Confidentiality and Non-Disclosure Agreements

13. Does the company enter into confidentiality and non-disclosure agreements with employees and third-parties concerning the trade secret? ___YES ___NO

14. Has the company established and distributed written confidentiality policies to all employees? ___YES ___NO

15. Does the company have a policy for advising company employees regarding the company’s trade secrets? ___YES ___NO

Computer-Stored Trade Secrets

16. If the trade secret is computer source code or other computer-stored information, how is access regulated (e.g., are employees given unique user names and passwords)?

17. If the company stores the trade secret on a computer network, is the network protected by a firewall? ___YES ___NO

18. Is remote access permitted into the computer network? ___YES ___NO

19. Is the trade secret maintained on a separate computer server? ___YES ____NO

20. Does the company prohibit employees from bringing outside computer programs or storage media to the premises? ___YES ___NO

21. Does the company maintain electronic access records such as computer logs? ___YES ___NO

Document Control

22. If the trade secret consisted of documents, were they clearly marked "CONFIDENTIAL" or "PROPRIETARY"? ___YES ___NO

23. Describe the document control procedures employed by the company, such as limiting access and sign in/out policies.

24. Was there a written policy concerning document control procedures, and if so, how were employees advised of it? ___YES ___NO

25. Identify the person most knowledgeable about the document control procedures, including title and contact information.

Employee Controls

26. Are new employees subject to a background investigation? ___YES ___NO

27. Does the company hold "exit interviews" to remind departing employees of their obligation not to disclose trade secrets? ___YES ___NO

Description of the Theft of Trade Secret

28. Identify the name(s) or location(s) of possible suspects, including the following information:

    Name (Suspect #1):

    Phone number:

Email address:

Physical address:

Employer:

Reason for suspicion:

Name (Suspect #2):

Phone number:

Email address:

Physical address:

Employer:

Reason for suspicion:

29. Was the trade secret stolen to benefit a third party, such as a competitor or another business? ___YES ___NO

If so, identify that business and its location:

30. Do you have any information that the theft of trade secrets were committed to benefit a foreign government or instrumentality of a foreign government? ___YES ___NO

If so, identify the foreign government and describe that information.

31. If the suspect is a current or former employee, describe all confidentiality and non-disclosure agreements in effect.

32. Identify any physical locations tied to the theft of trade secret, such as where it may be currently stored or used.

33. If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired:

Civil Enforcement Proceedings

34. Has a civil enforcement action been filed against the suspects identified above? ___YES ___NO

a. If so, identify the following:

i. Name of court and case number:

ii. Date of filing:

iii. Names of attorneys:

iv. Status of case:

b. If not, is a civil action contemplated? What type and when?

35. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

LAW ENFORCEMENT CONTACTS IN YOUR AREA: