OFFICE OF THE UNITED STATES INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR

MARCH/APRIL 2013 EDITION

Intellectual Property Spotlight

Contents

Introduction

I am pleased to report that the United States Sentencing Commission submitted to Congress amendments to the federal sentencing guidelines to add new sentencing enhancements for intellectual property-related crimes. Three of these amendments reflect changes called for by the Administration's March 2011 White Paper on Intellectual Property Enforcement Legislative Recommendations and the Administration's letter to the U.S. Sentencing Commission. The amendments would enhance offense levels for international trade secret and economic espionage; trafficking in counterfeit drugs; and sales of counterfeits to the military.

Also, I want to highlight two criminal intellectual property cases involving military equipment. In the first case, a former defense contractor employee was sentenced to 70 months for trade secret theft and exporting sensitive military technology to China after he stole thousands of electronic files involving missiles and rockets from his former employer. In the second case, a defense contractor employee was sentenced to one year in prison for conspiracy to commit criminal copyright infringement after he obtained unauthorized copies of industrial software from China and Russia and used the unauthorized software to conduct computer simulations for military contracts and law enforcement.

Finally, on April 26th, U.S. Government agencies recognized World Intellectual Property Day with a variety of programs. World IP Day is designed to increase public awareness of IP issues.

Victoria A. Espinel

U.S. Intellectual Property Enforcement Coordinator

Combating Trade Secret Theft and Threats to the Military

Former Employee of Defense Contractor Sentenced To 70 Months In Prison For Exporting Sensitive Military Technology To China and Trade Secret Theft

Military Technology Exports Conviction

"As an innovation leader, the United States is a target for those seeking to cut corners at the expense of American businesses and consumers," said U.S. Attorney Paul J. Fishman. "As this sentence shows, the Department of Justice is making great progress in the fight against trade secret theft in order to protect the engines of our nation's economic recovery."

On March 25th, Sixing Liu (aka "Steve Liu"), a Chinese citizen and former New Jersey-based defense contractor employee—who was convicted by a federal jury for exporting sensitive U.S. military technology to the People's Republic of China, stealing trade secrets and lying to federal agents—was sentenced to 70 months in prison. In addition to the prison term, Mr. Liu was sentenced to serve three years of supervised release and ordered to pay a $15,000 fine. In 2010, Mr. Liu stole thousands of electronic files from his employer, L-3 Communications, Space and Navigation Division, to position and prepare himself for future employment in China. The stolen files detailed the performance and design of guidance systems for missiles, rockets, target locators and unmanned aerial vehicles, and several contained export-controlled technical data that relates to defense items listed on the United States Munitions List. (Federal Bureau of Investigation (FBI); Immigration and Customs Enforcement (ICE)-Homeland Security Investigations (HSI); U.S. Customs and Border Protection (CBP); U.S. Attorney's Office (USAO) National Security Unit and Computer Hacking and Intellectual Property Section (CHIPS), both of Newark; U.S. Department of Justice's National Security Division, Counterespionage Section)

Software Piracy Conviction

"Each year, American companies lose intellectual property valued in the billions of dollars to international cybercriminals engaged in rampant digital theft," said U.S. Attorney Charles M. Oberly, III. "The successful prosecution of this conspiracy ring proves that neither the international cybercriminal behind a computer in China nor his customers behind computers in America are beyond the reach of U.S. law enforcement."

Chief Scientist of Government Contractor Sentenced to Prison—Used Pirated Software from Chinese and Russian Cybercriminals to Conduct Military Computer Simulations

On March 18th, Dr. Wronald Best, of Owensboro, Kentucky, was sentenced to one year in prison and three years of supervised release for conspiracy to commit criminal copyright infringement, in which Dr. Best obtained over $2.3 million in stolen software from Chinese and Russian cybercriminals. Between September 2008 and May 2011, Dr. Best conspired with computer software pirates located in China and Russia to obtain and utilize over 60 unauthorized copies of industrial-grade software worth over $2.3 million in the performance of government contracts for the military and law enforcement sectors. At the time, Dr. Best held the position of "Chief Scientist" at MPD, Inc., a Kentucky-based government contractor that services the U.S. and foreign militaries and law

enforcement agencies. Dr. Best told special agents that he used the unauthorized software to conduct computer simulations on components MPD, Inc. was designing for use in military helicopters, including the Black Hawk helicopter and the presidential "Marine One" helicopter, in Patriot missile components, and in police radar and breath analysis equipment widely used by American police departments. (ICE-HSI; Defense Criminal Investigative Service; USAO D. Del.)

Sentencing Commission Recommends Increased Penalties for Offenses Involving Trade Secrets, and Counterfeit Drugs and Military Goods and Services

On April 30th, the U.S. Sentencing Commission submitted sentencing guidelines amendments which will provide sentencing enhancements for offenses involving economic espionage and trade secret theft, and trafficking in counterfeit drugs and military goods and services. Acting pursuant to the Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. 112-269 (Jan. 14, 2013), which directed the Commission to review the guidelines applicable to Economic Espionage and Trade Secret offenses, the Commission recommended that the guidelines be increased by two levels for persons convicted of offenses related to the transmission of stolen trade secrets outside the United States, and four levels for persons convicted of offenses that would benefit a foreign government or instrumentality. Likewise, implementing Section 818 of the National Defense Authorization Act for Fiscal Year 2012, Pub. L. 112-81 (Dec. 31, 2011) (prohibiting trafficking in counterfeit military goods) and the Food and Drug Administration Safety and Innovation Act, Pub. L. 112-144 (July 9, 2012)(prohibiting counterfeit drug trafficking), the Commission recommended two level enhancements for offenses involving trafficking of counterfeit drugs and military goods and services.

Critical Infrastructure and Public Safety

"Operation Core Systems"

CBP and French Customs completed "Operation Core Systems," a six-month enforcement operation targeting counterfeit critical electronic components such as semiconductors, computer networking equipment, hard drives and memory cards. Combined, the two customs agencies seized 480 shipments of products potentially jeopardizing critical infrastructures, public safety, and computer network efficiency and security.

Michigan Computer Company, Owner Sentenced for International Counterfeiting and Environmental Crimes

On March 22nd, Mark Jeffrey Glover and his company, Discount Computers Inc. (DCI), were sentenced for trafficking in counterfeit goods and environmental crimes. Mr. Glover was sentenced to 30 months incarceration, 24 months of supervised release, and a $10,000 fine. Mr. Glover pleaded guilty to the charges on behalf of his company and himself in October 2012. DCI was also sentenced for storing and disposing of hazardous waste without a permit. DCI received a $2 million fine and must pay $10,839 in restitution. DCI operated as a broker of used electronic components such as computers and televisions. A large part of DCI's business involved exporting used cathode ray tube (CRT) monitors to Middle East and Asian countries. To evade Egypt's prohibition against importing computer equipment that was more than five years old, DCI replaced original factory labels on used CRT monitors with counterfeit labels which falsely reflected a more recent manufacture date. Over a five year period, DCI sent to Egypt more than 100,000 used CRT monitors with a total shipment value of at least $2.1 million. (ICE-HSI; Environmental Protection Agency (EPA)-Criminal Investigation Division (CID); USAO E.D. Mich.)

"The men and women of CBP protect our nation's economy, the safety of its people, and our national security against the harm of counterfeit goods," said Robert E. Perez, Director of Field Operations in New York.

CBP Seizes Thousands of Counterfeit Pharmaceuticals

In early March, U.S. Customs and Border Protection seized approximately 150,000 counterfeit and prohibited pharmaceuticals during a three-day operation at the international mail facility at John F. Kennedy Airport. The manufacturer's suggested

retail price of the seized pharmaceuticals was $1.9 million. (CBP's Pharmaceutical, Health and Chemicals Center of Excellence and Expertise in New York; ICE-HSI)

CBP Seizes Nearly 15,000 Toasters with Counterfeit Safety Markings

On March 8th and March 28th, CBP officers and import specialists assigned to the Los Angeles/Long Beach seaport complex seized 14,904 toasters from China bearing counterfeit Underwriters Laboratories (UL) safety markings. An independent product safety certification organization, UL tests and evaluates products for potential risk of fire, shock, and/or personal injury. The uncertified toasters were seized after UL confirmed that the safety markings on the toasters were counterfeit. The combined estimated manufacturer's suggested retail value of the products is $297,931. (CBP Los Angeles/Long Beach seaport)

Los Angeles-Area Man Sentenced to 15 Months for Distributing Counterfeit Pharmaceuticals

On April 4th, Edward Alarcon was sentenced to 15 months in federal prison for his involvement in a scheme to distribute more than 2,000 Chinese-made counterfeit pharmaceutical pills. After a three-day trial, Mr. Alarcon was convicted on two counts of trafficking in counterfeit OxyContin and Cialis. The evidence at trial showed he had purchased the bogus OxyContin from a Chinese national and that he had offered to sell counterfeit Cialis, Viagra and Levitra on Craigslist. (ICE-HSI; Food and Drug Administration (FDA)-Office of Criminal Investigations; United States Postal Inspection Service (USPIS); USAO C.D. Cal.)

Significant Sentences in IP Crimes

Member of Internet Piracy Group "IMAGiNE" Sentenced to 23 Months in Prison for Criminal Copyright Conspiracy

On April 10th, Javier E. Ferrer, a member of the Internet piracy group "IMAGiNE" was sentenced to serve 23 months in prison as well as three years of supervised release and ordered to pay $15,000 in restitution for his role in the IMAGiNE Group, an organized online piracy ring that sought to become the premier group to first release Internet copies of movies only showing in theaters. Mr. Ferrer is the fifth member of the IMAGiNE Group who has been sentenced to prison for the copyright conspiracy. Others involved in the conspiracy were sentenced to prison terms ranging from 23 months to 60 months in prison. (ICE-HSI Intellectual Property Rights (IPR) Coordination Center, USAO E.D.Va., DOJ Computer Crime and Intellectual Property Section (CCIPS), CCIPS Cyber Crime Lab, DOJ Criminal Division Office of International Affairs)

Raising Public Awareness Regarding IP Infringement

Theater Owners, MPAA, IPR Center Partner to Combat Movie Piracy

On April 26th, the National Intellectual Property Rights Coordination Center (IPR Center), the Motion Picture Association of America (MPAA), and the National Association of Theatre Owners announced the planned release of a new trailer aimed at educating the public about the laws against movie piracy. The 15-second trailer is designed to shed light on the serious problem of illegal recordings of movies and will begin airing in movie theaters nationwide this summer. Illegal recordings, or "camcording," in the theater is the single largest source of bootleg DVDs sold on the street and pirated copies of movies distributed on the Internet, and is a federal felony in the United States.

If you feel that you have been the victim of an intellectual property crime, you can report the crime by clicking on the button to the left, calling the IPR Center at 1-866-IPR-2060, or contacting a field office of the FBI. To help you determine what to do when reporting an intellectual property crime, see DOJ's "Reporting Intellectual Property Crime: A Guide for Victims of Counterfeiting, Copyright Infringement, and Theft of Trade Secrets." DOJ also has created forms/checklists that identify the information you will need to provide when referring copyright infringement and trademark offenses and theft of trade secrets.

If you would like to subscribe to the newsletter in the future, email IntellectualProperty@omb.eop.gov. If you would like more information about the Office of the IPEC, including a copy of the 2010 Joint Strategic Plan on Intellectual Property Enforcement, please visit our website.