Department of Justice

STATEMENT OF

JOSH GOLDFOOT
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET OF THE JUDICIARY COMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES

FOR A HEARING ENTITLED

"INTELLECTUAL PROPERTY: ENFORCEMENT ACTIVITIES BY THE EXECUTIVE BRANCH"

PRESENTED

MAY 7, 2024

STATEMENT OF JOSH GOLDFOOT
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
UNITED STATE DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY,
AND THE INTERNET OF THE
JUDICIARY COMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES

FOR A HEARING ENTITLED
"INTELLECTUAL PROPERTY: ENFORCEMENT ACTIVITIES
BY THE EXECUTIVE BRANCH"

PRESENTED
MAY 7, 2024

Good morning, Chairman Issa, Ranking Member Johnson, and distinguished Members of the Subcommittee. My name is Josh Goldfoot, and I am an Acting Deputy Assistant Attorney General in the Criminal Division at the Department of Justice. Thank you for the opportunity to testify today about the important work of the Department of Justice in prosecuting intellectual property crime. It is an honor to be here today with representatives of the agencies that detect and investigate intellectual property (IP) crime. Working together in a large interagency coalition, we seek consistent and effective IP policy both domestically and around the world.

Computer Crime and Intellectual Property Section (CCIPS) Mission, Priorities, and Cases

The core responsibility of the Criminal Division is to ensure the enforcement of U.S. law through effective prosecutions to vindicate the interests of the public and to deter future unlawful conduct. The Criminal Division prosecutes all federal crimes not otherwise specifically assigned to other Divisions. The Computer Crime & Intellectual Property Section—also known as CCIPS—is a section within the Criminal Division, and it executes the Criminal Division's work in enforcing criminal IP statutes. The members of the IP team at CCIPS prosecute criminal IP cases, as well as serve as a source of expertise for other prosecutors, including more than 260 Computer Hacking and Intellectual Property (CHIP) AUSAs and investigators across the country. CCIPS works closely with the investigative partners at the National Intellectual Property Rights Coordination Center (IPR Center) to coordinate among multiple jurisdictions in complex IP matters.

Like the Department as a whole, CCIPS has a range of law enforcement responsibilities, from prosecuting cybercrimes including network intrusions and ransomware, to acting as the Department's experts in the illegal use of cryptocurrency and developing issues at the intersection between digital evidence and criminal procedure. To meet these varying demands, the Department and CCIPS focus their finite resources on the categories of IP cases the Department has identified as having the highest priority, including:

- cases involving risks to public health and safety, such as those involving counterfeit pharmaceuticals, auto parts, or electrical components;
- large-scale commercial piracy and counterfeiting operations;
- IP crimes involving transnational organized criminal groups;
- IP crimes that involve a threat to critical infrastructure, national security, military operations, or the administration of government; and
- significant thefts of commercial trade secrets, particularly those with a foreign nexus.

CCIPS coordinates closely with the Counterintelligence and Export Control Section (CES) of the Department's National Security Division to evaluate potential criminal trade secret matters.

Examples of Significant Recent Complex Cases

i. Jetflicks

The Criminal Division, with assistance from the District of Nevada's U.S. Attorney's Office, is currently prosecuting the operators of one of the largest pirate TV and movie sites, known as Jetflicks, a subscription-based service that offered tens of thousands of movies and television episodes for unauthorized streaming or download. Eight defendants were charged in 2019. Two defendants, including Darryl Julius Polo, a programmer who left Jetflicks to start a competing pirate site called iStreamItAll in 2017, have pled guilty. Polo was sentenced to 57 months in prison and ordered to forfeit $1 million in criminal proceeds he obtained. As for the other six defendants, trial is currently scheduled for later this year. The charges and allegations contained in the indictment are merely accusations, and the defendants are presumed innocent until and unless proven guilty.

ii. Streit

The Criminal Division consulted with the Southern District of New York's U.S. Attorney's Office on the prosecution of Joshua Streit, who operated an illicit streaming site that offered live streams of major league sports programming without authorization, including content from Major League Baseball (MLB), the National Basketball Association, the National Football League, and the National Hockey League. Streit obtained the content mainly from legitimate sites operated or licensed by the sports leagues, using misappropriated credentials belonging to legitimate subscribers. Streit was charged with intrusion into MLB computers and attempting to extort approximately $150,000 from MLB in connection with that intrusion. Streit was initially charged with copyright infringement through streaming, computer intrusion, and extortion. He pleaded guilty to unauthorized access to obtain information from a protected computer, and in March 2023, he was sentenced to three years in prison, ordered to pay $3 million in restitution, and ordered to forfeit $500,000 in proceeds he obtained.

iii. Carrasquillo/Gears TV

The Criminal Division and the Eastern District of Pennsylvania's U.S. Attorney's Office prosecuted the operators of a large-scale pirated TV streaming site known as Gears TV (or Gears Reloaded). Gears TV offered real-time streaming of hundreds of cable and satellite TV channels and pay-per-view events, a "catch-up" feature that buffered the past 24 hours of content from many channels, as well as a library of downloadable movies. The operation brought in more than $35 million over the course of approximately 3 years. Three defendants pleaded guilty and were sentenced in early 2023. The court sentenced the leader, Omar Carrasquillo, to 66 months in prison ordered the forfeiture of $30 million of property traceable to his criminal offense, including real property, vehicles, and currency; and ordered him to pay $15 million in restitution.

iv. Fédération Internationale de Football Association (FIFA) Streaming

In December 2022, the District of Maryland's U.S. Attorney's Office and the Criminal Division, working with Homeland Security Investigations (HSI)-Baltimore and the IPR Center, disrupted more than 70 illicit streaming sites broadcasting World Cup soccer matches without authorization. Coordinating with representatives of FIFA and other rightsholders, investigators identified an initial group of 55 sites engaged in infringing streaming. The Department then sought and obtained seizure warrants for the sites' respective domains from the U.S. District Court for the District of Maryland and arranged for those seizures to be carried out by the relevant domain name registries or registrars that relied on U.S. technical infrastructure prior to the broadcast of the World Cup quarterfinal matches on December 10. A subsequent round of seizures of 23 domains was carried out several days later, on December 16, prior to the widely watched finals match. Several of the domains in the second round were identified through public discussions on social media, in which users of illicit streaming sites seized in the first round discussed other illicit streaming sites that were still operating. Although domain name seizures often result in only temporary disruption of infringing sites, in the wake of these high-profile seizures that were timed to disrupt illicit streaming access to a major sporting event, several illicit sports streaming sites announced they would stop providing infringing soccer content entirely.

v. Napolsky / Z-Library e-Book Piracy

The Criminal Division consulted with the Eastern District of New York's U.S. Attorney's Office on the prosecution of two Russian nationals who were charged with operating a site, Z-Library, which offered pirated e-books. Z-Library billed itself as "the world's largest library" and claimed to offer more than 11 million e-books for download. The site was operated on multiple domains, including z-lib.org, which were seized (along with approximately 200 mirror domains) contemporaneously with the defendants' arrest as they were transiting through Argentina in November 2022. A second round of seizures of other mirror domains was carried out in May 2023. The Department has sought extradition of both defendants from Argentina.

vi. Aksoy / Counterfeit Cisco

The Criminal Division and the District of New Jersey's U.S. Attorney's Office prosecuted Onur Aksoy, the CEO of a massive trademark counterfeiting operation, which trafficked in fraudulent and counterfeit Cisco networking equipment with an estimated retail value of hundreds of millions of dollars. Some of the counterfeit product ended up in critical supply chains, including hospitals, schools, government agencies, and the military. Aksoy pleaded guilty in June 2023, and was sentenced to 78 months' imprisonment on May 1, 2024.

vii. You (U.S. v. Xiaorong You)

The Criminal Division, the National Security Division, and the Eastern District of Tennessee's U.S. Attorney's Office prosecuted Xiaorong You, a Ph.D. chemist, who was convicted after a jury trial of conspiracy to commit trade secret theft, conspiracy to commit economic espionage, possession of stolen trade secrets, economic espionage, and wire fraud. The trade secrets, which were stolen from the Coca-Cola Company and Eastman Chemical (including trade secrets belonging to other major chemical and coating companies, such as Dow Chemical, BASF, and Sherwin Williams) and cost at least $119 billion to develop, related to formulations for BPA-free coatings for the inside of beverage cans. Evidence at trial showed that You and her co-conspirators stole these trade secrets to set up a new BPA-free coating manufacturer in China, for the benefit of You's company and the governments of China, Shandong province, and Weihai city, as well as the Chinese Communist Party, and received millions of dollars in grants from the Chinese government to do so. In May 2022, You was sentenced to 168 months in prison along with a $200,000 fine.

International Engagement

As these examples of criminal IP cases make clear, the internet and the globalization of trade make IP crime truly a global problem. To counter the problem of international IP crime, the Department focuses additional resources funded by the Department of State on international engagement, including developing relationships and engaging in cooperative enforcement efforts with foreign law enforcement agencies, supporting training, case-based mentoring and other capacity-building, where appropriate. Central to the Department's international efforts on IP enforcement is the International Computer Hacking and Intellectual Property (ICHIP) program, a network of federal prosecutors with expertise in IP crime and other high-tech legal issues stationed in U.S. missions in key regions around the world, and supported by U.S.-based legal experts specializing in internet fraud and public health, illicit markets, and cryptocurrency, as well as digital forensics experts in CCIPS's Cybercrime Lab.

In 2023, ICHIP attorneys delivered more than 50 skills development programs to international audiences on IP prosecution and investigation. In addition, ICHIPs provided numerous case-based mentoring efforts, working directly with foreign prosecutors and investigators to develop strategies to bring effective cases in the context of differing legal structures and technical capabilities.

Using All Available Tools to Counter IP (and Related) Crime

The Department places a high priority on criminal prosecution of IP crimes, but recognizes that piracy, counterfeiting, and trade secret theft are often connected with other forms of serious criminal activity, requiring a nimble, interdisciplinary approach. That approach is reflected in the organization of CCIPS, which combines in-house expertise on computer intrusions, network attacks, electronic evidence, cryptocurrency and other technology-focused legal issues, with expertise in intellectual property enforcement. This approach is also in the Department as a whole, using all available tools to combat criminal activity that involves IP, such as:

- Pursuing counterfeit pharmaceutical cases through both trademark counterfeiting authorities (*i.e.*, 18 U.S.C. § 2320) and, in cases involving harmful or deadly substances such as fentanyl, Title 21 statutes that can provide significantly higher penalties.

- Seeking to disrupt internet sites involved in IP crime, where such sites pose an immediate risk of economic or physical harm. This includes the Department's use of asset forfeiture authority against the domain names of sites used in the distribution of counterfeit or fraudulent pharmaceuticals, personal protective equipment (PPE), or other medical goods during the Covid-19 pandemic, and against sites engaged in for-profit illicit streaming of the FIFA World Cup and other major sporting events.

The Disruptive Technology Strike Force

While IP is a key driver of the U.S. economy across many sectors, some technologies protected by IP rights have national security implications that warrant extra attention. The Department, led by my colleagues in the National Security Division, takes a multi-pronged approach to identify and counter nation-state threats to U.S. IP and technology that affect U.S. security interests. The Criminal Division works with the National Security Division to advise on trade secret and economic espionage cases and prioritize those with an international or nation-state connection.

In February 2023, the Deputy Attorney General announced the creation of the "Disruptive Technology Strike Force" (Strike Force), a partnership between the Department and the Department of Commerce designed to enforce U.S. laws protecting U.S. advanced technologies from illegal acquisition and use by nation-state adversaries. Under the leadership of the Department's National Security Division and the Department of Commerce's Bureau of Industry and Security (BIS), the Strike Force brings together experts throughout government – including the Federal Bureau of Investigation (FBI), HSI, Defense Criminal Investigative Service (DCIS), and seventeen U.S. Attorney's Offices in metropolitan regions across the country – to target illicit actors, strengthen supply chains and protect critical technological assets from being acquired or used by nation-state adversaries. The Strike Force combats export control and sanctions violations, smuggling, and trade offenses related to the unlawful transfer of sensitive information, goods, and military-grade technology to nation-state adversaries.

Five recent Strike Force cases charged former employees of U.S. companies with stealing confidential and proprietary information related to sensitive technology and attempting to take such information to the People's Republic of China (PRC), and one case charged a defendant with seeking to obtain technology from U.S. manufacturers on behalf of Chinese end users.

In March 2024, PRC resident and Canadian national Klaus Pflugbeil was arrested and PRC-based Yilong Shao was indicted for allegedly conspiring to send to an undercover agent millions of dollars-worth of proprietary technology used in the manufacturing of electric car batteries. Both defendants are former employees of a Canadian manufacturer that used the proprietary technology in the battery-manufacturing process, but they now allegedly operate a PRC-based business and sought to use the trade secrets to advance their company.

In March 2024, California resident and PRC national Linwei Ding was arrested for allegedly stealing from Google more than 500 unique files containing confidential proprietary information relating to artificial intelligence technology. According to the indictment, Ding secretly affiliated himself with two PRC-based technology companies, including one that he founded and served as CEO for, while working as a software engineer for Google.

In February 2024, California resident Chenguang Gong was arrested for allegedly transferring more than 3,600 files containing proprietary information from his employer, including files with blueprints for sophisticated missile-detection technology. According to the complaint, Gong sought funding from the PRC-administered "Talent Programs," which recruit individuals overseas with expertise sought after by the PRC, to develop similar technology.

In May 2023, Liming Li of California was arrested for his alleged theft of sensitive technology related to advanced manufacturing software programs from his Southern-California-based employers and using that information to market his own competing company to businesses in China.

In May 2023, California man and former Apple employee Weibao Wang was charged in connection with a scheme to steal Apple source code and other proprietary information related to autonomous systems. Allegedly, he left Apple to work as an engineer for a U.S.-based subsidiary of a China-based company to work on the development of self-driving cars, and, following a search of his residence, Wang left the country for China.

The charges and allegations mentioned above are merely accusations. The defendants are presumed innocent until and unless proven guilty.

Litigation Challenges: Valuation in IP Cases

One significant challenge the Department has faced in obtaining deterrent sentences in IP cases – and one in which Congress may be able to help – is the issue of valuation or measuring the magnitude of an IP crime.

In federal criminal IP cases, sentences for trade secret offenses are driven largely by the "loss" amount, while piracy and counterfeiting sentences are driven by what the U.S. Sentencing Commission's Guidelines Manual (Guidelines) calls the "infringement amount." In the United States, many criminal trade secret thefts involve extremely valuable trade secret information and risk significant potential economic harm to the trade secret owner, but are interrupted before defendants can fully inflict such harm by exploiting a stolen trade secret. As a result, diligent victim response and effective law enforcement action may result in charged conduct involving substantial potential or intended harm, but minimal actual loss. Several recent court decisions call into question reliance on "intended loss" to determine sentences in trade secret theft cases, exacerbating the disparity and limiting the Department's ability to deter trade secret theft. The Department understands the U.S. Sentencing Commission to be working to address this specific issue, presenting for Congressional approval that alternative measures of the magnitude of harm, such as a defendant's intended loss or a defendant's gain, are appropriate considerations in determining the offense level for IP offenses.

Similarly, in illicit streaming piracy cases, the relevant provision of the existing Guidelines does not specifically address how courts should value individual pirated streams or performances for purpose of sentencing, and the U.S. Sentencing Commission has thus far been unwilling to amend this provision to address valuation in streaming cases. Congress may wish to consider whether additional guidance on streaming is necessary, and we of course would be happy to provide any assistance to Congressional or U.S. Sentencing Commission staff that might help resolve this challenge to adequately capture the seriousness of the offense and help deter illicit streaming piracy in the future.

Conclusion

The Department appreciates the opportunity to present information about the ongoing efforts to protect IP rights, both within the Department and in collaboration with the other agencies represented here today. I am happy to answer any questions you may have.