January
2016
Volume 64
Number 1

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

Monty Wilkinson
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Contractor
Becky Catoe-Aikey

Law Clerk
Mary C. Eldridge

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201.

Prosecuting Intellectual Property Crimes

In This Issue

Introduction

Sally Q. Yates
Deputy Attorney General
U.S. Department of Justice

It is my great pleasure to introduce this edition of the United States Attorneys' Bulletin devoted to Intellectual Property (IP). IP crime in the United States and abroad threatens not only our public safety and economic well-being, but also our national security. Counterfeit products, such as auto parts, pharmaceuticals, and military equipment can cause death and serious bodily injury. Theft of proprietary designs, technology, and innovations by competitors can wreak havoc on American industry, creating unfair market advantages, eroding profits, and causing loss of jobs. Economic espionage by state actors seeks to harm our national security through attacks on our infrastructure and businesses. Criminals increasingly use cyber means to carry out these offenses, attempting to become a faceless enemy committing crimes without attribution. We, as prosecutors, must vigorously defend against these types of crimes, and continue to utilize all available resources to do so.

As Deputy Attorney General, I serve as the Chair of the Department of Justice Task Force on IP, composed of senior representatives within the Department. Since its creation in 2010 by then-Attorney General Eric Holder, the Department's IP Task Force has confronted this threat with a strong and coordinated response. Its mission is to support prosecutions in priority areas, provide heightened civil enforcement, achieve greater coordination among federal, state, and local law enforcement partners, and increase focus on international enforcement efforts.

Specifically, the Department focuses its efforts to aggressively investigate and prosecute a wide range of IP crimes, with a particular emphasis on: (1) public health and safety, (2) theft of trade secrets and economic espionage, and (3) large-scale commercial counterfeiting and piracy. Today our enforcement efforts at the Department are more vigorous, more strategic, more collaborative, and more effective than ever before.

This edition of the United States Attorneys' Bulletin is the latest resource available to assist prosecutors in the fight against IP crimes. This issue provides topical guidance and information on IP, from investigation to sentencing. This Bulletin contains articles concerning: the IP Task Force and its function; guidance on prosecuting an IP case; copyright enforcement; the Department's strategy on countering economic espionage; the National IP Rights Center led by U.S. Immigration and Customs Enforcement's Homeland Security Investigations; the IP enforcement programs of the Office of Justice Programs; sentencing considerations; and articles providing case examples in the prosecution of counterfeit prescription drugs, counterfeit semiconductors, and online commercial counterfeiting operations.

I encourage each of you to work with your fellow prosecutors and law enforcement partners to participate in the Department's multi-faceted approach to combatting this type of crime. It is through your leadership and vigilance as prosecutors that we will continue to effectively stay ahead of the ever-adapting threat of IP crime.

Department of Justice Task Force on Intellectual Property: A Coordinated Response to Combat Intellectual Property Crime

Miriam H. Vogel
Associate Deputy Attorney General
United States Department of Justice

"[P]rotecting the nation's intellectual property is a vital part of the Justice Department's mission." *Remarks by Attorney General Loretta E. Lynch at MassChallenge Roundtable Discussion*, Oct. 2, 2015, *available at* http://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-announces-new-intellectual -property-enforcement-program.

I. Introduction

Why does the Department of Justice focus its leadership efforts and precious resources on intellectual property (IP) crime? The Department is keenly aware that IP crime is anything but victimless —it is a crime that threatens our nation's well-being, attacking our economy, public welfare, and national security.

We are fortunate to benefit from an economy that is thriving from brilliant innovations and breakthroughs in technology and health. Our innovations are also the envy of the world. Unfortunately, as our developments become more efficient and important, the motivation and means to enable IP crime continue to grow accordingly. With the spread of innovation comes the threat of increased harms to an increased number of people by counterfeit products that can cause serious bodily injury or even death. The criminals who carry out IP offenses increasingly use cyber means to steal more swiftly, effectively, and with less traceability. We, therefore, have had to become faster, smarter, and better coordinated to track them down.

The Department has responded to these threats with a strong and coordinated approach. Through the leadership and coordination of the Attorney General's IP Task Force, created 2010, the Department has remained coordinated in confronting the growing number of domestic and international IP crimes. Through its members, the Task Force works to identify and implement a multi-faceted strategy with our federal, state, and international partners to effectively combat this type of crime.

We appreciate this opportunity to ensure that the investigators and prosecutors who fight IP crime on the front lines are acquainted with the tools that are available through the Task Force writ large or through specific Task Force members.

II. Mission, priorities, and composition

The mission of the Department's IP Task Force is to support prosecutions in priority areas, provide heightened civil enforcement, achieve greater coordination among federal, state, and local law enforcement partners, and increase focus on international enforcement efforts.

Specifically, the IP Task Force supports the Department's efforts to aggressively investigate and prosecute a wide range of IP crimes, with a particular focus on: (1) public health and safety, (2) theft of trade secrets and economic espionage, and (3) large-scale commercial counterfeiting and piracy. The Department places a special emphasis on the investigation and prosecution of IP crimes that are committed or facilitated by cyber-enabled means or perpetrated by organized criminal networks. The IP Task Force also supports state and local law enforcement's efforts to address criminal intellectual property enforcement by providing grants and training.

IP Task Force members include the Assistant Attorney Generals (or equivalent) for the following components:

- Antitrust Division
- Civil Division
- Criminal Division
- Federal Bureau of Investigation
- National Security Division
- Office of Justice Programs
- Office of Legislative Affairs
- Office of Public Affairs
- United States Attorneys' offices/Executive Office for United States Attorneys

The IP Task Force also works closely with the Office of the Intellectual Property Enforcement Coordinator, housed in the White House Office of Management and Budget.

III. Members of the IP Task Force

The Department investigates and prosecutes a wide range of IP crimes. Primary investigative and prosecutorial responsibility within the Department rests with the FBI, the United States Attorneys' offices, the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), the National Security Division (NSD), and, with regard to offenses arising under the Food, Drug, and Cosmetic Act, the Consumer Protection Branch of the Civil Division. Each Task Force member plays an essential role in the coordinated effort to investigate, prosecute, and prevent IP crimes, as discussed in each brief summary below.

A. Antitrust Division

The mission of the Antitrust Division is to promote economic competition through enforcing and providing guidance on antitrust laws and principles. Consumers, and the economy as a whole, benefit from the competition and innovation that result from consistent application of sound antitrust principles to intellectual property rights. The Division accomplishes its mission by enforcing the Federal antitrust laws against illegal, collusive, or exclusionary conduct, while supporting the incentives to innovate created by intellectual property rights; promoting the procompetitive use of intellectual property rights through guidelines, appellate briefs, policy statements, reports, hearings, workshops, and speeches; and actively engaging with our foreign counterparts and multilateral organizations to promote application of competition laws to intellectual property rights that is based on analysis of competitive effects, not domestic or industrial policy goals.

More information about the Antitrust Division is *available at* http://www.justice.gov/atr.

B. Civil Division

The Civil Division serves a critical role in protecting and enforcing intellectual property rights and in protecting the public interest in the proper functioning of the intellectual property laws. In the intellectual property field, as elsewhere, the Division's principal function is to represent the United States, federal agencies, and federal officials in civil litigation, both as a party and amicus curiae. In conjunction with the Office of the Solicitor General, Civil Division plays a leading role in formulating and presenting the views of the United States on intellectual property matters in response to invitations from the Supreme Court, the Federal Circuit, and other courts. In addition, Civil Division attorneys participate in outreach and training programs to promote the protection of intellectual property rights and combat trade in counterfeit goods. The components of the Civil Division principally involved in intellectual property matters are the Consumer Protection Branch, the Intellectual Property Section of the Commercial Litigation Branch, and the Appellate Staff.

The Consumer Protection Branch leads the Justice Department's efforts to enforce consumer protection statutes throughout the United States. Its cases are rooted in our nation's fundamental consumer protection laws, establishing crucial precedents and protecting American consumers from threats to their health, safety, and wallet. The Consumer Protection Branch works closely with agencies such as the Food and Drug Administration, the Federal Trade Commission, the Consumer Product Safety Commission, the National Highway Traffic Safety Administration, and the Consumer Financial Protection Bureau.

The Intellectual Property Section of the Commercial Litigation Branch represents the United States in matters where a patent, copyright, trademark, or trade secret is at issue. Many of the cases the Section handles involve complex technologies, such as pharmaceutical compositions and highly sophisticated electronic devices. In order to meet the challenges presented by these cases, all attorneys assigned to the Section have a degree in one of the physical sciences or in an engineering field, and are eligible for admission to practice before the United States Patent and Trademark Office in patent matters.

The Appellate Staff represents the United States, its agencies, and officers in civil cases in the federal courts of appeals. The Appellate Staff handles appeals involving all of the subject-matter areas litigated by the Civil Division, including intellectual property matters, and practices in all 13 of the federal courts of appeals, as well as in the United States Supreme Court. The Appellate Staff's portfolio includes many of the most difficult and controversial civil cases in which the Federal Government is involved.

More information about the Civil Division is *available at* http://www.justice.gov/civil; the IP Section of the Commercial Litigation Branch at http://www.justice.gov/civil/intellectual-property-section; the Consumer Protection Branch at http://www.justice.gov/civil/consumer-protection-branch; and the Appellate Staff at http://www.justice.gov/civil/appellate-staff.

C. Criminal Division

The Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) pursues three overarching goals: to deter and disrupt computer and IP crime, to guide the proper collection of electronic evidence by investigators and prosecutors, and to provide technical and legal advice and assistance on these issues to agents and prosecutors in the United States and around the world. CCIPS accomplishes its mission by pursuing and coordinating investigations and prosecutions, and helping others to do so; by engaging in activities that build the international legal and operational environment that allows for successful investigations and prosecutions; by providing expert legal and technical advice and support to the Department, investigative agencies, and other executive branch agencies; and by

developing and advocating for policies and legislation relating to computer crime, IP crime, and collection of electronic evidence. CCIPS's work often entails close coordination on national security, intelligence, and international issues.

More information about CCIPS is *available at* www.cybercrime.gov.

D. Federal Bureau of Investigation

Preventing intellectual property theft is a priority of the FBI's criminal investigative program. The FBI specifically focuses on the theft of IP products that can impact consumers' health and safety, such as counterfeit aircraft, car, and electronic parts. Their recent investigative successes are due to linking the considerable resources and efforts of the private sector with law enforcement partners on local, state, federal, and international levels.

Given the level of IP protection priority and an interest in maximizing the use of resources, the FBI has recently announced a new collaborative strategy. This new strategy builds upon the work previously done by the Department, while also working with industry partners to make enforcement efforts more effective. As part of this strategy, the FBI will partner with third-party marketplaces to ensure they have the right analytical tools and techniques to combat intellectual property concerns on their Web sites. The FBI also will serve as a bridge between brand owners and third-party marketplaces in an effort to mitigate instances of the manufacture, distribution, advertising, and sale of counterfeit products. This new strategy will help law enforcement and companies better identify, prioritize, and disrupt the manufacturing, distribution, advertising, and sale of counterfeit products. High level, more complex crimes can then be investigated by the FBI and other partner law enforcement agencies of the National Intellectual Property Rights Coordination Center. *See* Department of Justice Press Release, *Justice Department Announces New Strategy to Combat Intellectual Property Crimes and $3.2 Million in Grant Funding to State and Local Law Enforcement Agencies* (Oct. 2, 2015), *available at* http://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-announces-new-intellectual-property-enforcement-program.

More information about the FBI's investigation of intellectual property rights is *available at* https://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr. For more information regarding the National Intellectual Property Rights Coordination Center, please see the article in this issue entitled "IPR Center: Conducting Effective IP Enforcement."

E. National Security Division

The NSD's mission is to carry out the Department's highest priority: to combat terrorism and other threats to national security. With respect to intellectual property, NSD's Counterintelligence and Export Control Section works with the FBI, DHS, and U.S. Attorney's offices across the country to investigate, prosecute, and otherwise disrupt economic espionage and export control offenses. Additionally, the Office of Intelligence provides legal support to the FBI and other members of the Intelligence Community in conducting surveillance under the Foreign Intelligence Surveillance Act, and, in particular, investigations involving the theft of intellectual property with national security dimensions. As a reflection of NSD's prioritization of national security threats involving malicious cyber activity, in 2012 NSD and CCIPS jointly stood up the National Security Cyber Specialists Network, composed of prosecutors in every U.S. Attorney's office and attorneys at Main Justice. This is a resource for training and coordination on computer hacking offenses with national security implications, many of which involve the theft of trade secrets and sensitive military technology.

More information about the National Security Division is *available at* http://www.justice.gov/nsd, as well as the article entitled "DOJ's Strategic Plan for Countering the Economic Espionage Threat" included in this issue.

F. United States Attorneys' offices

The United States Attorneys serve as the nation's principal litigators under the direction of the Attorney General. Through the Cyber and Intellectual Property subcommittee of the Attorney General's Advisory Committee, designated U.S. Attorneys advise the Attorney General about policies and issues relating to intellectual property enforcement. The subcommittee is led by its chairperson, U.S. Attorney David Hickton of the Western District of Pennsylvania, and its vice-chair, U.S. Attorney Rod Rosenstein of the District of Maryland.

In each United States Attorney's office, one or more Assistant United States Attorneys (AUSAs) has received specialized training in the enforcement of intellectual property laws through the Computer Hacking and Intellectual Property (CHIP) program. CHIP attorneys have four major areas of responsibility including: (1) prosecuting computer crime and IP offenses, (2) serving as the district's legal counsel on matters relating to those offenses and the collection of electronic evidence, (3) training prosecutors and law enforcement personnel in the region, and (4) conducting public and industry outreach and awareness activities. These CHIP attorneys and other AUSAs work closely with special agents from the FBI, Immigration and Customs Enforcement, and other federal law enforcement agencies to investigate and prosecute violations of federal copyright, trademark, and trade secrets laws.

More information about United States Attorney's offices is *available at* http://www.justice.gov/usao. Please visit http://www.justice.gov/usam/usam-9-50000-chip-guidance for more information about the CHIP program.

G. Office of Justice Programs

Housed in the Department's Office of Justice Programs, the Bureau of Justice Assistance (BJA) provides leadership and assistance to state and local partners, including the Intellectual Property Theft Enforcement Program (IPEP), in coordination with the Department of Justice's Computer Crime and Intellectual Property Section and Task Force on Intellectual Property. The IPEP was initiated at the direction of the Attorney General in FY 2009, and consists of three major components: law enforcement efforts at the state and local level, a national training and technical assistance program, and a public education campaign. Since that time, BJA has awarded over $19 million in funding to support our partners in their fight against IP crime, including grants and training and technical assistance, over $14 million of which was in awards to local law enforcement agencies.

More information about the Office of Justice Programs is *available at* http://ojp.gov/, as well as the article entitled "Intellectual Property Enforcement Programs: Helping State and Local Law Enforcement Combat Intellectual Property Crime" included in this issue.

IV. Conclusion

Drawing on the strengths of each of its members and each of its partners in both government and private industry, the Department's enforcement efforts against IP crime are more strategic, collaborative, and impactful than ever before. The Task Force will continue to support the Department's coordinated approach to effectively combatting IP crime in the United States and abroad— working to identify and evolve the Department's response as criminals continue to advance their schemes.

For more information about the IP Task Force, updates on IP enforcement, and additional resources, please visit http://www.justice.gov/iptf. ❖

ABOUT THE AUTHOR

❑**Miriam H. Vogel** is Associate Deputy Attorney General. In addition to serving as the staff lead on the Department's Intellectual Property Task Force, she works with several components on behalf of the Deputy Attorney General, including Antitrust and the Community Relations Service. Prior to coming to the Department of Justice, she served as an in-house attorney and in private practice, with a focus on intellectual property law. ✠

Deciding When to Prosecute an Intellectual Property Case

Christopher S. Merriam
Deputy Chief for Intellectual Property
Computer Crime and Intellectual Property Section
U.S. Department of Justice

Kendra R. Ervin
Assistant Deputy Chief for Intellectual Property
Computer Crime and Intellectual Property Section
U.S. Department of Justice

I. Introduction

Federal prosecutors know that deciding whether to prosecute a particular case requires the exercise of judgment and discretion, which can take years of experience and many cases to develop. Although intellectual property (IP) crimes are not charged as regularly as many other types of federal offenses, the prosecution of IP cases can have a significant effect in protecting the public and limiting economic harm to victims, while at the same time creating a substantial deterrent to similar conduct by others. How should you decide whether a particular case of trafficking in counterfeit computer chips, copying and distribution of pirated music or software over the Internet, or the theft of trade secrets should be charged, even where a victim or investigator provides evidence to prove all the elements? What special considerations may come into play in a given case? Federal prosecutors may need to recalibrate the usual standards for case consideration when evaluating the merits of an IP case based on a few characteristics of such cases, including:

- IP crime always has a direct victim (the holder of the IP rights infringed), but it also undermines the IP system as a whole, may involve fraud perpetrated on the recipient of the counterfeit good or pirated work, and will often involve related offenses ranging from smuggling and money laundering to computer intrusions and the distribution of malware.
- Although the majority of IP infringement may be addressed through civil action by the rights holder, there are many instances where civil remedies are not effective because of the difficulty in identifying a party through civil process, infringers doing business overseas, or in cases where repeat infringers ignore or avoid civil judgments.
- Effective enforcement of IP laws is essential to the foundation of the modern economy in both protecting consumers and encouraging innovation.

- The protection of IP rights in cases involving the public health and safety, large scale commercial piracy and counterfeiting, and the theft of trade secrets are DOJ priority prosecution areas identified by the Deputy Attorney General through the IP Task Force.

The Computer Crime and Intellectual Property Section's *Prosecuting Intellectual Property Crimes* manual serves as a valuable resource for evaluating these, as well as the other issues, that arise in IP cases. *See* Department of Justice, Computer Crime and Intellectual Property Section, *Prosecuting Intellectual Property Crimes* (2013). In general, with respect to IP crimes, federal prosecutors should take into account the same considerations as they would with any federal crime. *See, e.g., U.S. Attorneys' Manual* § 9-27.220. While individual U.S. Attorney's offices may evaluate these factors using different standards, the discussion below attempts to tailor these factors to issues likely to surface in criminal IP matters.

II. The federal interest in prosecution of IP crimes

In determining the scope of the federal interest that would be served by a prosecution of a particular IP case, the attorney for the government needs to weigh several relevant considerations, including:

> (1) [current] Federal law enforcement priorities; (2) The nature and seriousness of the offense; (3) The deterrent effect of prosecution; (4) The person's culpability in connection with the offense; (5) The person's history with respect to criminal activity; (6) The person's willingness to cooperate in the investigation or prosecution of others; and (7) The probable sentence or other consequences if the person is convicted.

Id. § 9-27.230. This article discusses each of these factors below with detailed attention to IP crimes. The last factor—the probable sentence—warrants particular attention in light of several amendments over the past decade to sentencing guideline § 2B5.3 to more accurately reflect the loss caused by IP crime.

A. The federal focus on IP crime

Recognition of the importance of IP to the national economy, and the growing scale of IP theft, led the Department of Justice to designate IP crime as a "priority" for federal law enforcement as early as 1999. In 2010, Attorney General Holder instituted the current version of the Department's Intellectual Property Task Force to emphasize the importance of intellectual property in a wide range of DOJ responsibilities. The work and priorities of the IP Task Force are spelled out in greater detail in a separate article in this issue, but it is worth emphasizing the particular focus on the identified prosecution priorities: (1) Health and Safety of the American Public, (2) Theft of Trade Secrets and Economic Espionage, and (3) Large-Scale Commercial Counterfeiting and Piracy Operations. To support investigations and prosecutions in this area, the Department has more than 260 Computer Hacking and Intellectual Property (CHIP) attorneys across the country who receive special training to address both IP and cyber-crimes, and 16 attorneys in the Criminal Division's Computer Crime and Intellectual Property Section specializing entirely on IP crime. Both the FBI and ICE/HSI have agents specifically assigned to handle IP cases, and a total of 23 domestic and international law enforcement agencies coordinate on IP cases through the National Intellectual Property Rights Coordination Center, while the Department's Bureau of Justice Assistance provides grants and training to support IP investigations and prosecutions by state and local authorities.

B. The nature and seriousness of the offense

Just as with other criminal offenses, the nature and seriousness of IP crimes varies, and the consideration of the specific facts and circumstances surrounding each case is critical. Limited federal resources should not be diverted to prosecute inconsequential cases or cases in which the violation is only

technical. *U.S. Attorneys' Manual* § 9-27.230. Prosecutors may consider any number of factors to determine the seriousness of an IP crime, including:

1. Whether the counterfeit goods or services endanger the public's health or safety (*e.g.*, counterfeit drugs or automotive parts)
2. The nature of the trade secret information (*e.g.* critical technologies with military or other sensitive applications)
3. The scope of the infringing or counterfeiting activities (*e.g.*, whether the subject infringes or traffics in multiple items or infringes upon multiple industries or victims), as well as the volume of infringing items manufactured or distributed
4. The scale of the infringing or counterfeiting activities (*e.g.*, the amount of illegitimate revenue and any identifiable illegitimate profit arising from the infringing or counterfeiting activities)
5. The number of participants and the involvement of any organized criminal group
6. The scale of the victim's loss or potential loss, including the value of the infringed item or trade secret information, the impact of the infringement or trade secret theft on the market for the infringed item, and the damage to the rights holder's or trade secret owner's business
7. Whether the victim or victims took reasonable measures (if any) to protect against the crime
8. Whether the purchasers of the infringing items were victims of a fraudulent scheme, or whether there is a reasonable likelihood of consumer mistake as a result of the subject's actions

C. The deterrent effect of prosecution

Deterrence of criminal conduct is one of the primary goals of the criminal justice system. Experience demonstrates that many infringers will not be deterred by civil liability, which they can treat as a cost of doing business. For example, even when the rights holder has obtained a permanent injunction or consent decree, that civil remedy may not necessarily deter some defendants. A defendant may respond to such civil remedies by altering the item upon which they are infringing, such as counterfeiting automotive parts bearing marks of one automotive manufacturer after being the subject of an injunction obtained by another automotive manufacturer. Another defendant may shut down his operations only to quickly reopen under a different corporate identity.

Criminal prosecution may more effectively deter a violator from repeating his or her crime. Criminal prosecution of IP crimes is also important for general deterrence. Many individuals may commit intellectual property crimes not only because they can be relatively easy to commit with technological advances and more sophisticated methods of manufacturing and distribution, but also because the subjects believe they will not be prosecuted. Criminal prosecution plays an important role in shaping public perceptions of right and wrong. The resulting public awareness of effective prosecutions can have a substantial deterrence effect. Even relatively small scale violations, if permitted to take place openly and frequently, can lead members of the public to believe that such illicit conduct is tolerated in American society. While some cases of counterfeiting or piracy may not result in provable direct loss to the rights holder, the widespread commission of IP crimes with impunity can be devastating to the value of such rights.

D. The individual's culpability in connection with the offense

Multiple individuals working in concert, such as a company that traffics in counterfeit goods or pirated software, often commit IP crimes. *See Prosecuting Intellectual Property Crimes* § XI.E (2013) (discussing special considerations for cases involving corporations). The individuals in such an organization are not necessarily equally culpable. For example, a prosecutor may reasonably conclude that some course other than prosecution would be appropriate for a relatively minor participant. In considering the relative culpability of specific individuals within a larger organization, a number of non-exclusive factors have proven helpful, including: (1) whether the person had oversight responsibility for others, (2) whether the person specifically directed others to commit the offense, (3) whether the person profited from the offense, (4) whether the person was specifically aware of the wrongful nature of the activity, as evidenced by the receipt of a warning such as a "cease and desist" letter from the rights holder or a seizure notice letter from Customs and Border Protection (CBP), or by a statement to collaborators admitting wrongfulness, but nonetheless continued to engage in the activity, and (5) whether the person took affirmative steps, such as creating misleading records or destroying evidence, to deter investigation, and thereby facilitate commission of the offense.

E. The individual's history with respect to criminal activity

The subject's history with respect to criminal activity will, of course, be extremely fact dependent. Defendants may have a history of engaging in a pattern of fraudulent conduct not necessarily limited to IP crimes. It should not be assumed that commission of an IP crime is an exception to an otherwise law-abiding life. The repeat-offender provisions in the intellectual property crime statutes, *e.g.* 18 U.S.C. § 2320(b)(1)(B), and the United States Sentencing Guidelines, try to ensure that repeat offenders receive stiffer sentences.

In addition to the defendant's criminal history, it is appropriate to consider his or her history of civil IP violations. Sources for determining the defendant's history of civil IP offenses include civil litigation records, the victim's legal department and private investigators, and any state consumer protection agencies to which consumers might have complained.

F. The individual's willingness to cooperate in the investigation or prosecution of others

A defendant's willingness to cooperate will depend on the individual. Nevertheless, it is important to recognize that in IP cases, defendants often have a substantial capacity for cooperation, if they are, in fact, willing. Since IP crimes often require special materials, equipment, or information, and can involve multiple participants across the supply chain, defendants often can provide substantial assistance. A defendant might provide valuable information concerning a domestic or foreign source of counterfeit goods or pirated works. For instance, if a defendant is investigated for selling counterfeit health care products on a retail basis, he could provide information as to the wholesaler of those counterfeit products. The wholesaler, in turn, could provide information regarding the manufacturer, or about other retailers.

G. The probable sentence or other consequences upon conviction

The consequences that may be imposed if an IP prosecution is successful include imprisonment, restitution, and forfeiture. In *Prosecuting Intellectual Property Crimes*, the sentencing provisions are discussed at § VIII.B-C, whereas restitution (which is generally mandatory in IP cases) is discussed at § VIII.D, and forfeiture (which is generally available in IP cases) is discussed at § VIII.E. The probable sentence is worthy of attention in light of revisions over the past decade to sentencing guidelines § 2B1.1 for Economic Espionage Act (EEA) cases and § 2B5.3 for all other IP offenses.

Completed EEA cases are sentenced under § 2B1.1, with a base offense level of 6. The value of the stolen trade secret information largely drives the defendant's sentence as the offense level increases according to the amount of loss under § 2B1.1(b)(1). Section 2B1.1, Application Notes, outlines a number of general methods for calculating loss, and the *Prosecuting Intellectual Property Crimes* Manual § VIII.C.2 provides further explanation regarding factors to consider for loss calculations in trade secret cases, as well as case law describing potential ways to value trade secrets.

Additionally, as of November 1, 2013, the offense level is increased two points if the defendant knew or intended that the trade secret would be transported or transmitted out of the United States, *see* U.S.S.G. § 2B1.1(b)(12)(A) (2015), and four points if the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent, with a minimum offense level of 14. *See id.* § 2B1.1(b)(12)(B). Other enhancements that often arise in EEA cases include the two-level "sophisticated means" enhancement under § 2B1.1(b)(10(C) and the two-level adjustment for abuse of a position of trust or use of a special skill under § 3B1.3.

For all other IP offenses, § 2B5.3 governs the sentencing calculations. Since 2000, there have been five rounds of amendments to this guideline. Several of these amendments are highlighted below, and the *Prosecuting Intellectual Property Crimes* Manual § VIII.C.1 discusses each in more detail, and provides an overview of the guideline calculations for IP offenses governed by § 2B5.3, including commonly sought enhancement and departure considerations.

- In 2000, the base offense level was increased from 6 to 8, and, in addition to the infringement amount, the number and type of special offense characteristics were increased to include characteristics for manufacturing, uploading, or importing infringing items; for infringement not committed for commercial advantage or private financial gain; and for risk of serious bodily injury or possession of a dangerous weapon in connection with the offense. *See* U.S.S.G. App. C (Amendments 590, 593).
- In 2005 on a temporary basis, and in 2006 as permanent, a new specific offense characteristic addressing infringement of pre-release works was added. *See* U.S.S.G. App. C (Amendments 675, 687).
- In 2006 on a temporary basis, and in 2007 as permanent, § 2B5.3 was amended to specify that in cases under 18 U.S.C. § 2318 or § 2320 involving counterfeit labels, the infringement amount is based on the retail value of the infringed items to which the labels would have been affixed. *See* U.S.S.G. App. C (Amendments 682, 704).
- Most recently, as of the November 1, 2013, if the offense involved a counterfeit drug or counterfeit military goods and services under certain conditions, the offense level is increased by 2. *See* U.S.S.G. App. C (Amendment 773). The amendment also specified a minimum offense level of 14 for offenses involving counterfeit military goods and services. *See id.*

III. Whether the person is subject to prosecution in another jurisdiction

The *U.S. Attorneys' Manual* § 9-27.220 also notes that a prosecutor may properly decline to take action despite having sufficient admissible evidence when the person is subject to effective prosecution in another jurisdiction. In IP cases, as in other cases, "[a]lthough there may be instances in which a Federal prosecutor may wish to consider deferring to prosecution in another Federal district, in most instances the choice will probably be between Federal prosecution and prosecution by state or local authorities." *U.S. Attorneys' Manual* § 9-27.240 (cmt). To make this determination, prosecutors should weigh all relevant considerations, including: (1) the strength of the other jurisdiction's interest in prosecution, (2) [t]he other jurisdiction's ability and willingness to prosecute effectively, and (3) [t]he probable sentence or other consequences if the person is convicted in the other jurisdiction. *Id.* § 9-27.240.

Unlike in many other types of criminal offenses, a prosecutor in an IP case arguably may not be able to defer to a prosecution in the location of the primary victim. For example, a multinational corporation headquartered in one state may be the victim of trade secret theft without any nexus between the misappropriation and the district in which the victim company is based. Because of the defendant's constitutional and statutory right to be tried in the state and district in which the crime was "committed," U.S. Const. art. III § 2 cl. 3; U.S. Const. amend. 6; 18 U.S.C. § 3237, a prosecutor based in the home state of the victim arguably may not have proper venue over the defendant unless he or she can show that the "locus delecti" of the counterfeiting took place in that district. This determination must be made "from the nature of the crime alleged and the location of the act or acts constituting it." *United States v. Rodriguez-Moreno,* 526 U.S. 275, 280 (1999).

Thus, in IP cases, a federal prosecutor often will be called upon to vindicate the rights of a victim IP holder based in another district, another state, or even another country, because the defendant may not be subject to prosecution in the victim's district, state, or nation. Federal prosecutors should also recognize that local or state authorities may not have a great interest in punishing violations of the rights of out-of-state victim IP holders. By contrast, ensuring uniform and reliable national enforcement of the IP laws is an important goal of federal law enforcement.

This goal takes on added significance for federal prosecutors when the victim is based in a foreign country because of the importance of IP in modern international trade. With consistent enforcement of IP rights, the United States will continue to set an example of vigorous IP rights enforcement and to be perceived as hospitable to foreign firms that would register their IP and engage in business here.

Local and state authorities may also believe that since many IP rights are conferred by the federal government, they do not have the ability to prosecute any IP crimes. Federal IP laws, however, generally do not preempt state and local IP laws. There is a provision for federal preemption for copyright infringement, 17 U.S.C. § 301, although this preemption permits prosecution for other kinds of crime, and some states have passed laws that indirectly criminalize conduct involving certain pirated works. Moreover, even if the local or state authorities express a strong interest in prosecution, they may not have the ability or willingness to prosecute the case effectively due to competing priorities and limited resources. Consequently, a prosecutor should evaluate for each individual case whether state or local law enforcement exists as a viable alternative to federal prosecution.

IV. The adequacy of a noncriminal alternative in an IP case

Prosecutors may consider the adequacy of noncriminal alternatives when addressing an IP case. Some civil remedies, including ex parte seizure of a defendant's infringing products and punitive damages, may be available for certain violations of copyright and trademark rights. 15 U.S.C. § 1116(d) (2015) (trademark remedies); 17 U.S.C. §§ 502-505 (2015) (copyright remedies). Also, for importers of trademark-infringing merchandise, CBP may assess civil penalties not greater than the value that the merchandise would have were it genuine, according to the manufacturer's suggested retail price for first offenders, and not greater than twice that value for repeat offenders. These civil fines may be imposed in CBP's discretion, in addition to any other civil or criminal penalty or other remedy authorized by law. 19 U.S.C. § 1526(f) (2015). The availability and adequacy of these remedies should be carefully considered when evaluating an IP case.

Yet civil remedies may be futile under some circumstances. For example, IP crimes are unusual because they often are committed without the victim company's knowledge. The victim usually has no

direct relationship with the infringer—before, during, or after the commission of the crime. If a victim remains unaware of a violation by a particular defendant, civil remedies generally will be unavailing. Furthermore, without criminal sanction, infringers or counterfeiters might treat the rare case of the victim's civil enforcement of its rights as a cost of doing business.

Another important factor to consider when contemplating civil remedies is that infringers may be judgment proof. In most cases, the infringer traffics in counterfeit items worth far less than the authentic ones, and with the increasing prevalence of online sales of counterfeit and pirated goods, the infringer only needs limited resources to operate his or her business.

There are a number of other circumstances where existing civil remedies may simply be an insufficient deterrent. For example, there may be cases where there have been prior unsuccessful efforts by a victim to enforce IP rights against the defendant or the existence of circumstances preventing such efforts. Criminal charges may be necessary if counterfeiting, piracy, or theft of trade secrets continues despite the entry of a permanent injunction or consent decree in a civil case.

V. Conclusion

Because defendants in IP cases can have several victims, including the IP holders or trade secret owners, society at large, and the recipients of the infringing goods or works, and because reliable enforcement of federally created IP rights is so important to the growing information economy, federal prosecutors should carefully consider opportunities to prosecute IP cases. Prosecutors should be aware of the special characteristics of IP cases when evaluating them against traditional principles and exercising their prosecutorial discretion. Further guidance is available from the *Prosecuting Intellectual Property Crimes* Manual (2013), or from the IP Team at the Computer Crime and Intellectual Property Section (CCIPS) at (202) 514-1026. ❖

ABOUT THE AUTHORS

❑ **Christopher S. Merriam** is the Deputy Chief for Intellectual Property with the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. Mr. Merriam leads a group of 15 attorneys dedicated to intellectual property prosecutions and related issues. During his time at CCIPS, Mr. Merriam has prosecuted cases of copyright and trade secret theft, and acted as the national contact for trade secret theft cases arising under the Economic Espionage Act of 1996. He has also worked directly with law enforcement colleagues in more than 20 nations to help improve criminal enforcement of intellectual property laws.

Before joining the Justice Department in 2001, Mr. Merriam was a criminal defense lawyer with the firm of Rochon & Roberts in Washington, DC. Mr. Merriam was an E. Barrett Prettyman Fellow at the Georgetown University Law Center Criminal Justice Clinic, where he taught criminal law and practice. ✠

❑ **Kendra R. Ervin** is the Assistant Deputy Chief for Intellectual Property with the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. Ms. Ervin assists Deputy Chief Christopher Merriam in leading a group of 15 attorneys dedicated to IP prosecutions and related issues. In her five years with CCIPS, Ms. Ervin has prosecuted large-scale, multi-jurisdictional IP crimes, participated in domestic and international IP enforcement training and outreach, and helped to develop and draft legislative and policy initiatives addressing all facets of IP crime.

Prior to joining CCIPS, Ms. Ervin was employed as an associate at the law firm of Williams & Connolly, where she specialized in patent litigation. Ms. Ervin also served as a law clerk on the United States Court of Appeals for the Federal Circuit. ✠

This article updates an earlier article written by David Goldstone for the March 2001 issue of the United States Attorneys' Bulletin.

Loss Amount in Trade Secret Cases

William P. Campos
Assistant United States Attorney
Intellectual Property Crimes Coordinator
Eastern District of New York

I. Introduction

Intellectual property plays an important role in the United States economy. President Obama noted that "[o]ur single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century." *See* http://www.whitehouse.gov/the-press-office/remarks-president-exportimport-banks-annual-conference . Likewise, President Clinton noted that "[t]rade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation's national security and economic well-being." *See* Presidential Statement on Signing the Economic Espionage Act of 1996, 2 Pub. Papers 1814-15, 1996 WL 584924 (Oct. 11, 1996).

Economic espionage is a significant threat to American businesses, particularly as the United States moves to a high-technology economy. The theft of sensitive business information is not only damaging to businesses, but is also difficult to detect when done by company insiders.

Congress responded to the adverse impact that trade secret theft has on the U.S. economy in enacting the Economic Espionage Act of 1996 (EEA): "The development and production of proprietary economic information is an integral part of U.S. business and is thus essential to preserving the competitiveness of the U.S. economy." S. Hrg. 104-499, at 2, 1996 WL 90824 (Feb. 28, 1996) (opening statement of Sen. Arlen Specter). "A piece of information can be as valuable to a business as in fact a factory is. The theft of that information could do more harm than if an arsonist torched that factory." *Id*. at 3, 1996 WL 90789 (Feb. 28, 1996) (opening statement of Sen. Herb Kohl).

In considering whether to enact the EEA, Congress found that "[o]nly by adopting a national scheme to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge and thus safeguard our national security." S. Rep. 104-359, 11-12, 1996 WL 497065 (July 30, 1996); *see also* H.R. Rep. 104-788, reprinted in 1996 U.S.C.C.A.N. 4021, 4025 (Sept. 16, 1996) (finding that a "comprehensive federal criminal statute" "will serve as a powerful deterrent to this type of crime" and would "better facilitate the investigation and prosecution of [trade secret theft]").

II. The Guidelines

The EEA, codified at Title 18, United States Code sections 1831 to 1839, provides for the criminal prosecution of trade secret theft and misappropriation. An important factor in determining a criminal defendant's appropriate sentencing range under the U.S. Sentencing Guidelines (U.S.S.G. and the Guidelines) is the calculation of the "loss amount" pursuant to Section 2B1.1 of the Guidelines. This

article is intended to address the methods that have been, or could be, used in calculating the loss amount in trade secret cases.

Generally, the applicable loss amount to be applied to the §2B1.1 table is the greater of the actual or intended loss to the victim. *See* U.S.S.G. § 2B1.1, app. n.3(A) (2015). Under the Guidelines, actual loss is measured as "the reasonably foreseeable pecuniary harm that resulted from the offense," and intended loss is measured as the "pecuniary harm that was intended to result from the offense and includes intended pecuniary harm that would have been impossible or unlikely to occur (e.g., as in a government sting operation, or an insurance fraud in which the claim exceeded the insured value)." *Id*. cmt. n.3(A)(i-ii). The Guidelines also provide a non-exhaustive list of factors that can be used to estimate the loss amount. *See Id.* cmt. n.3(A)(i-ii); *United States v. Ferguson*, 584 F. Supp. 2d 447, 451 (D. Conn. 2008) (describing the §2B1.1 cmt. 3(C) factors as "a non-exhaustive list of factors a court might consider in estimating the loss.").

For example, if property is taken, copied, or destroyed, the measure of loss may be the fair market value of the property, or the court may consider using the cost to the victim of replacing that property if the fair market value is impracticable to determine or inadequately measures the harm. *See* U.S.S.G. § 2B1.1, cmt. n.3(C)(i) (2015). But, regardless of which method is chosen to calculate loss, the Government's calculation need not be absolutely certain or precise. "The court need only make a reasonable estimate of the loss." *See id.* § 2B1.1 cmt. n. 3(C).

Many thefts of trade secrets cases, however, involve no loss of tangible property or even actual loss, depending on how quickly the offender was apprehended by law enforcement agents. In November 2009, therefore, the Guidelines were amended to include Application Note 3(C)(ii), which sets forth that "[i]n the case of proprietary information (e.g., trade secrets), the cost of developing that information or the reduction in the value of that information that resulted from the offense" is to be considered in estimating the loss amount. The amendment made explicit what several courts had already done, namely, to consider the research and development costs as an alternative measure of the loss amount in a trade secret case. *See* e.g. *United States v. Ameri*, 412 F.3d 893, 900 (8th Cir. 2005); *See also United States v. Four Pillars Enterprise Company*, 253 F. App'x 502, 512 (6th Cir. 2007) (unpublished opinion); *United States v. Wilson*, 900 F.2d 1350, 1355-56 (9th Cir. 1990). The legislative history of the EEA also touches on the significance of the research and development costs associated with trade secrets:

> As this Nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow. . . . This material is a prime target for theft precisely because it costs so much to develop independently, because it is so valuable.

S. Rep. No. 359, 104th Cong., 2d Sess. (1996).

In trade secret cases, however, there is oftentimes no actual market for the information that was stolen—it had been kept secret. In those cases, as stated in U.S.S.G 3. § 2B1.1, cmt. n.(C)(ii), the loss amount may be the cost of developing the stolen information or the reduction in value of that information that resulted from the offense. Regardless of which method is chosen to calculate loss, the Government's calculation need only be a "reasonable estimate of the loss," as required by § 2B1.1 cmt. n.3(C).

III. Preparing for sentencing

In preparing to determine the appropriate loss amount in a trade secret theft sentencing, there first must be a determination as to whether a loss amount can be reasonably calculated. Among the factors to consider is whether the defendant was paid for the item or information stolen. The amount paid may be an appropriate measure of the market value of the trade secret and, hence, the loss amount. If the defendant did not actually sell the information before the arrest, then one should determine whether he tried to sell it. Again, the amount of the proposed sale may be an appropriate measure of the market price, and the loss

amount. In any event, the item or information stolen may have taken years to develop, and one should also try to determine the research and development costs incurred by the victim. While the research and development costs may not be the best or sole component of the estimate of Guidelines loss, it may be the easiest to obtain and explain.

Explaining the Guidelines loss to the court could be challenging. Oftentimes the defendant is unable to sell the information or otherwise cause his plan to reach fruition. In those cases, the defendant will argue that the loss amount is zero. The victims of the theft correctly point out that the stolen information could have caused a catastrophic loss to the company. Given these competing views, which often amounts to a binary decision matrix (i.e., the loss is zero or 100 percent), it is important to consider the individual court's views and to maintain one's credibility with the court. Consequently, to the extent possible, one should provide the court with multiple loss calculation methodologies, which likely result in different loss amounts. If the court has a range of options, it is less likely to assign a value of zero simply because it rejects one of them.

IV. Examples of loss amount calculations

A good example of providing a court with several loss calculation methodologies is *United States v. Sergey Aleynikov*, No. 10 CR 96, 2011 WL 1002237 (S.D.N.Y. Mar. 11, 2011). Aleynikov, a former computer programmer at Goldman Sachs & Co., was convicted of trade secret theft and Interstate Transportation of Stolen Property, for stealing Goldman Sachs's proprietary computer code to benefit his new employer. The Government first argued that the stolen computer code had a fair market value despite not being for sale or available to the public, in much the same way a house has a fair market value despite the owner's refusal to sell it. Other commercially available computer programs performed tasks similar to those performed by the stolen programs and could serve as a useful measure of the loss. After all, the theft provided the defendant with a free version of software he would otherwise have had to pay millions to purchase from third parties. Next, the Government argued that, assuming a fair market value was impracticable to determine, the cost to the victim of replacing the code should be used. Finally, the Government argued that the cost of developing the code, as contemplated in §2B1.1 cmt. 3(C)(ii), should be used, which would be at least in the range of $7 million to $20 million. This was accepted by the court. The Government provided thoughtful methodologies to support each of the suggested sentencing options. It should be noted, however, that this case was later reversed by the Second Circuit on grounds of statutory construction. *See* 676 F.3d 71 (2d Cir. 2012).

Likewise, in *United States v. Samarth Agrawal*, 726 F.3d 235 (2d. Cir. 2013), the Government provided alternate loss methodologies to the court. Agrawal, a former trader at Societe Generale, was convicted of trade secret theft and Interstate Transportation of Stolen Property. The jury found that he stole proprietary computer code used for the firm's high frequency securities trading business. Agrawal printed the code onto thousands of sheets of paper, which he then physically removed from the bank's New York office to his New Jersey home. There, he could use them to replicate Societe Generale's trading systems for a competitor who promised to pay him hundreds of thousands of dollars.

Testimony at Agrawal's trial suggested that the company benefiting from the theft expected that the stolen strategy would help the company realize a profit of between $10 million and $40 million. Indeed, Societe Generale had generated profits of $10 million per year for three years using the proprietary code. At sentencing, the defendant argued there was no actual loss and no intended loss. The Government agreed that there had been no actual loss. Ultimately, however, the Government's successful argument for a loss amount of between $7 million and $20 million was based, in part, on the fact that the cost in developing the stolen programs was approximately $9.9 million. Agrawal was sentenced to 36 months' incarceration.

In *United States v. Hanjuan Jin*, 833 F.Supp.2d 977 (N.D. Ill. 2012), *affirmed*, 733F.3d 718 (7th Cir. 2013), the defendant was charged with economic espionage and theft of trade secrets pursuant to 18 U.S.C. §§1831 and 1832, respectively. The defendant, a software engineer at Motorola, stole the iDen proprietary telecommunications technology. She planned to leave the United States and work in China. A November 2011 bench trial resulted in her conviction of theft of trade secrets, but acquittal of economic espionage. The judge imposed a 48-month prison sentence. Both her conviction and 48-month sentence were affirmed.

At sentencing, the Government explained that Motorola's 2011 iDen-related revenues were $365 million. The Government also provided the sentencing judge a loss amount calculation based on the research and development costs associated with some of the stolen information. Based on the research and development costs of between $20 million and $50 million, the Guidelines range was 121-151 months. Ultimately, despite the high Guidelines range, the court sentenced the defendant to 48 months' incarceration because of her significant health issues.

In *United States v. Walter Liew*, 11 CR 573 (N.D.CA Dec. 9, 2013) (unpublished opinion), *Liew* and his co-conspirators were convicted by a jury of economic espionage, among other crimes. *Liew* stole trade secrets from the DuPont Company, consisting of the processes to manufacture titanium dioxide (TiO2), and sold them to a Chinese company. *Liew* obtained $28 million from the Chinese company.

At sentencing, the Government noted the difficulty in accurately determining loss where the stolen information represented "decades of research and design at DuPont." Govt. Sentencing Memo at 6. Indeed, one DuPont employee who testified at trial stated that, during his tenure at the company, approximately $150 million was spent annually to improve the TiO2 facilities. *See Id.* at 7. The Government rested on the certainty of the $28 million that Liew obtained.

The court sentenced *Liew* on the Trade secret counts to 120 months' imprisonment. His 180 month sentence also included his convictions on a witness tampering charge and false statements charges relating to a bankruptcy proceeding and income tax returns.

V. Conclusion

The Economic Espionage Act is intended to protect innovation and creativity, which is essential to our economic well-being and our national security. Trade secret theft prosecutions, therefore, are a significant tool for ensuring that protection. The high-flying rhetoric of the EEA, however, can meet an unsightly demise without a defensible nuts-and-bolts calculation of an appropriate loss amount, which is the single most important feature in determining the defendant's sentencing guidelines. ❖

❑ **William P. Campos** is an Assistant United States Attorney in the Eastern District of New York, where he serves as the Coordinator for Intellectual Property Crimes. Before joining the United States Attorneys' Office, Eastern District of New York, in June 2007, Mr. Campos was an Assistant District Attorney with the Manhattan District Attorney's Office, as well as a litigation associate at Sedgwick LLP. ✠

Prosecuting Copyright Infringement Cases and Emerging Issues

Jason Gull
Senior Counsel
Computer Crime and Intellectual Property Section
U.S. Department of Justice

Tim Flowers
Trial Attorney
Computer Crime and Intellectual Property Section
U.S. Department of Justice

I. Introduction

Over the past century, various new technologies have emerged that have posed significant challenges to copyright enforcement. From the player piano to radio, the photocopier to the cassette tape, new technologies for using, copying, and disseminating creative works have provided great opportunities for copyright owners and their audiences, but also have often strained existing copyright laws, in many cases undermining the ability of authors to realize the benefits of copyright in their works. These disruptive technologies have frequently led to legal changes designed to preserve copyright law's incentive structure and ensure that copyrights can be effectively enforced. Perhaps no technology has expanded opportunities for creating and distributing creative works more than the Internet. Certainly none has posed more significant challenges to copyright enforcement. From pirate FTP sites that offer free downloads of software, to peer-to-peer file sharing, new Internet phenomena have often left copyright law, and law enforcement, struggling to keep pace.

Ten to fifteen years ago—that is, in the ancient past by Internet standards—movies, music, and other media content available on the Internet was usually distributed in the form of files that could be downloaded. Although smaller, embedded video and audio files were certainly not unheard of, in general, for larger media files like complete movies or songs, users needed to download an entire file (and even wait until the download was complete) before a media file could be listened to or watched. For a large movie file being downloaded on a typical home Internet connection in the early 2000s, this could take not just hours, but several days. However, once downloaded, a permanent copy of the media file resides on the user's computer, and generally can be replayed or further distributed to others (although some distributors of Internet media content have employed digital rights management systems that can limit playback to specific devices, time periods, etc.).

II. Streaming

Internet streaming is a prime example of the type of Internet technology that is both incredibly useful and, at the same time, poses significant challenges to effective criminal enforcement. Streaming services offer movies, music, and other media content to users in real time, allowing them to click a button on a browser window or mobile device app and start watching or listening to movies or music almost immediately. Unlike downloading a digital media file, streaming does not require a user to wait until an entire file download is complete before content can be seen or heard. For users, streaming can offer greater flexibility; instead of having to download and store a complete library of works, users can

stream media from the "cloud" to multiple devices and locations wherever they have an Internet connection. For media providers, streaming offers the potential benefit of greater control over media files and a more persistent connection with users, providing more opportunities for advertising.

The growth of streaming media use has been staggering. YouTube, perhaps the best-known streaming video site today, was founded only a decade ago. Netflix's streaming video service is even younger and, on an average evening, Netflix alone now accounts for more than a third of total Internet traffic in the United States. According to broadband networking firm, Sandvine, in autumn 2015, Netflix accounted for 36.5 percent of North American downstream Internet traffic during peak evening hours. Sandvine Global Internet Phenomena Report, Dec. 2015, *available at* https://www.sandvine.com/trends/global-internet-phenomena/. Altogether, streaming services like Netflix and YouTube, along with many other smaller players like Hulu, HBO Go, Pandora, and Spotify, now account for more than two thirds of total North American Internet traffic during peak times, up from about one third of traffic just five years ago.

In the past decade, as high-speed broadband Internet service has become increasingly common, copyright pirates have gotten into the streaming game, too, with illicit sites offering access to streams of thousands of movies, television shows, and music files, often for free. MegaVideo, NinjaVideo, and TVShack are some of the better known sites involved in streaming against which the Department of Justice has taken action in recent years, but many pirate streaming sites continue to operate, and new ones are being created all the time.

Compared to the old "download" model, streaming is resource-intensive, requiring not only significant storage space for media files, but also massive amounts of bandwidth to ensure that media can be streamed to many users simultaneously, without latency or delays that result in poor video or sound quality and a bad user experience. Streaming sites can be expensive to run, so many are supported by subscription fees or "donations." However, streaming offers the same advantages to copyright pirates that it does to legitimate media sites, including a persistent connection with users as they watch or listen to media files. This allows streaming site operators to insert their own advertising, either during pauses in video or audio content or displayed around a video frame on screen. According to the 2012 indictment against the operators of Megaupload, that organization and its associated streaming sites brought in more than $25 million in advertising revenue. *See United States v. Kim Dotcom et al.*, No. 1:12CR3 (E.D. Va., filed Jan. 5, 2012), *at* paragraph 18.

Many illicit streaming sites are also engaged in a more insidious form of "advertising"—the delivery of malware to users' devices. According to research commissioned by the Digital Citizens Alliance, nearly a third of the illicit streaming sites researchers examined exposed visitors to some form of malware, ranging from invasive adware to remote-access Trojans, and operators of pirate streaming sites can earn significant amounts of revenue from malware networks that will pay sites operators for every site visitor they can infect. Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data, Digital Citizens Alliance, (Dec. 2015) *available at* http://www.digitalcitizensalliance.org/cac/ alliance/ content. aspx? page=digitalbait.

If the growth in legitimate streaming services is impressive, the growth in illicit streaming sites serving up pirated content is alarming. Between 2010 and 2012, the amount of bandwidth devoted to infringing video streaming was estimated to have grown by more than 470 percent, or more than two and a half times the growth in legitimate streaming over the same period. David Price, Sizing the Piracy Universe, NetNames, (Sept. 2013) *available at* http://www.netnames.com//sites/default/files/netnames-sizing_piracy_universe-FULLreport-sept2013.pdf. And that growth occurred despite the Department's takedown of the widely-used streaming provider, MegaVideo, and its associated site, Megaupload.com. There is reason to believe that infringing streaming has continued to increase in bandwidth and frequency since then.

III. Criminal copyright enforcement

Over the past 25 years, criminal copyright enforcement online has concentrated mainly on sites engaged in making and distributing pirated copies of works, whether those works consist of computer software, videogames, movies, music, or books. But illicit streaming services challenge law enforcement's ability to pursue infringement criminally. The Copyright Act grants the authors of creative works a set of exclusive rights, including the rights to reproduce copies of the work, to distribute copies of the work to the public, to prepare derivative works based on the copyrighted work, and (with respect to certain classes of works) to perform or display the work publically. The list of exclusive rights protected by copyright are enumerated in 17 U.S.C. § 106. Criminal law currently provides felony penalties for willful infringements of only two of these rights: an infringement involving violation of either the reproduction or distribution rights can be punished as a felony, so long as the infringement is above a certain threshold level (a total of 10 or more copies, with a total retail value of $2500, within a specific 180-day period), or involves online distribution of a work being prepared for commercial distribution (such as a movie that has not yet been released publicly in theaters).

Streaming does not fit neatly within the "reproduction" or "distribution" framework. Streamed content is transmitted and watched or listened to more or less in real time, as the content is being streamed. Generally speaking, streaming does not leave the user with a copy of content that can be replayed or redistributed later. The nature of digital audio and video is such that any time an audio or video file is "played," the file must be copied bit-by-bit from one part of a device to another, stored temporarily in a buffer, or sent from one device to another. It is not well-settled whether this type of copying and sending necessarily constitutes "reproduction" or "distribution" of the copyrighted work for purposes of copyright law. For further discussion of the copyright interests implicated by streaming, *see, Promoting Investment and Protecting Commerce Online: The ART Act, the NET Act and Illegal Streaming*, Statement of Maria A. Pallante, Register of Copyrights, before the House Judiciary Subcommittee on Intellectual Property, Competition, and the Internet, 112th Congress, 1st Session, (June 1, 2011), *available at* http://copyright.gov/regstat/regstat060111.html. Rather, streaming more clearly implicates a different exclusive right under copyright: the right to perform a work publicly. Unlike infringements of the reproduction or distribution rights, infringements of the public performance right are not subject to felony criminal penalties. Willful infringements involving public performance may be prosecuted criminally, but are only subject to misdemeanor penalties, and only if the offense is committed for purposes of commercial advantage or private financial gain. By contrast, criminal infringements of the reproduction or distribution right can be punished as felonies even in the absence of commercial or financial purpose (although the offense is subject to higher penalties if such a purpose can be shown).

This gap between the penalties for infringing reproduction and distribution on the one hand, and streaming on the other, is significant. A digital pirate who operated an illegal site that made available dozens of pirated movies that were downloaded hundreds of times could be subject to felony penalties of up to 3 years imprisonment (or 5 years if done for financial gain), whereas an operator of an illicit streaming Web site who streamed those same movies to thousands of users, collecting thousands of dollars in advertising or subscription revenue, could face only a maximum punishment of one year in prison. Given the pervasiveness of streamed content, those penalties seem unlikely to provide an effective deterrent to would-be digital pirates.

Efforts to close this gap in the law have failed to gain traction. In 2011, Congress considered two bills codifying felony streaming penalties—the House's controversial Stop Online Piracy Act (SOPA) and the Senate's Commercial Felony Streaming Act. Both bills were met with considerable resistance. SOPA was withdrawn in early 2012 after widespread controversy (including concerns voiced by the White House) about the potential effects the bill's site-blocking proposals could have for Internet governance and for free expression. Some representatives of private sector media and technology companies engaged in streaming services or technologies of their own, and who were involved in

licensing disputes and civil litigation with copyright owners, also voiced concerns about the bills. Although these companies were generally supportive of greater penalties for pirate streaming sites in principle, they expressed concern that the proposed felony provisions might somehow be read to cover the companies' own conduct in the future, leading to a chilling effect on their companies' development of new services and on contract negotiations. Media coverage became increasingly negative.

Even celebrities like Justin Bieber contributed to the bills' demise. His public reaction to the Commercial Felony Streaming Act, which occurred during a Minnesota radio interview, was a watershed moment for the proposed legislation. *See* http://talkingpointsmemo.com/dc/does-the-commercial-felony-streaming-act-threaten-internet-freedom. After a radio host insinuated that Bieber, who had first been "discovered" after posting videos of himself singing popular songs on YouTube, could have been prosecuted under the proposed legislation, Bieber angrily responded that the bill's sponsor, Senator Amy Klobuchar, "needs to be locked up, put away in cuffs." Although Bieber's comment was based (perhaps not surprisingly) on a less-than-complete understanding of the proposed law, and it is unlikely that Sen. Klobuchar's bill could have been applied to the kind of amateur uploading that catapulted Bieber to fame, his off-the-cuff comment encapsulated real public concern about potential overbreadth. Since 2012, many in both the public and private sector have expressed support for strengthening criminal penalties for infringing streaming, including the Department of Justice, as well as the White House's Office of the Intellectual Property Enforcement Coordinator. The Register of Copyrights has also noted the lack of adequate deterrence provided by existing law. Although no new legislative proposals to address streaming penalties have advanced in Congress this term, given the growing popularity and importance of both legitimate and illicit streaming, it seems likely that a new legislative fix will be reintroduced sometime in the future.

Even if existing criminal copyright law might not adequately address illicit streaming, prosecutors are nevertheless not powerless to address the issue. There are at least a few avenues for pursuing criminal cases against pirate streaming sites. Prosecutors may be able to bring felony copyright charges against streaming sites based on the infringing distribution the sites may commit alongside infringing streaming, or based on infringements committed in the process of assembling the streaming site itself. There may also be alternative felony charges based on related criminal conduct.

Particularly because streaming is resource-intensive, operators of illicit streaming sites often rely on multiple sources of revenue. Some offer downloads of copies as a "premium" feature available only to those willing to pay a subscription fee or "donation." If so, those downloads may serve as the basis for a felony copyright charge.

Where a streaming service hosts its own pirated content, the process of creating the site itself may involve sufficient levels of infringing copying to exceed the copyright felony threshold. Illicit streaming sites often offer thousands of pirated movie and music files. Even based on a conservative estimate of the value of each pirated file on the site's server, *e.g.* $20 per movie file, or $1 per music track, the number and value of infringing files that were copied to the site in the first place may be sufficient to exceed the felony threshold of 10 copies and $2500 under 17 U.S.C. § 506 and 18 U.S.C. § 2319, providing the copies were made within a specific 180-day period, and the server (or a mirror of it) is located within the United States.

As noted above, recent research indicates that a substantial number of illicit streaming sites may be supporting themselves not only by pushing advertising to their users, but also by pushing malicious software onto their users' computers and mobile devices as well. Even if felony copyright penalties are not available, where an illicit streaming site is being used to distribute malware, other felony charges, such as the Computer Fraud and Abuse Act (18 U.S.C. § 1030), may be warranted. Even if no felony charges may be available against an illicit streaming site, prosecutors should keep in mind that misdemeanor penalties may still be possible. Unlike felony copyright charges, a misdemeanor charge requires proof of a commercial purpose or private financial gain, but given the resources required to operate a streaming site, most streaming sites will have some identifiable profit motive or source of

revenue, and often multiple sources. While misdemeanor penalties may not be ideal, they are not necessarily toothless, either. Although each misdemeanor charge carries a maximum penalty of one year imprisonment, depending on the facts of a particular case, it may be possible to charge multiple misdemeanor counts.

IV. Conclusion

The first step to addressing a problem is recognizing its existence. Legislators, prosecutors, and stakeholders all recognize that existing criminal copyright provisions are inadequate to address the increasing problem of infringing streaming. Although legislative solutions have thus far proven elusive, there is momentum behind fixing the shortfalls in the existing criminal copyright law. Doing so would greatly enhance the Department's ability to engage in effective criminal enforcement against infringing Internet streaming. Until then, prosecutors still have some tools at their disposal to pursue illicit streaming sites. Given the continuing rapid growth in illegal Internet streaming services, they should have no shortage of potential targets as well. ❖

ABOUT THE AUTHORS

❑ **Jason Gull** is a Senior Counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice. At CCIPS, in addition to prosecuting criminal copyright, trademark, trade secret, and other intellectual property cases, he advises federal prosecutors and investigators on intellectual property, computer crime, and electronic evidence issues. Mr. Gull is active in policy matters, including coordinating with other U.S. Government components on the development and implementation of legislation, regulations, and international agreements related to intellectual property and cybercrime. He has represented the United States in several international fora, including the Council of Europe and the World Intellectual Property Organization, and has conducted training on IP and cybercrime enforcement in Europe, Asia, and Latin America. Prior to joining CCIPS in 2001, Mr. Gull was a litigator for private law firms in Chicago and San Francisco, where he was involved in intellectual property, securities, insurance coverage, unfair business practices, and white collar criminal cases. ✠

Tim Flowers is a Trial Attorney in the Computer Crime and Intellectual Property Section of the United States Department of Justice. Although Mr. Flowers's practice is heavily focused on litigating cases across the spectrum of computer-based and intellectual-property crimes, he has also conducted various outreach activities as part of CCIPS' Cybersecurity Unit. Mr. Flowers recently co-authored, along with colleague Brian Levine, "*Your Secrets Are Safe With Us: How Prosecutors Protect Trade Secrets During Investigation and Prosecution,*" which appeared in the AMERICAN JOURNAL OF TRIAL ADVOCACY. Before joining CCIPS, Mr. Flowers was a judicial law clerk to the Honorable Samuel H. "Hardy" Mays, Jr. on the United States District Court for the Western District of Tennessee and the Honorable Ronald Lee Gilman on the United States Court of Appeals for the Sixth Circuit. ✠

DOJ's Strategic Plan for Countering the Economic Espionage Threat

Richard S. Scott
Deputy Chief
Counterintelligence and Export Control Section
National Security Division

Alan Z. Rozenshtein
Attorney Advisor
Office of Law and Policy
National Security Division

The theft of trade secrets by foreign actors is an increasing threat to United States national and economic security. In June 2015, the National Security Division (NSD) of the United States Department of Justice (DOJ) released its "Strategic Plan for Countering the Economic Espionage Threat." All proceeding quotes will be from this plan, unless otherwise noted. This article provides a summary of the strategic plan and how NSD is implementing it in conjunction with United States Attorneys' offices (USAOs) across the country.

I. Disrupting economic espionage through an "all tools" and "whole of government" approach

To respond effectively to economic espionage, DOJ must support a whole-of-government approach, just as it does with other national security threats. Although NSD will, when possible, seek criminal prosecutions to disrupt economic espionage activities and hold criminal actors accountable, non-criminal tools must also be used where effective and appropriate. NSD will focus on the following six areas to counter the economic espionage threat.

A. Advancing domestic criminal investigation and prosecution

In investigating economic espionage, NSD will explore all potential criminal violations implicated by the offense conduct. The key statute is the Economic Espionage Act (EEA), which includes both 18 U.S.C. § 1832, the general statute criminalizing the theft of trade secrets for the benefit of someone other than the owner, *see* Mark L. Krotoski's article, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, from the November 2009 *Bulletin*, and 18 U.S.C. § 1831, which prohibits the knowing theft of trade secrets where the culpable individual or organization "intend[s] or know[s] that the offense will benefit any foreign government, foreign instrumentality, or foreign agent." The nexus to a foreign power carries heightened penalties, as compared to trade secret theft under § 1832. Under § 1831, individuals are subject to 15 years' imprisonment and a maximum fine of $5 million, while organizations are subject to a fine of $10 million or three times the value of the stolen trade secret, whichever is greater. 18 U.S.C. § 1831(a), (b) (2015).

Effective use of the EEA may include "charging individual foreign defendants even if they are located in countries where they believe they are beyond the reach of justice; charging foreign-based enterprises notwithstanding challenges regarding service of process; [and] charging the knowing beneficiaries of trade secrets stolen by state actors." NSD will also encourage and support the use of a

broad range of statutes, including computer fraud and abuse, tax fraud, bankruptcy fraud, wire fraud, obstruction of justice, and export control violations, along with asset forfeiture and other civil remedies.

NSD's commitment to the criminal prosecution of economic espionage is exemplified by the government's recent success in *United States v. Liew*, 2014 WL 2586329 (N.D. Cal. June 9, 2014), the first ever jury conviction under § 1831. After an eight-week trial in 2014, the jury found that Liew, his company, USA Performance Technology, Inc., and Robert Maegerle, a former employee of E.I. du Pont de Nemours & Company (DuPont), conspired to steal trade secrets from DuPont regarding its chloride-route titanium dioxide production technology. Titanium dioxide is a commercially valuable white pigment with numerous uses, including coloring paint, plastics, and paper. The global titanium dioxide market has been valued at roughly $12 billion, and DuPont has the largest share of that market. Liew and his co-conspirators were found to have sold the trade secrets for large sums of money to state-owned companies of the People's Republic of China. The purpose of their conspiracy was to help those companies develop large-scale chloride-route titanium dioxide production capabilities in China, including a planned 100,000-ton titanium dioxide factory in Chongqing. In July 2014, Liew was sentenced to serve 15 years in prison, forfeit $27.8 million in illegal profits, and pay more than $500,000 in restitution.

B. Promoting foreign criminal enforcement

Economic espionage is inherently transnational, and cooperation with foreign partners is, therefore, an important tool. The promotion of foreign criminal enforcement includes interdiction of international transfers of proprietary information, information sharing (whether though mutual legal assistance treaties or law enforcement-to-law enforcement channels), and international prosecutions of economic espionage.

C. Using civil, regulatory, and other options

Non-prosecution alternatives can also help neutralize the economic espionage threat, and NSD will both encourage prosecutors to consider their use and will support any such efforts. Alternatives include the April 1, 2015 Executive Order to "designate foreign companies and foreign actors involved in cyber intrusions that resulted in the theft of trade secrets, as well as designations under the Commerce Department's Entity List for individuals and entities involved in economic espionage." *See* Exec. Order No. 1369480 FR 18077 2015 WL 1461837(Pres. Apr. 1, 2015). To enhance DOJ's effective use of these tools, NSD will work to improve communication and collaboration with the Treasury Department, the Commerce Department, and other relevant agencies and regulatory bodies.

D. Enhancing focus on beneficiaries of economic espionage

Foreign companies and individuals knowingly benefiting from the theft of U.S. intellectual property will be considered "as potential criminal defendants, as designees for sanctions under executive orders, or as candidates for addition to the Department of Commerce's Entity List." Even if criminal charges are not brought against the full range of actors involved, "a thorough analysis of the culpable foreign actors will improve understanding of the specific incident, advance an assessment of the economic espionage threat, and inform consideration of appropriate non-criminal countermeasures." In addition to the important and well-established role that computer forensics play in investigations, NSD will increase the usage of forensic accounting specialists to enhance and improve the Government's ability to identify both the perpetrators and the beneficiaries of the theft.

E. Increasing interaction with the intelligence community

Coordination with the U.S. Intelligence Community (USIC)—especially the National Security Agency and the Central Intelligence Agency—is critical to satisfy discovery obligations (e.g., in the

context of prudential search reviews), advance investigations, and otherwise disrupt the economic espionage threat through the "all tools" approach. NSD will strive to increase such coordination.

F. Recognizing successful use of non-prosecution tools

Because non-prosecution tools have historically received inadequate recognition, the "benefits of devoting substantial prosecutorial and investigative resources to pursue non-criminal means to disrupt a threat" have been underappreciated. In conjunction with the Executive Office for U.S. Attorneys, NSD is working to create new administrative mechanisms to recognize non-prosecution successes.

II. Heightening threat awareness and delivering coordinated training

NSD will take a number of steps to heighten awareness of the economic espionage threat and deliver coordinated training.

First, NSD will "promote sustained threat awareness among U.S. Attorneys' Offices." NSD will encourage and facilitate briefings from the FBI and the USIC for USAOs on economic espionage threats in their districts. The briefings will "focus on industries and other institutions targeted by foreign adversaries, as well as on specific actors and foreign instrumentalities known to engage in theft of intellectual property." The purpose of these briefings is to: (1) raise awareness among USAOs of economic espionage and specific threat trends, (2) assist DOJ and law enforcement in selecting private outreach targets, (3) provide a mechanism for sharing experiences and best practices, and (4) foster close relationships between prosecutors, agents, and intelligence analysts.

Second, NSD will "elevate threat awareness among targets of economic espionage." Because "[e]conomic espionage is perpetrated predominately against private sector victims," "private companies must be at the forefront of effort to combat this threat." In particular, "deterrence must begin with targeted outreach to U.S. companies and other institutions to enhance their understanding of the nature and severity of the threat, devise appropriate countermeasures, and mitigate losses of intellectual property" against both cyber- and insider-enabled economic espionage in a manner that both advances the government's goals and protects the victim from further negative consequences.

USAOs will be at the forefront of this outreach. USAOs should "establish new relationships with potential victims within their districts and . . . take advantage of existing outreach systems in place at local FBI field offices." USAO and FBI representatives should "make joint visits to companies so they can answer questions from both corporate security and in-house corporate counsel," and include, as appropriate, "specific threat information approved for dissemination to cleared officials to enable companies to device appropriate countermeasures." "NSD will periodically survey National Security/Anti-Terrorism Advisory Council (NS/ATAC) Coordinators and National Security Cyber Specialist (NSCS) representatives to assess their understanding of the economic espionage threat in their districts and to obtain their evaluation regarding the status and quality of ongoing local outreach initiatives."

NSD will also highlight the espionage threat to labs and universities, including through a working group focused on protecting Department of Energy laboratories and federally funded research universities.

Third, NSD will "deliver coordinated training" on the economic espionage threat. NSD will introduce a comprehensive training plan on economic espionage, which will "cover the intersection of economic espionage and cyber-related issues, as well as a discussion of the all-tools approach." Training venues will include both large, national conferences, like the NSCS Training and the NS/ATAC Coordinator Conference, as well as smaller events like the annual Introduction to National Security Investigations and Prosecutions Seminar and the biannual Theft of Trade Secrets/Economic Espionage Seminar, both held at the National Advocacy Center. NSD's Director of Training and Workforce

Development will work with NSD's Counterintelligence and Export Control Section to develop training materials on economic espionage—including best-practices checklists and FAQs—and distribute them through the NSCS and NS/ATAC Coordinator networks. NSD will also encourage increased coordination between DOJ and FBI on economic espionage-related training.

III. Providing technical advice and expertise

NSD will explore new tools and authorities to fight economic espionage. It will examine "potential gaps in existing statutory authorities and, as necessary, draft and propose new legislation related to economic espionage." NSD will provide technical advice to congressional committees and review proposed legislation and recommend legislative improvements. NSD will also continue to track and provide advice and comments on potential changes to the Federal Rules of Criminal Procedure—as it did recently relating to service of process on overseas entities—and the United States Sentencing Guidelines—as it has done with respect to sentencing enhancement for trade secrets transported outside the United States and trade secrets benefiting foreign actors.

NSD will also continue to provide technical advice and assistance to foreign partners as they develop their own economic espionage legislation.

IV. Conclusion

USAOs, in conjunction with investigators and analysts in the FBI, are at the front lines of the fight against economic espionage, and will need to use and support all appropriate tools and resources across the Federal Government. NSD is available to provide coordination, guidance, and assistance. USAOs should feel free to contact Richard Scott, Deputy Chief of the Counterintelligence and Export Control Section, on all matters related to economic espionage, and Christine Kringer, Director of NSD's Protection of National Assets Outreach Program, regarding outreach efforts. Richard can be reached at 202-233-2263 and at richard.s.scott@usdoj.gov, and Christine can be reached at 202-305-4656 and at christine.kringer@usdoj.gov. ❖

ABOUT THE AUTHORS

❑ **Richard S. Scott** is a Deputy Chief in the Counterintelligence and Export Control Section in the National Security Division. Prior to joining the Department in 2008, he was a law clerk for Judge Michael M. Baylson in the Eastern District of Pennsylvania and an associate at the law firm of Williams & Connolly LLP in Washington, D.C. ✠

❑ **Alan Z. Rozenshtein** is an Attorney Advisor in the Office of Law and Policy in the National Security Division. After clerking for Judge J. Harvie Wilkinson III on the U.S. Court of Appeals for the Fourth Circuit, he joined the Department of Justice through the Attorney General's Honors Program. ✠

IPR Center: Conducting Effective IP Enforcement

Bruce M. Foucart
Director
National Intellectual Property Rights Coordination Center

I. Introduction

The negative impacts of intellectual property (IP) theft are not immediately apparent, but they are significant: the crime can wreak havoc on the U.S. economy, threaten the health and safety of American consumers, and fund greater forms of violent and illegal activities. In response to these dangerous effects, and to improve collaboration among federal agencies involved in the fight against intellectual property rights (IPR) violations, the government created the National Intellectual Property Rights Coordination Center (IPR Center) in 2000. The IPR Center is a joint task-force organization led by U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), made up of 21 partner agencies, consisting of 17 federal agencies and 4 international agencies, including Interpol, Europol, and law-enforcement authorities from the governments of Mexico and Canada, with an officer from U.S. Customs and Border Protection (CBP) holding a deputy director position. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/ipr-center-fact-sheet/view. The task-force structure enables the IPR Center to effectively leverage the resources, skills, and authorities of each partner agency and provide a comprehensive response to traditional customs fraud and the trafficking of various types of contraband.

The overall defined mission of the IPR Center is to stand at the forefront of the Government's response to global intellectual property theft, enforce international trade laws, and ensure national security by protecting the public's health and safety and the U.S. economy by combating predatory and unfair trade practices that threaten the global economy. We accomplish that mission through a multi-layered approach that includes investigations to identify and dismantle criminal organizations, interdiction through targeting and inspections to keep illegal goods out of the U.S. supply chain, and outreach and training with domestic and international law enforcement organizations to strengthen capabilities worldwide. This strategic approach allows the Government to immediately assign resources to prevent tragic accidents related to the proliferation of counterfeit pharmaceuticals, investigate counterfeiting linked to violent organized criminal groups, and protect an industry workforce responsible for developing cutting-edge technology.

II. Organization structure

A. The Intellectual Property Unit

The Intellectual Property Unit (IPU), comprised of special agents, intelligence research specialists, and management and program analysts, recognize the threat of piracy. The IPU provides the coordination needed to facilitate successful investigations into the criminal organizations involved in piracy. This unit also coordinates enforcement operations relative to international and domestic threats identified in the intellectual property environment.

The IPU is comprised of two sections: IP Crimes and Intellectual Property Rights Intelligence.

IP Crimes Section: This section oversees all national programs and operations related to intellectual property, manages ongoing national IP initiatives, and tracks and reports all investigations related to intellectual property. Most IPU operations and initiatives include participation from multiple IPR Center partners. The programs cover a variety of areas, from products affecting health and safety to securing online commerce. The IP Crimes Section manages several national IP enforcement initiatives.

Intellectual Property Rights Intelligence Section (IPRIS): This section coordinates directly with the 23 IPR Center partners to compile information into a workable format and strategically share that information in such a way as to create the strongest impact. The section receives leads from multiple sources and conducts deconfliction with the partner agencies. It also provides leads to HSI field offices to facilitate their investigations and works closely with the private industry to identify viable targets for both criminal and civil actions. IPRIS intelligence analysts collect, analyze, and share timely and accurate intelligence information for the use of IPR Center partners. This includes the use of government databases, intelligence production and analysis tools, and open source information in the generation of targets leads for referral to IPR Center partner agencies. IPRIS further supports field office investigations with subject matter expertise in IPR trends, developments, and challenges. IPRIS examines reports of IP theft made through the IPR Center "IPR Button," which is currently utilized by approximately 200 Web sites. The IPR Button provides a mechanism for both the public and the industry to report suspected IPR violations. Since its inception in 2012, the IPR Button has generated over 20,000 submissions. These submissions are vetted and processed by IPRIS for dissemination to respective agency partners for potential investigative actions.

The IPR Center has partnered with private industry through the assignment of IPRIS agents to the National Cyber-Forensics and Training Alliance (NCFTA) in Pittsburgh, Pennsylvania. The NCFTA is a non-profit organization that brings together experienced agents and analysts, governmental experts, and leaders in the business world to form an integral alliance between academia, law enforcement, and industry. By merging a wide range of cyber expertise in one location, the NCFTA provides a conduit for information sharing between private industry and law enforcement. Because the NCFTA is a non-profit organization, it provides a neutral forum wherein private industry and law enforcement can exchange information regarding emerging and ongoing threats.

B. Trade Enforcement Unit

The IPR Center's Trade Enforcement Unit (TEU) is prioritized to combat predatory and unfair trade practices that threaten the U.S. economy and national security, restrict the competitiveness of U.S. industry in world markets, and place the U.S. public's health and safety at risk. The principal federal law enforcement agencies responsible for enforcing U.S. international trade laws and regulations are HSI and CBP. A common mission of the two agencies is to ensure that all goods entering the United States do so in compliance with U.S. laws and regulations. HSI commercial trade fraud investigations are a powerful enforcement tool for ensuring these goals are met.

To successfully conduct an illegal trade fraud investigation, HSI and CBP must work together. To complete its commercial trade fraud mission, HSI will investigate and refer for prosecutions and civil penalties willfully noncompliant importers, exporters, customs brokers, and other entities and individuals involved in international commerce, in order to provide a highly visible deterrent factor and disrupt and dismantle transnational criminal organizations. Illicit trade fraud investigations focus on commercial importations involving false statements and deceptive business practices. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/commercial-fraud-enforcement. Illicit trade fraud investigations are important components of an overall trade strategy and can result in significant seizures, civil penalties, and/or criminal prosecutions.

C. Outreach and Training Unit

The primary purpose of this unit is to expand industry awareness of the IPR Center's mission, authority, and capabilities with regard to intellectual property and substandard or dangerous imports. It also serves to encourage the sharing of related intelligence resulting in viable leads. The unit provides the face-to-face contact with IP industries, leading to greater networking. In accomplishing this facet of the mission, the unit participates in numerous conferences and accepts opportunities to deliver presentations and participate in panel discussions regarding copyright and trademark protection.

In addition to the industry outreach mission, the unit supports the training of state and local law enforcement, provides trainers and materials to foreign law-enforcement academies, and accepts requests from federal departments, foreign governments, and other international law enforcement entities, such as Interpol and Europol, for training and outreach opportunities. The unit conducted 422 outreach and training programs focusing on HSI best practices to domestic and foreign law enforcement, prosecutors, judges, and industry representatives, reaching approximately 21,456 individuals. The 422 outreach programs conducted in FY15 was a 32 percent increase over the 290 outreach programs conducted in FY14.

III. Operational portfolio

A. IPU programs

On July 18, 2007, President Bush issued an executive order establishing an interagency working group on import safety to address the dangers found in imported apparel, pet food ingredients, toys, seafood, and other consumer products. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact_sheets/Operation%20 Guardian%20Fact %20Sheet %20FINAL%20-%20IPR%20DIRECTOR%20APPROVAL.pdf/view. To address the goals and objectives identified by the working group, the IPR Center developed and implemented Operation Guardian, a multi-agency umbrella program designed to combat the importation and trafficking of substandard, tainted, and counterfeit products that pose a health and safety risk to consumers. The collaborative work of Guardian has led to the seizure of commodities such as aircraft and automobile parts, pharmaceuticals, personal-care products, electrical devices, and food products.

Operation Chain Reaction (OCR): This comprehensive initiative targets counterfeit goods entering the supply chains of the Department of Defense (DOD) and other U.S. Government agencies. OCR is primarily focused on microelectronics, in part because they are used in virtually every system because and they are easy to counterfeit. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/operation-chain-reaction-fact-sheet. Counterfeit microelectronics pose a significant health and safety threat, potentially having catastrophic outcomes. These outcomes include the potential to delay DOD missions, affect the reliability of weapon systems, imperil the safety of service members, and endanger the integrity of sensitive data and secure networks. Beyond microelectronics, OCR has expanded to other commodities procured by the DOD and U.S. Government, including counterfeit pharmaceuticals, network equipment, and aircraft parts. The increased enforcement focus on semiconductors, and the safety and security risks they present, resulted in a five percent increase in seizures from FY13 to FY14. *Id.*

Operation Apothecary: This effort was launched in 2004 to address and attack potential vulnerabilities in the entry process that might allow for the smuggling of commercial quantities of counterfeit, unapproved, controlled, and/or adulterated drugs. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/Operation%20Apothecary %20Fact%20Sheet%20/view. Consumers purchase pharmaceuticals over the Internet with the belief that the products advertised are legitimate products when, in fact, the products are often a counterfeit or unapproved version that may have been manufactured in unsanitary conditions and/or not subjected to

any safeguards or quality controls. *Id.* Criminals posing as legitimate pharmaceutical providers advertise prescription drugs and/or inexpensive alternatives for sale without requiring a valid prescription. Since 2008, as part of Apothecary, the IPR center has participated in the Interpol-led operation called Pangea. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports /fact-sheets/ Operation%20Pangea%20Fact%20Sheet%20FINAL%20-%20IPR%20DIRECTOR % 20 APPROVAL.pdf/view. Operation Pangea is the largest global Internet-based operation focusing on illicit Web sites selling fake or counterfeit medicines. Pangea engages police, customs, and national regulatory authorities to target Web sites supplying fake and illicit medicines, and also works to increase awareness of the serious health risks. More than 100 countries participate in Pangea every year. *Id.*

Operation Plastic Beauty: This operation was initiated in January 2015, to combat the sale of counterfeit personal healthcare and beauty products. Plastic Beauty is an IPR Center initiative targeting the fabrication, illegal production, and/or illegal importation of counterfeit personal healthcare and beauty products. It targets, tracks, and prosecutes individuals who sell counterfeit personal healthcare and beauty products as legitimate products. Plastic Beauty addresses the potential vulnerabilities in the entry process that might allow for the smuggling of commercial quantities of counterfeit healthcare and beauty products via the Internet, International Mail Facilities, Express Courier Hubs, and land borders. Consumers purchase personal healthcare and beauty products with the belief that the products advertised are legitimate when, in fact, they are often a counterfeit or fake version of the product that may have been manufactured in unsanitary conditions and not subjected to any safeguards or quality controls. Criminals posing as legitimate brand representatives and providers advertise the sale of fake cosmetics and personal healthcare products across the nation.

Operation Engine Newity: The IPR Center manages Operation Engine Newity in conjunction other law enforcement agencies that collaborate to counter the threat of counterfeit automotive, aerospace, rail, and heavy industry related components that are illegally imported and distributed throughout the United States. These counterfeit components represent a grave threat to public safety due to the critical nature of transportation-related applications, and can include such items as airbags, brake pads, steering rods, and bearings. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/operation-chain-reaction-fact-sheet. The faulty operation of these devices can cause bodily harm and, in some cases, could result in a catastrophic mass-transit incident. Operation Engine Newity seeks to bring to bear all elements of federal law enforcement to counter this threat by educating industry stakeholders and the public, interdicting the counterfeit goods at the ports of entry, and investigating and prosecuting individuals who traffic these goods for monetary gain. A key element of Operation Engine Newity is strong engagement with industry. This partnership is critical to success as members of industry are experts on the products and the possible risks from counterfeit parts. For this reason, the IPR Center makes outreach and engagement a top priority of this program.

Operation In Our Sites (IOS): This is an HSI initiative that targets entities that distribute counterfeit products through infringing Internet Web sites. IOS is focused on developing long-term investigations that identify targets, assets, and financial schemes used in operating infringing Web sites domestically and internationally. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/operation-in-our-sites. Through this strategy, HSI seeks to arrest and prosecute offenders and seize assets and domain names/Web sites. The criminally seized domain names are redirected to the IPR Center seizure banner, which serves as a tool in educating the public about the perils of counterfeit items available on the Internet. The operation coordinates with rights holders to utilize their civil/ legal/administrative remedies to shutdown infringing Web sites and re-direct their civilly-seized Web sites to an Anti-Piracy/Counterfeiting Banner. The usage of this banner is based on a licensing agreement between ICE, HSI, and the rights holder, and it provides a conduit for the public to provide information on IPR violations, while also serving as a method to educate the public

about IP theft. The IPR Center continues to develop new and innovative strategies to protect intellectual property rights and seeks to adapt to the ever changing environment on the Internet.

Operation Team Player: The IPR Center launched this operation in June 2013, to target the sale and trafficking of counterfeit sports merchandise, apparel, and tickets. Because this is a multi-million dollar criminal industry, the trafficking of these items is extremely lucrative and becomes more profitable in markets involving successful and popular teams. The culmination of a sports season involving playoffs and championship games are events that stimulate the sale of counterfeit items. Throughout the year, HSI field offices determine the most effective mechanisms to initiate enforcement operations in their area of responsibility. The IPR Center works with the appropriate HSI office to assist in coordinating operations, related press releases, and press events for significant sporting events involving all major sports organizations, to include the National Football League (NFL), Major League Baseball, National Basketball Association, National Hockey League, and National Collegiate Athletic Association. The IPR Center coordinates with the NFL and the host HSI office for the Super Bowl to announce annual seizure numbers for Operation Team Player and to inform the public of the threat counterfeit items present to the U.S. economy and public health and safety. Past successful operations have included the targeting of retail stores, flea markets, and vendors. Additional targeting is coordinated with CBP to target inbound shipments of counterfeit sports apparel and other items at ports of entry across the United States. The IPR Center also strongly encourages HSI offices to coordinate operations with the U.S. Postal Inspection Service and state and local law enforcement agencies.

B. TEU programs

Anti-Dumping and Countervailing Duty (AD/CVD) Program: HSI investigations involve schemes to evade the payment of duties imposed by the U.S. Government on certain imports. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/anti-dumping-fact-sheet/view. The additional duties assessed level the playing field for domestic producers competing with foreign exporters that are engaged in the practice of dumping foreign government subsidies. With the assistance of CBP and Department of Commerce (DOC), HSI investigates importers and other entities attempting to illegally circumvent payment of required duties through illicit transshipment, mislabeling, and undervaluation. Dumping occurs when a foreign producer sells a product in the United States either at a price below that producer's sales price in its home market or at a price that is lower than cost of production. Subsidizing occurs when a foreign government provides financial assistance to benefit the production, manufacture, or exportation of a good. When DOC determines that an imported product is being dumped or subsidized, and the U.S. International Trade Commission finds that a U.S. industry producing a similar product is materially injured or threatened with material injury, an antidumping duty order or countervailing duty order is imposed as a remedy to the illegal trade practice.

Once an AD/CVD order is issued, DOC instructs CBP to collect the AD/CVD on imports of the product into the United States to offset the unfair trade practice. One of the most high-profile anti-dumping cases, which started with a lead from CBP import specialists, involved the illegal importation and distribution of mislabeled Chinese honey. *See* Press Release, U.S. Immigration and Customs Enforcement, (Feb. 20, 2013), https://www.ice.gov/news/releases/ice-and-cbp-announce-charges-linked-major-commercial-fraud-enterprise. It was determined that the honey was mismarked as coming from other countries in order to evade over $180 million in countervailing duties. The lengthy investigation, which included undercover operations, led to almost 30 indictments, prison sentences of all non-foreign fugitives, more than $35 million in fines imposed, and the seizure of 4,500 55-gallon drums of honey.

Environmental crimes and wildlife trafficking: On July 1, 2013, President Obama issued the Executive Order "Combating Wildlife Trafficking." Exec. Order No. 13648 78 FR 40621 (July 1, 2013). EO 13648 mandated the creation of an interagency task force to combat global wildlife trafficking, a multi-billion dollar illicit business. HSI is a participating member of the Wildlife Trafficking Task Force.

The Task Force was established to formulate a national strategy for combatting wildlife trafficking that will be incorporated into the President's Strategy to Combat Transnational Organized Crime. HSI collaborates with the U.S. Fish and Wildlife Services, the National Oceanic and Atmospheric Administration, and the National Marine Fisheries Service, to enforce the Endangered Species Act and the Lacey Act when individuals import/export certain species into or from the United States, or when they possess, distribute, or transport, any species in interstate or foreign commerce. HSI uses its customs authorities to pursue criminal prosecutions when wildlife is smuggled over the border. Commonly trafficked wildlife includes elephant ivory, rhino horns, turtle shells, and exotic birds and reptiles.

In addition, HSI investigates the illegal importation of automobiles, farm equipment, and engines that are smuggled or imported into the United States in order to avoid Department of Transportation and Environmental Protection Agency safety and emission standards. We also enforce federal laws and regulations intended to preserve air, land, and water resources by targeting the illegal importation and exportation of hazardous waste and ozone depleting substances.

Forced Labor Program: The TEU shares responsibility with HSI's International Operations in managing the Forced Labor Program for all HSI forced labor investigations. HSI investigates allegations of forced child labor and forced labor relating either to the manufacture or production of goods overseas that are exported to the United States, or labor in the United States that results from coercion, debt bondage/indentured labor, or other non-voluntary means of forcing an individual to provide work or a service. HSI headquarters, HSI domestic offices, and HSI international offices around the world conduct and assist with forced labor investigations needing information or collateral investigations. Products manufactured or produced by forced or indentured labor do not always differ in appearance from products made by legitimate labor. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/fcl-fact-sheet.

Forced labor may be a result of trafficking sex workers, indentured labor at factories, or cultural norms that are practiced in countries around the world (such as children being leased or sold into indentured servitude or made to work as a result of the debt bondage of their families). Worksite investigations are usually how forced labor is discovered. HSI cooperates with various IPR Center partners to share information and collaborate in efforts to combat forced labor.

The HSI Forced Labor Program is committed to identifying foreign manufacturers that are seeking to illegally import merchandise into the United States in violation of 19 U.S.C. § 1307, which prohibits the importation of goods produced by convict, forced, or indentured labor under penal sanction, including forced or indentured child labor. U.S. importers, foreign manufacturers, and criminal organizations that are responsible for facilitating forced labor may be subject to criminal prosecution and the seizure and forfeiture of their merchandise, if found to be involved in using forced labor. Forced child labor is a heinous issue, and international standards severely restrict the work that a child may perform. Forced labor investigations often require coordination with other U.S. Government agencies, as well as with non-government organizations and victim assistance personnel.

Free Trade Agreements Program: The TEU manages the Free Trade Agreements (FTA) program for HSI investigations of individuals and companies engaging in FTA and legislative preference program violations. Merchandise that enters the United States under an FTA does so under favorable duty rates. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/fta-fact-sheet/view. HSI's most significant investigative concern is conspiracy between companies to circumvent FTA origin requirements by entering goods using false country of origin claims. In many cases, goods are transshipped through an FTA country to disguise their true origin and eligibility, with the intent of receiving a duty preference established by the FTA. FTA violations also occur when importers falsely claim a product is manufactured in an FTA signatory country from qualifying materials, when it is actually made from non-qualifying, non-signatory originating materials. HSI trade fraud investigations are conducted to detect fraud and promote FTA compliance. They may result in significant

recoveries of revenue. HSI, in conjunction with CBP, engages with domestic and international partners to share intelligence and collaboratively investigate violations. Additionally, HSI and CBP have developed and distributed training material consistent with current international trade agreement obligations.

Textile Program: The TEU manages the textile program, which focuses on investigations of criminal and civil violations of customs laws involving textiles. The violations are executed through a variety of fraudulent schemes and practices, including false invoicing, false claims of origin, false markings/labeling, misclassification, false description, and smuggling. This effort is in support of the overall goal of HSI and CBP to ensure that inadmissible goods do not enter the U.S. commerce, that duties are not evaded, and that there is compliance with applicable laws. CBP is responsible for enforcing the legal requirements of these agreements and of other U.S. laws applicable to the textile industry. HSI is responsible for conducting investigations of significant criminal and civil violations of these laws. Successful investigations produce significant seizures, civil penalties, and/or criminal prosecutions. HSI, in coordination with CBP, is responsible for coordinating Textile Production Verification Team (TPVT) visits. Since 1987, these teams have been deployed to foreign textile factories to verify production of textiles that have been exported to the United States under free trade agreements and legislated trade programs. The TPVTs are comprised of special agents, import specialists, and regulatory auditors who are trained to verify production and manufacturing capabilities of the factories visited. These teams visit roughly 175 factories across 10 foreign countries every year.

Tobacco smuggling: The TEU manages the tobacco smuggling program for all HSI tobacco smuggling investigations. HSI tobacco smuggling investigations include, but are not limited to: the domestic and international smuggling of cigarettes, the trafficking in counterfeit or stolen cigarettes, the smuggling of cigarettes in violation of embargoes, and international money laundering investigations where one of the underlying crimes is tobacco-related. Over recent years, tobacco smuggling has become a lucrative criminal enterprise, resulting in the annual loss of billions of dollars in tax revenue and customs duties around the world. *Factsheet* , NAT'L INTELL. PROP. RTS. COORDINATION CTR., https://www.iprcenter.gov/reports/fact-sheets/tobacco-smuggling-fact-sheet. While the extent of tobacco smuggling in the U.S. cannot be precisely determined, HSI has made great strides disrupting and dismantling transnational criminal organizations involved in illicit tobacco trade.

Illicit tobacco activities are attractive to international and domestic criminal groups because of the high profits and relatively low risk of prosecution. Tobacco smuggling into the United States results in the loss of federal and state excise tax revenue. In an effort to evade duty, smugglers under-report weight on shipments, undercount and undervalue cigarettes (which have a compound duty), improperly mark the country of origin, and divert products from customs bonded and duty free facilities. Tobacco smuggling often involves falsely manifesting shipments from foreign countries and illegal manipulation of the in-bond system. Contraband and counterfeit cigarettes are commonly smuggled into the United States in ocean containers and are falsely described as items such as plastic, furniture, or toys. HSI has expanded cooperation with international law enforcement agencies and customs services to combat this problem.

HSI conducts independent tobacco smuggling investigations and joint investigations to monitor, combat, and disrupt, illicit tobacco trade with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Alcohol and Tobacco Tax and Trade Bureau (TTB), and the Food and Drug Administration (FDA), as well as numerous state and local enforcement agencies, due to overlapping jurisdiction. The 2010 implementation of the Prevent All Cigarette Trafficking Act prohibited Internet sales of tobacco, therefore increasing the incentive of illicit tobacco trade. Additionally, diversion and smuggling of tobacco may have increased in order to avoid paying higher costs and taxes.

IV. Enforcement resources

Trade Enforcement Coordination Centers: On January 18, 2012, HSI and CBP Headquarters issued a Commercial Fraud Working Group Field Evaluation and Implementation Plan. *National Intellectual Property Rights Coordination Center: Trade Enforcement Unit Overview (2015).* The objective of the Joint Commercial Fraud Enforcement Improvement Plan was to establish procedures and guidelines between HSI and CBP to facilitate and expedite the exchange of commercial fraud information between the agencies, thus leading to successful criminal prosecutions and civil actions for trade violations. One of the recommendations was to establish integrated commercial trade fraud units at the field level. Many of the recommendations in the paper were met by integrating the HSI and CBP commercial fraud units into Trade Enforcement Coordination Centers (TECCs). TECCs promote information sharing among all entities involved in trade enforcement, assist in proactively identifying trade schemes, and foster complete threat assessments. They further help in creating an integrated team, working side-by-side on a daily basis, and reinforce the already-established HSI-CBP partnership.

To identify and effectively combat illicit trade, the TECCs combine resources by co-locating HSI and CBP personnel in close proximity to the customs examination area. TECCs ensure joint CBP and HSI oversight and prioritization of the enforcement and interdiction process in the local area, and involve HSI early during the importation or exportation phase and/or during the interdiction process. Fraud schemes discovered by the TECCs include illegal transshipment through third countries, falsifying the country of origin, exploitation of the in-bond system, and stealing the identity of a legitimate business or importer. The TECCs enable HSI and CBP to present a united front and a more complete case analysis for the presentation of cases to United States Attorneys' offices. They also allow for increased commercial enforcement activity and civil penalties.

HSI's National Targeting Center—Investigations: The primary purpose of NTC-I is to enhance and support HSI's investigative efforts, including intellectual property rights, commercial fraud, financial crimes, gang enforcement, counter-proliferation, and human trafficking and smuggling. HSI and CBP are uniquely positioned to disrupt and dismantle transnational criminal organizations that seek to exploit our border security efforts.

CBP'S National Targeting Center—Cargo/Passenger: The National Targeting Center (NTC), led by CBP, serves as the central targeting and coordination center, and plays a critical role in promoting border security, public safety, and national security through the identification and prevention of the unlawful entry, movement, and smuggling of people, goods, and contraband, that could pose a threat to the United States. Together with other DHS agencies, such as the Transportation Security Administration and the U.S. Coast Guard, the integration of HSI at the NTC strengthens DHS's ability to better target and interdict bulk cash, narcotics, weapons, and other smuggled goods, in addition to enhancing HSI program area efforts, such as financial crimes, gang enforcement, intellectual property rights, and human trafficking and smuggling.

Import Safety Commercial Targeting and Analysis Center: The Import Safety Commercial Targeting and Analysis Center (CTAC) is a CBP facility designed to streamline and enhance federal efforts to address import safety issues. The Import Safety CTAC combines the resources and manpower of CBP and other government agencies to protect the American public from harm caused by unsafe imported products, by improving communication and information-sharing, and reducing redundant inspection activities.

National Targeting and Analysis Groups: When there is a need for creative and effective analytical support on major trade issues, National Targeting Analysis Groups (NTAG) have been invaluable in supporting national trade strategies and field enforcement operations. There are four NTAG's located across the country, each focusing on different major trade issues having a direct impact

on the health, safety, and economic interests of the United States. NTAGs are located in Dallas, TX (Free Trade Agreements), Los Angeles, CA (Intellectual Property Rights), New York, NY (Textile), and South Florida (AD/CVD).

Centers of Excellence and Expertise: The Centers of Excellence and Expertise bring all of CBP's trade expertise to bear on a single industry in a strategic location. They are staffed with numerous trade positions using account management principles and operational skills to authoritatively facilitate trade. The centers also serve as resources to the broader trade community and to CBP's U.S. Government partners. Personnel answer questions, provide information, and develop comprehensive trade facilitation strategies to address uniformity and compliance concerns. The centers transform the way CBP approaches trade operations and work with the international trade community. The centers represent CBP's expanded focus on "Trade in the 21st Century" by aligning with modern business practices, focusing on industry-specific issues, and by providing tailored support to unique trading environments. The centers were established to increase uniformity of practices across ports of entry, facilitate the timely resolution of trade compliance issues nationwide, and further strengthen critical agency knowledge on key industry practices.

Regulatory Audit: Regulatory Audit (RA) conducts post-entry compliance audits of large, multinational companies and audits of various entities active in importing merchandise into the United States. With 10 field offices and a nationwide staffing of over 360 professional auditors, RA's audit staff possesses the technical skills and experience to conduct a wide variety of audits. RA assists special agents and AUSAs on a number of different types of civil and criminal investigations of businesses and individuals that commit violations of regulations and laws. RA has the capability and experience to support all types of enforcement cases, including trade fraud—antidumping and countervailing duty (AD/CVD), undervaluation, money laundering, merchandise smuggling, visa fraud, and human smuggling, among others. Auditors work very closely with HSI agents to set the objectives, scope, and/or methodology of the audit that can be tailored for each case, based on the needs of the agents. HSI offices can fill out and submit a referral questionnaire to their local RA office to request assistance at any time. The referral questionnaire and RA contact information are available on the HSI National IPR Center Documents Web page.

V. Going forward

Going forward, the IPR Center will continue to place emphasis on the targeting of counterfeit goods that threaten the health and safety of the American consumer. The proliferation of counterfeit pharmaceuticals in the Northern California area was linked to five deaths last year; counterfeit electrical components destined to be used on nuclear submarines were sold to key defense contractors; and a counterfeit performance bicycle broke under the stress of common usage, causing major injuries to the rider. Through the development of enhanced administrative and operational efforts, the IPR Center can limit the destructive effects of counterfeit goods.

One important and current administrative initiative at the IPR Center is the specific documentation of serious injuries, links to criminal organizations, and impacts to businesses and the economy, all associated with counterfeiting. The U.S. Food and Drug Administration has shared examples of individuals immediately developing a rash after using counterfeit cosmetics. There are known instances of teenagers experiencing vision loss after using counterfeit decorative contact lenses. The Los Angeles Police Department has evidence linking pirated goods to violent street gangs. And, we have received confirmation that a group in Michigan was selling counterfeit pharmaceuticals to fund terrorist activities in the Middle East. Presenting specific cases to consumers, domestic and international law enforcement, and the legal community will improve the IPR Center's educational outreach campaign.

The IPR Center will continue to strengthen our collaboration with industry and international law enforcement. No organization is more equipped to protect copyrights and trademarks, and no organization has more intelligence identifying the location of counterfeiters than the IPR Center. The outreach and intelligence sharing with industry is a major resource that must be leveraged to develop strong investigations. Interaction with industry makes our agents more effective, and it offers innumerable contributions to investigations. Representatives from all industry sectors have a standing invitation to visit the IPR Center, with the purpose of starting a productive dialog about preventing intellectual property theft.

The IPR Center is committed to collaborating with international law enforcement on worldwide anti-counterfeiting operations. In June 2015, the center coordinated with Interpol to support Operation Pangea, an effort that brought together 115 countries and 236 agencies to combat the sale of illegal medicines online. Last year's operation led to the seizure of over 20 million fake and illicit medicines worth an estimated $81 million. It also resulted in the arrests of 156 individuals and additional pieces of information supporting 429 investigations. *See INTERPOL, Operations—Pangea VIII*, http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea.The IPR Center will continue to support Project Transatlantic as part of Operation In Our Sites, an HSI- and Europol-led effort that teamed industry with law-enforcement agencies across 27 countries to shutdown 37,479 domain names that were illegally selling counterfeit merchandise online to unsuspecting consumers in FY 15.

Finally, the IPR Center will adapt to illegality and proactively develop innovative operations to address counterfeit goods that present health and safety hazards. In March 2014, HSI participated in the takedown of a massive multimillion-dollar ring that sold counterfeit health and beauty items like lip balm, baby oil, petroleum jelly, and sanitary pads. *See CNN, Massive fake health and beauty supplies ring busted*, http://www.cnn.com/2014/03/08/justice/new-york-counterfeit-beauty-supplies. Over the last two years, the number of personal care products seized—including shampoo, deodorant, and lotion—has tripled. In response to those developments, the IPR Center created Operation Plastic Beauty in late 2014 to target these types of items. As new counterfeiting patterns and trends emerge, the IPR Center will aggressively address them with strategic enforcement techniques.

VI. Conclusion

Each year, more than 11 million maritime containers arrive at our seaports. At land borders, another ten million arrive by truck and three million by rail. An additional quarter billion more cargo, postal, and express consignment packages arrive through air travel. The agencies within the Department of Homeland Security remain vigilant in targeting shipments posing a risk to the American people. In 2014, the number of IPR seizures totaled 23,140, with an estimated value of almost a quarter trillion dollars. IPR Center-related enforcement efforts in 2014 led to 683 arrests, with 454 indictments and 461 convictions. *See Department of Homeland Security, Intellectual Property Rights Seizure Statistics—Fiscal Year 2014*, https://www.iprcenter.gov/reports/ipr-center-reports/fy-2014-ipr-seizure-statistics/view. Seizure statistics for 2015 are still being calculated, but early evidence suggests those figures are trending significantly higher. The IPR Center is committed to supporting IP enforcement that protects consumers and the U.S. economy, while terminating criminal distribution networks.❖

ABOUT THE AUTHOR

❑**Bruce M. Foucart** is the Director for the National Intellectual Property Rights Coordination Center, which is located in Arlington, VA. The center operates as a task force of 23 partner agencies (19 key U.S. agencies and 4 international partners) who together stand at the forefront of the U.S. Government's response to global intellectual property theft. In addition to leading the IPR Center, Mr. Foucart is responsible for U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations' (HSI) criminal trade fraud investigations program. ✠

Operation In Our Sights

Justin S. Herring
Assistant United States Attorney
District of New Jersey

I. Introduction

Given the central role that the Internet plays in almost every aspect of society, U.S. Attorneys' offices nationwide have focused on aggressively prosecuting cybercrime. As part of that effort, federal prosecutors have adapted older investigative tools and methods to make them more effective in combatting crimes today. This article describes how my former office, the U.S. Attorney's Office for the District of Maryland, "seized" Web site domains as part of Operation In Our Sights (IOS) in 2011 and 2012. IOS is an initiative run through the National Intellectual Property Rights Coordination Center to target Web sites used to sell counterfeit merchandise. More information about IOS is available in the article entitled "Intellectual Property Enforcement Programs: Helping State and Local Law Enforcement Combat Intellectual Property Crime" included in this issue.

The Web sites operate like most online retail or "e-commerce" sites, but instead of selling legitimate products, they sell counterfeit goods. In most cases, the operators of these sites are located outside the United States and are, therefore, difficult or impossible to prosecute. But by seizing the domain names, IOS raised awareness and deterred the sale of counterfeit products, and temporarily disrupted the sale of counterfeit goods. As a result, we were able to enhance the impact and effectiveness of our investigation and criminal prosecution.

We participated in five "rounds" of domain seizures in 2011 and 2012. To maximize the impact, each round involved seizures coordinated across several districts and, in one case, several countries. Because the primary goal was to raise awareness among customers or potential customers for counterfeit products, the seizures were timed to generate as much media coverage as possible. For instance, one round of seizures was executed the week before the Super Bowl, and focused on sports-related products like jerseys and sneakers. Another round occurred just before Black Friday and Cyber Monday.

II. Legal authority

We seized domains with warrants issued under 18 U.S.C. § 981(b). Title 18 U.S.C. § 2323(a)(2) allows § 981 seizure warrants to be issued for property subject to forfeiture under most IP criminal

statutes, including 18 U.S.C. § 2320 (trafficking in counterfeit goods). To do so, we were required to show a nexus between the crime of trafficking counterfeit goods and the domain names. In most cases, this was straightforward. The Web sites often directly advertising “knock-offs” or “replicas” for sale, and undercover buys confirmed that the products were, in fact, counterfeit.

The warrants were served on the top-level domain registry—usually Verisign, which is the registry for “.com” and “.net” domains. At the time of these seizures, all the top-level domain registries involved were in the United States and subject to U.S. legal process. (This, of course, is increasingly no longer true.). Each of the warrants ordered the registries to direct all traffic to a government server, which would display a seizure "banner" showing that the Web site was now in the hands of the U.S. Government, and reminding the viewer that counterfeit products were illegal.

III. The seizures

Each round of seizures progressively targeted more Web site domains. The first seizure warrant was for five Web site domains. Each domain was obviously selling trademarked, counterfeit merchandise, such as NFL jerseys and clothing sporting logos for Red Bull and the Baltimore Orioles. One Web site even used a trademark in its name: "pumaforever.com." Agents made undercover purchases of merchandise from each Web site. The transaction was usually similar to the online purchase of any legitimate product. The agents browsed the apparent counterfeit items on the Web site. The agents then put their selections in a “shopping cart" and used a credit card to make the purchases. After the purchase, an email would be sent with a receipt and tracking number for the purchase. The merchandise was shipped to the agent (from China, in every case), and an industry representative examined each product and confirmed that it was counterfeit.

Based on this evidence, showing probable cause for the seizure was straightforward. It was obvious from the front page of the Web sites hosted at these domains that they were used to traffic counterfeit products, and the undercover purchases confirmed that. It quickly became apparent, however, that the sellers were using multiple domains to sell counterfeit goods, and for each seller we had seized only one or two of the many domains they were using. Thus, in subsequent rounds of IOS, we expanded the number of domains seized by identifying groups of domains being used by the same seller.

Once we could show that a group of domains linked to a single seller, we could seize all the domains together. Some of the means used were fairly “low tech,” as online investigations go. For instance, an undercover agent simply emailed the customer contact for Web sites that were already seized, expressed disappointment that the old Web site was down, and asked for a new place to buy counterfeit items. That usually prompted the sellers to provide a new domain name to the undercover agent. An undercover agent also asked several counterfeit sellers, via email, if they had other Web sites. That usually got a response as well.

Simply examining the Web sites and using publicly available domain registration information made it easy to link multiple domains together. In many cases, the sellers made little effort to cover their tracks, so multiple domains run by a single seller often shared common domain registration information, such as the same email address, company name, and/or company address. Inspecting the Web sites themselves provided useful evidence. Web sites used by the same seller often had identical looking pages. Even if the “front page” was different, the “contact us” page or the checkout and payment page was often identical. Sellers often used the same contact email across multiple domains. In other cases, different Web sites re-directed users to a common domain for finalizing purchases.

This evidence not only helped us identify additional domains for seizure, it also enabled us to seize domains without having to make an undercover purchase from each domain. As long as we had probable cause to show that the Web sites were all being used to sell counterfeit goods, we could seize all the domains without having to make a purchase from each one. Although we did not make undercover

purchases through every domain, the Web site at each domain was inspected by an agent to confirm that it was similar to other Web sites used by the same seller and that it was being used to sell counterfeit items.

The second and third warrants we prepared in 2011 used these methods for 27, and then 71 domains respectively. In early 2012, we participated in another round of domain seizures aimed at sports apparel, and timed to occur just before the Super Bowl. Using all the techniques described above, we seized 241 domains selling counterfeit football jerseys and other sports-related counterfeits.

Later in 2012, we participated in another IOS initiative aimed at Web sites selling counterfeit prescription drugs. (This was the last round of seizures I was involved in, but IOS has continued to this day.). We prepared warrants to seize 686 domains. The domain seizures were part of an internationally coordinated seizure of Web sites and payment processors for online sellers of counterfeit medications, such as Viagra and Lipitor. In addition to all the techniques described above, the agents used a "Web crawler" to obtain evidence for domain seizures. Web site creators often replicate the same Web site under different domain names—which is easier than creating a new Web site from scratch each time. The Web crawler scanned the Web sites and created a unique hash value out of the various components of the Web site. This hash value was then compared to other Web sites. If there was even the slightest difference in the Web sites, the hash values would be different. If the hash values were identical, the Web site template was the same, and the Web sites would behave and function the same, even though the domains were different. The Web crawler allowed us to efficiently link together dozens, or even hundreds, of different sites used by the same seller, and seize them all using a single affidavit.

IV. Conclusion

Our use of seizure warrants to seizure Web site domain names on IOS shows how federal prosecutors can utilize old law enforcement tools and adapt them to combat new crimes that are carried out online. By doing so, we made the investigation and prosecution more effective, both by stopping the criminal activity and promoting specific and general deterrence. ❖

ABOUT THE AUTHOR

❑ **Justin S. Herring** was an AUSA in the District of Maryland from 2010 to 2014, where he was designated as a Computer Hacking and Intellectual Property prosecutor. He is currently an AUSA in the Computer Hacking and Intellectual Property Section in the District of New Jersey. ✠

Prosecuting Counterfeit Prescription Drug Cases

Andrew Lay
Assistant United States Attorney
White Collar Unit
Eastern District of Missouri

I. Introduction: A "gooey mess" in the Eastern District of Missouri

Sometime in February 2010**,** Dr. Abid Nisar of Town and Country, Missouri, received a fax transmission at his oncology practice from a company called "BDMI." BDMI's fax contained a chemotherapy drug price list. BDMI's fax stated that the list was provided to Dr. Nisar on a "confidential basis," with the forwarding or distribution of the materials "strictly prohibited." BDMI's fax suggested that Dr. Nisar could purchase cancer chemotherapy prescription drugs at 14 to 60 percent off their average wholesale price in the United States, thereby saving his oncology practice an average of ".40 cents on every dollar spent on oncology medications."

Oddly, BDMI's fax advised Dr. Nisar that any drug purchases from BDMI "were best used to supplement the medication purchases for medical practices, not in lieu of traditional wholesalers." The "best way" to utilize BDMI's services was "to purchase a percentage of medications" from BDMI while continuing to use "current wholesaler(s) for all other medications."

Dr. Nisar began purchasing most of his cancer chemotherapy drugs from BDMI, and packages began appearing at his office that had been shipped from England. Some of Dr. Nisar's international drug packages were marked as "gifts" on their customs declarations, and had no return address. The prescription cancer drugs inside the BDMI packages had different drug trade names than what Dr. Nisar previously had been using with local breast cancer patients (e.g. Mabthera® instead of Rituxan®), and—at least according to their labeling—were manufactured by different companies in different factories (e.g. Roche in Switzerland versus Genentech in Vacaville, California).

Typically, BDMI's prescription cancer drugs' dosage and use instructions were in foreign languages. Some of BDMI's chemotherapy drugs, according to their drug labeling, required storage and shipment at uniformly cold temperatures to ensure the drugs' efficacy and safety.

On October 13, 2010, Dr. Nisar received a BDMI shipment that included Mabthera®, a Turkish cancer chemotherapy drug that is similar to what is marketed in the U.S. as Rituxan®. A nurse working for Dr. Nisar complained to BDMI that the inside of the package was "a gooey mess," with a "gooey substance" covering the warm prescription drugs in the package. One of the cold packs in the box was damaged during shipment and leaked, making the boxes of the prescription drugs in the package wet and disintegrated. Dr. Nisar received a credit from BDMI for this damaged package, but kept ordering more drugs from BDMI.

Ultimately, Dr. Nisar and several other Missouri doctors and clinic employees were charged in the Eastern District of Missouri with receiving misbranded and adulterated drugs in interstate commerce. The District also prosecuted two Californian residents who operated BDMI (James Newcomb and Sandy Behe), one English national (Richard Taylor) who was shipping some of Dr. Nisar's drugs to Missouri, two Canadians (Kamaldeep Sandhu and Navdeep Sandhu), and two Turkish men (Ozkan Semizoglu and Sabahaddin Akman) for smuggling and related crimes. Sentences ranged from probation to 30 months in prison. Over $5 million was forfeited during the investigation, in addition to over $1.6 million in civil

Medicare fraud False Claims Act settlements. Other doctors and shippers involved in this scheme were also charged in the Southern District of California, the Eastern District of New York, and other districts. All of the doctors faced collateral consequences, including the loss of medical licenses and exclusion from participation in federal programs. *See generally* 42 U.S.C. § 1320a-7(b)(2), (b)(7) (2015) (discussing U.S. Department of Health and Human Services' exclusion authority); *Travers v. Shalala*, 20 F.3d 993 (9th Cir. 1994) (finding exclusion to be mandatory after a doctor's "no contest" diversion guilty plea).

The investigation recovered large amounts of suspect prescription drugs from various doctors' offices and other locations. Some of the seized Altuzan® (a Turkish cancer treatment drug that is similar to Avastin®, but not approved for sale in the United States) was later determined by the U.S. Food and Drug Administration to be counterfeit: the drug vials contained dirty water and mold, but no active drug ingredients.

II. FDA's closed system of drug distribution

A brief overview of federal drug manufacturing and labeling laws is critical for understanding how to prosecute the distribution of counterfeit and unapproved prescription drugs. For specific legal issues, AUSAs should always consult with knowledgeable persons at the Consumer Protection Branch of the U.S. Department of Justice, and the Office of Chief Counsel for the Food and Drug Administration (FDA).

Anyone marketing a drug in the United States must first prove to the FDA that the drug is safe and effective, and that the manufacturing and distribution methods consistently create a uniform and stable drug. Drug manufacturers typically start the process by submitting a new drug application to the FDA pursuant to 21 U.S.C. § 355(a). The application for approval discusses, in great detail, how the drug works, how the drug will be manufactured, and precisely what the drug's label will say. Before a new drug may be introduced into interstate commerce, the FDA must approve the manufacturing process, labeling, and packaging. 21 U.S.C. § 355(b)(1) (2015). The approval process addresses the chemical composition of the drug, *id.* § 355(b)(1)(B)-(C), the drug's safety and effectiveness, *id.* § 355(b)(1)(A), elements of the drug's distribution, such as "the methods used in, and the facilities and controls used for the manufacture, processing, and packing" of the drug, *id.* § 355(b)(1)(D), and the "labeling proposed to be used" for the drug, *id.* § 355(b)(1)(F). *See* 21 C.F.R. § 314.50(c) (2014).

A drug is "misbranded" if its labeling is false or misleading in any particular way. 21 U.S.C. § 352(a) (2015). The term "labeling" is broadly defined as "all labels and other written, printed, or graphic matter (1) upon any article or any of its containers or wrappers, or (2) accompanying such article." *Id.* § 321(m). A drug is also deemed to be misbranded unless its labeling bears adequate directions for use. *Id.* § 352 (f)(1); 21 C.F.R. § 201.5 (2014).

A drug is "adulterated" if it was prepared, packed, or held under insanitary conditions where it may have become contaminated, or if it was packed or held in a manner inconsistent with current good manufacturing practices. 21 U.S.C. § 351(a)(2)(A)-(B) (2015).

Title 21 U.S.C. § 321(g)(2) defines a "counterfeit drug" as *either* a drug *or* a label that bears a trade name that falsely represents who actually manufactured, packed, or distributed it.

Critically, FDA's approval process is specific to each manufacturer and each product. 21 C.F.R. § 314.50 (2014). In sum, the federal drug laws create a "closed system" of drug manufacture and distribution that is designed to guarantee safe and effective drugs for consumers in the United States. Imported drugs with the same chemical composition as FDA-approved drugs are illegal because they are manufactured outside the United States' closed system of drug distribution that protects consumers from potentially unsafe pharmaceuticals. *In re Canadian Import Antitrust Litigation*, 470 F.3d 785, 790-91 (8th Cir. 2006). Importing unapproved drugs of unknown pedigree is not a minor violation of federal law. Misbranded drugs create more than "hyper-technical" violations of the FDA laws:

> It is, rather, a manifestation of a congressional plan to create a "closed system" designed to guarantee safe and effective drugs for consumers in the United States. Drugs that are not properly labeled for sale under federal law sometimes may be similar in substance to those that are sold legally within the United States. In other cases, however, they may be drugs with chemical compositions that are not yet approved by the FDA, drugs not manufactured in accordance with FDA rules, or drugs not transported or stored in a manner that is deemed safe by the FDA . . . . [T]he labeling requirements cannot be segregated from other [FDA] requirements in this way. Instead, they work in conjunction with the other statutory standards and FDA regulations to create a system that excludes noncompliant and potentially unsafe pharmaceuticals. This "closed system" ensures that approved prescription drugs are "subject to FDA oversight" and are "continuously under the custody of a U.S. manufacturer or authorized distributor," thus helping to ensure that the quality of drugs used by American consumers is consistent and predictable.

Id. at 790 (citations omitted).

The legislative history to the Prescription Drug Marketing Act of 1987 (PDMA) is instructive. In the PDMA, now codified at 21 U.S.C. § 333(b)(1), Congress limited the importation of prescription drugs after finding that "the integrity of the distribution system for prescription drugs is insufficient to prevent the introduction and eventual retail sale of substandard, ineffective, or even counterfeit drugs." Prescription Drug Marketing Act, Pub. L. No. 100-293, 102 Stat. 95 (1988) (codified as amended 21 U.S.C. 9 §§ 331, 353, 381). Congress specifically noted the danger that imported drugs may become "subpotent or adulterated during foreign handling and shipment." *Id.* Congress was further concerned that drug importation was "[a] catalyst for a continuing series of frauds against American manufacturers and ha[d] provided the cover for the importation of foreign counterfeit drugs." *Id.*

Anyone who receives misbranded or adulterated drugs from interstate commerce for later delivery into interstate commerce for pay is subject to either felony or misdemeanor criminal penalties. 21 U.S.C. § 331(c) (2015). Anyone who traffics in counterfeit drugs is guilty of a felony. 18 U.S.C. § 2320(a)(4) (2015). This general intellectual property statute contains enhanced penalties and forfeiture options for counterfeit drug cases. *Id*. § 2320(b)(3), (c). There are also enhanced fines and terms of imprisonment for "knowingly or recklessly" causing or attempting to cause serious bodily injury or death. *Id*. § 2320(b)(2).

III. Health care program reimbursement for prescription drugs

For most prescription drugs, doctors write the prescription and then patients fill the prescription at a pharmacy of their choosing. The pharmacy then directly submits a claim to a public or private health care program and receives reimbursement. Under this payment arrangement, a doctor has no financial incentive to use unapproved drugs that are cheaper than FDA-approved drugs, as the pharmacy (not the doctor) selects the drug to fill the prescription and receives money for the drugs from the program.

However, for some prescription drugs that are infused or injected into patients, doctors purchase the drugs and then submit claims for reimbursement to health care programs for the drugs and the cost of infusing or injecting them. Cancer chemotherapy drugs such as Rituxan®, Herceptin®, Neupogen®, and Avastin®, are examples of infusion drugs for which doctors seek direct reimbursement. Similarly, Botox® (covered by most health care programs for some conditions like migraine headaches) and orthopedic injectable devices like Synvisc® are other examples of drugs or products where the doctor seeks direct reimbursement from either a program or a patient.

AUSAs should consult with the Office of Inspector General for the U.S. Department of Health and Human Services for coverage guidance for specific drugs, but the Medicare and Medicaid programs generally will not cover or pay for unapproved prescription drugs. Instead, health care programs set fee

schedules for prescription drugs using the prices for FDA-approved drugs. *See generally* DEP'T OF HEALTH AND HUMAN SERVS., OFFICE OF AUDIT SERVICES, ADEQUACY OF MEDICARE PART B DRUG REIMBURSEMENT TO PHYSICIAN PRACTICES FOR THE TREATMENT OF CANCER PATIENTS (2005), found in the "Reports and Publications" section of the Office of Inspector General for the U.S. Department of Health and Human Services' Internet Web site.

Given that program reimbursement is usually set by the price of FDA-approved drugs, buying unapproved drugs that are 60 percent cheaper than their FDA-approved counterparts provides significant profit opportunities for doctors. In accounting terms, illegal, unapproved drugs create a significantly lower "cost of goods sold" that gives medical practices much higher net income. Taking into account that a large oncology practice with 200 cancer patients could easily spend $200,000 a month on FDA-approved chemotherapy drugs, the financial incentives for purchasing unapproved prescription drugs are tremendous (e.g., paying just $80,000 for unapproved drugs that are 60 percent cheaper gives a hypothetical practice with 200 chemotherapy patients a monthly increased profit of $120,000).

IV. Referral sources: Getting started

The United States Attorney's Office for the Eastern District of Missouri successfully started counterfeit prescription drug investigations from several sources. First, drug salespersons for U.S.-based licensed drug wholesalers made credible complaints to law enforcement when local oncologists or dermatologists suddenly stopped purchasing drugs, yet kept regular office schedules, which included plenty of scheduled infusions and injections. Particularly for cancer medications, there may be one or, alternatively, a small number of legitimate licensed local drug wholesalers from which doctors can make legitimate drug purchases. Drug salespersons can typically identify the local doctor's purchasing history, the market price of FDA-approved drugs, and key staff within the local doctor's office. The possibility of drug sales reps contacting law enforcement was why BDMI—the illegal drug wholesaler operating in Missouri and other states—encouraged physicians to keep buying some of their drugs from authorized wholesalers or drug companies.

Second, tracing international shipments has also been a useful referral source. The U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement, has referred cases to the District after noticing multiple suspicious packages being sent to a doctor's office, home, or post office box. Similarly, agents have identified the names and other shipping characteristics of foreign shippers of unapproved drugs, and then used DHS's entry records to identify persons and addresses within the United States receiving multiple shipments from suspicious senders.

Finally, banking, shipping, or call center records may reveal multiple U.S.-based customers, giving numerous districts investigative leads. The Eastern District of Missouri sent information about other doctors to Montana, California, Maryland, Iowa, New Mexico, and other states, after finding BDMI's customer list and its purchase history for all of their U.S. doctor/customers, triggering search warrants and, ultimately, prosecutions in other districts.

V. Successful investigating strategies

If a doctor is buying unapproved drugs in your district, a good strategy to begin with is subpoenaing the doctor's drug purchase records from all licensed U.S.-based drug wholesalers and obtaining the doctor's recent health care program drug billing. For the last year, has the doctor purchased only 100 units of approved drugs, but billed Medicare for 300 units? Was there a dramatic decrease in drug ordering from legitimate sources recently, but no corresponding decline in claims for drug reimbursement to health care programs? As the prescriber, it may be hard for the doctor to credibly claim to have no knowledge of what drugs are being used with his or her patients.

If unapproved drugs are recovered from either an intercepted Customs seizure or a doctor's office, then asking drug manufacturers if they have any sales data on the specific lots of drugs that were seized can be productive. Dr. Nisar had drugs on the shelf in his Missouri office that were initially shipped by drug manufacturer Roche to the Red Crescent Society of Iran, as well as other drugs from other drug companies that were initially shipped and sold in Sierra Leone, Africa. Some drugs could be stolen. Other drugs with a certain lot number may have previously been confirmed as counterfeit. Sending samples of the drug and the drug's labeling to either the drug companies or to FDA for scientific testing is also useful. The Eastern District of Missouri's prosecutions demonstrate that forensic testing can change what investigators believe is an unapproved drug investigation into an inquiry involving counterfeit drugs.

If either the labeling or the drug material inside the vial or syringe is not authentic, then the drug is "counterfeit" under federal law. The Eastern District of Missouri did seize some Botox® where the box containing the drug vials was counterfeit, but the drug inside the vial appeared to be authentic. Some unapproved drug smugglers may use false exterior box packaging for unapproved drugs to make them more closely resemble FDA-approved drugs. For instance, some smugglers may trade a box using foreign languages and trade names with a counterfeit English language box and the U.S. drug trade name to make the drugs more marketable. Some of the drug vials have holograms that are hard to counterfeit, forcing counterfeiters to buy empty used vials and then re-fill them with new tops.

Often, unapproved drug distributors have operations in multiple countries. In the Missouri cases, some drugs were sourced from Sierra Leone, shipped from Turkey to England, and then smuggled to doctors/customers in the United States. Participants in the scheme used bank accounts in California, Canada, Ireland, England, and Turkey, and used a call center in Canada to handle customer contacts. These types of businesses often have to rely heavily on email, given the number of participants and time zones. If a U.S.-based Internet Service Provider is involved, a search warrant for that domestic email account can be useful, even when other participants are using foreign-based Internet Service Providers. AUSAs should consult with the Office of International Affairs before conducting any investigative activities that may involve foreign nationals or evidence in foreign countries. Investigators who seek foreign documents, such as bank or corporate records, should make their requests early, as requesting foreign documents is often a lengthy process.

VI. Charging strategies and sentencing issues

Perhaps the simplest charging strategy is the receipt in interstate commerce of misbranded or adulterated drugs (or devices) for later delivery for pay. 21 U.S.C. § 331(c) (2015). Typically, unapproved drugs are misbranded in a variety of ways. Foreign language labeling could indicate inadequate dosage and use instructions. If the drug is counterfeit, then the label is misbranded because it falsely represents the substance to be something it is not. If the lot numbers on the package or vial are false, the drug may be misbranded because the labeling does not enable FDA to accurately trace the true manufacturing history of the drug. Moreover, the drugs are usually adulterated because the smuggler's methods of storage and shipping do not meet current good manufacturing practices. Adulteration can be easier to establish if the drug's labeling contains requirements to keep the drugs at constant cold temperatures and not to freeze or shake them, as with labels for the U.S. cancer drugs Herceptin®, Rituxan®, and Neupogen®.

Misbranding and adulteration can be charged as a strict liability misdemeanor or, if there is proof of intent to defraud or mislead, as a felony. Proof of intent may be available, for example, if the doctor or office staff lied to U.S.-based drug salespersons or patients about the source of the practice's drugs, or hid drugs with foreign language labeling from office staff or patients.

Anyone who dispenses or sells a counterfeit drug commits a misdemeanor offense. *Id.* § 331(i)(3). If there is proof of intent to defraud or mislead, then the crime is a felony. *Id.* § 333(a)(1)-(2).

As noted above, there is a similar Title 18 felony charge for trafficking in counterfeit drugs, with enhanced penalties and forfeiture options. 18 U.S.C. § 2320(b)(3)-(c) (2015).

Health care fraud, 18 U.S.C. § 1347, or making false statements to a health care program, 18 U.S.C. §§ 1035, are charging options for health care providers who have sought reimbursement from health care programs for unapproved drugs. Drug claims are "false" in that they use "J codes" that incorrectly represent to the program that a certain FDA-approved drug was used with patients during the infusion or injection session when, in reality, the patient received another drug. The key motive behind much of the unapproved drug purchasing is increasing profit by submitting claims to the health care program for approved drugs, while substituting cheaper, unapproved drugs. Typically, savings are not passed onto the patients, and doctors neither request nor receive informed consent from patients for using the unapproved drugs.

Felony misbranding, adulteration, counterfeit drug, and health care fraud charges all typically lead to sentencing under U.S.S.G. § 2B1.1. The amount of program loss or health care provider profit are key considerations. AUSAs should investigate if the doctor's office had any damaged or "gooey mess" shipments or health care problems from individual patients, given the reckless risk of bodily injury enhancement. *See, e.g.*, *United States v. Mateos*, 623 F.3d 1350, 1371 (11th Cir. 2010) (when the defendant is personally aware that her conduct in providing compromised medications to HIV patients could cause infections or other complications, the enhancement applies, even if there is no evidence that individual patients were actually harmed); *United States v. Hoffman*, 9 F.3d 49, 50 (8th Cir. 1993) (defendant in car insurance fraud scheme who intentionally caused automobile accidents subject to enhancement even if "staged" accidents occurred at slow speeds, because the Government only needs to show defendant acted recklessly, not that defendant intended to cause serious bodily injury). In investigations, drug integrity and patient complaints may not be documented significantly (or at all) in the health care provider's medical records of the actual patients, but may be extensively discussed in email or text messages when the provider seeks a refund for the damaged package or problem-causing shipment.

Smuggling goods or merchandise into the United States under circumstances that are contrary to law (e.g., the laws against misbranding and adulterating drugs) under 18 U.S.C. § 545 is another useful charge to consider. The fair market value of the drugs smuggled into the country is a key sentencing consideration under a smuggling charge. *United States v. Dall*, 918 F.2d 52, 54 (8th Cir. 1990) (using U.S.S.G. § 2T3.1 when imposing a sentence, based on smuggled drugs' fair market value, in prosecution of large supplier of unapproved animal drugs in the United States, who met with his customers to discuss smuggling the drugs into the United States, made the arrangements with European suppliers to send the drugs to Canada, and met with bank officials regarding a letter of credit for one of his customers).

When charging licensed health care professionals, AUSAs should consider whether a parallel civil investigation should be started to ensure complete public health care program recovery. Consulting with your office's Civil Division and, as appropriate, the Civil Frauds section of the U.S. Department of Justice, is time well spent. Any convictions, even corporate or misdemeanor charges, can lead to collateral consequences, including the loss of state medical licenses and exclusion from participation in federal programs, such as Medicare and TRICARE. AUSAs should consult with the Office of Counsel to the Inspector General, U.S. Department of Health and Human Services, if defense counsel raises questions about potential exclusion.

VII. Conclusion

Food and drug laws "touch phases of the lives and health of people which, in the circumstances of modern industrialism, are largely beyond self-protection." *United States v. Dotterweich*, 320 U.S. 277, 280 (1943). The patients who received smuggled drugs in the Eastern District of Missouri had no practical ability to test the drugs they received or determine their efficacy before infusion. Prosecuting

unapproved and counterfeit drug cases creates not just restitution for health care programs, but also serves important public safety purposes. One conviction can protect a large and vulnerable population of local cancer patients or put a nationwide ring of unapproved drug smugglers out of business.❖

ABOUT THE AUTHOR

❑**Andrew Lay** has been an Assistant United States Attorney since 1998, handling primarily Government fraud cases. Mr. Lay joined the Eastern District of Missouri in 2005. ✠

Chipping Away at a Threat to Our Military and National Security: The Trafficking of Counterfeit Semiconductors

Edward Chang
Assistant United States Attorney
District of Connecticut

I. Introduction

Fifteen years ago, when the U.S. Attorneys' Bulletin published an issue on the topic of enforcing intellectual property rights, the lead article presciently envisioned prosecutions that involved "counterfeit computer chips." *See* David Goldstone, "Deciding Whether to Prosecute an Intellectual Property Case," *U.S. Attorneys' Bulletin*, Mar. 2001, *available at* http://www.justice.gov/sites/default /files /usao/legacy /2006/ 06/30 /usab4902.pdf. That eventually came to pass in a pair of landmark prosecutions by the U.S. Attorney's Office for the District of Columbia, in *United States v. Wren*, No. 1:10 Cr. 245 (D.D.C. indictment filed Sept. 8, 2010) (*VisionTech*), and *United States v. Aljaff*, No. 1:09 Cr. 208 (D.D.C. indictment filed Aug. 21, 2009) (*MVP Micro*). Each case involved a U.S. company that was producing or trafficking in counterfeit semiconductors, some of which were being sold to the U.S. military or to defense contractors. In each case, the charges against the company's owner and other employees included trafficking in counterfeit goods, mail fraud, and conspiracy.

In 2011, Congress addressed the threat posed to military and national security interests by the ready availability of counterfeit electronic parts. The Senate Armed Services Committee conducted a hearing on counterfeit electronic parts in the defense supply chain, which culminated in a written report. *See* Committee on Armed Services, United States Senate, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, May 21, 2012, *available at* https://www.gpo.gov/fdsys/pkg/CRPT-112srpt167/pdf/CRPT-112srpt167.pdf. (Senate Report). Congress then re-drafted 18 U.S.C. § 2320, which prohibits trafficking in counterfeit goods, and added a new provision, with enhanced penalties, for trafficking in counterfeit military goods.

Since then, there have been several additional prosecutions involving the trafficking of counterfeit semiconductors, two of which included charges for trafficking in counterfeit military goods: *United States v. Yang*, No. 1:13 Cr. 305 (D. Md. indictment filed June 12, 2013), and *United States v. Picone*, No. 3:13 Cr. 128 (D. Conn. indictment filed June 25, 2013) (*Epic*). This article will provide background information and guidance for prosecutors who are handling these types of cases, including highlights of specific challenges and lessons learned.

II. The illegal trade in counterfeit semiconductors

Semiconductors, sometimes known as integrated circuits, are electronic components that are used for a broad spectrum of applications, ranging from ordinary personal devices, computers, and household appliances, to the most sophisticated scientific, industrial, and military systems and equipment. There are many kinds of semiconductors, including memory chips, specialized controllers, and general-purpose microprocessors. A manufacturer of semiconductors may produce semiconductors that share the same basic function, but are designed to operate in different environments. For example, a military-grade memory chip may be designed to operate properly in extreme temperatures that would damage or render inoperable a similar industrial- or commercial-grade memory chip.

Semiconductors, of course, are critical components in military systems and equipment. One variant of the Joint Strike Fighter, for example, contains more than 3,500 semiconductors. *See* Senate Report at 1. Although military systems are often expected to operate for decades, the production lifecycle for semiconductors and other electronic components can be as short as 18 months. *Id.* at 9 (reporting that nearly 800,000 electronic components have gone out of production in the last decade). As a result, the military, and its contractors and suppliers, often must rely on a secondary market for semiconductors, especially for semiconductors that are no longer produced by the original manufacturer, either to maintain older systems and equipment or to assemble new systems and equipment from older designs.

Semiconductors in the secondary market can be new, originating from existing inventory, or they can be used and/or refurbished, having been salvaged from discarded electronic equipment. Such discarded equipment, sometimes known as "e-waste," often makes its way to China, where it may be "disassembled by hand, washed in dirty rivers, and dried on city sidewalks." *Id.* at 6. Even if a salvaged component initially performs, it may have suffered latent damage from excessive heat or electro-static discharge while being detached from a circuit board. *See id.* at 7. There is no way to predict how well a salvaged component will perform, how long it will last, or what the impact of its failure will be. *See id.*

Semiconductors typically bear markings, which can include the name or trademark of the manufacturer, a part number, and a batch or a date code. Those markings can be altered— *i.e.*, a semiconductor can be "re-marked"—to make it appear as if the semiconductor were manufactured by a different company, on a different date or in a different batch, or to a higher grade or quality standard. For example, new markings can be applied to a semiconductor after the original markings have been sanded off. Alternatively, new markings can be applied after a thin layer of black epoxy has been used to cover the original markings, a process known as "blacktopping."

Counterfeit semiconductors have been found in the SH-60B Seahawk helicopter, the C-27J and C-130J cargo planes, the P-8A Poseidon airplane, and in mission computers for the THAAD missile system. *See id.* at 25-60.

III. Prosecutions involving counterfeit semiconductors

Prosecutions involving counterfeit semiconductors have generally involved charges for trafficking in counterfeit goods, if knowing use of a "counterfeit mark" can be established, or for mail or

wire fraud, if the evidence shows that false representations were made as to the semiconductors' history, quality, origin, or other characteristics.

A. Trafficking in counterfeit goods

A comprehensive primer on prosecuting offenses under 18 U.S.C. § 2320 can be found in section III of the Office of Legal Education's *Prosecuting Intellectual Property Crimes*, 4th ed. (IP Manual). In brief, to establish a substantive violation of 18 U.S.C. § 2320(a)(1), the government must establish each of the following elements:

- First, that the defendant trafficked in goods
- Second, that the defendant used a counterfeit mark in connection with those goods
- Third, that the defendant knew that the mark was counterfeit, and
- Fourth, that the defendant acted intentionally

B. Leonard B. Sand, 3 Modern Federal Jury Instructions ¶ 54A.01 (2015)

In establishing the second element, prosecutors (and agents) are generally advised to consult with the victim, *i.e.*, the owner of the trademark. *See* IP Manual at 108-09. This is especially critical in cases involving counterfeit semiconductors because semiconductor manufacturers have access to information and expertise that is not readily available elsewhere.

In many cases, the counterfeit nature of a semiconductor can be discerned based solely on a visual examination. Semiconductors routinely bear markings, including the manufacturer's trademark, a part number, and a date code or batch code. Manufacturers maintain databases with production history records that can be used to identify counterfeits based on these markings—for example, a semiconductor that shows a date code after the manufacturer stopped producing the part is obviously counterfeit. In the photograph shown below, which was used in the *VisionTech* case, the semiconductor manufacturer Analog Devices, Inc. (ADI) annotated the photograph of a semiconductor obtained through an undercover buy to show why the semiconductor was known to be counterfeit:

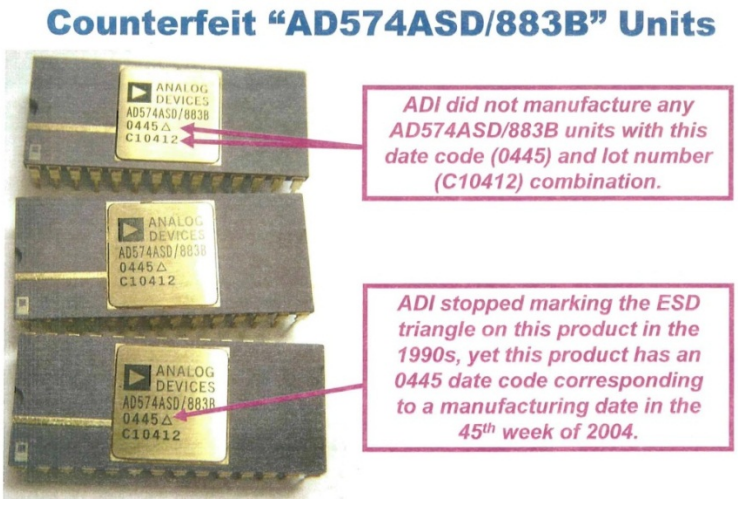

Figure 1: Excerpt from Government's sentencing memorandum in *VisionTech*

Semiconductors that are likely to be counterfeit can also be identified by the presence of sanding marks, by evidence of "blacktopping," or by poorly copied trademarks.

In cases where a visual inspection is inadequate, there are a variety of techniques that semiconductor manufacturers can use to identify counterfeits, including acetone testing, decapsulation (de-capping), and X-ray analysis. A description of these techniques is included in the appendix to the Senate Report.

When working with industry sources, prosecutors should be aware that the term "counterfeit" is generally used more broadly than the term "counterfeit mark" under 18 U.S.C. § 2320(a)(1). In other words, a semiconductor that is described as "counterfeit" may be characterized as such for a variety of reasons, including markings that are inconsistent (like the ADI semiconductor shown above). Although it may require only the smallest leap of inference to jump from a fraudulent date code to the conclusion that the trademark itself is spurious, it may be more prudent to secure direct testimony or evidence of that critical fact. *Cf. United States v. Cone*, 714 F.3d 197, 205-11 (4th Cir. 2013) (holding that alteration of underlying product was insufficient to sustain conviction where trademark itself was not shown to be spurious).

In establishing the third element, the government must prove that the defendant knew the mark in question was counterfeit, or was at least willfully blind to that fact. *See United States v. Zayyad*, 741 F.3d 452, 463 (4th Cir. 2014). As usual, evidence of knowledge may be direct or circumstantial, including repeated purchases from questionable suppliers, a history of customs seizures, unusually low prices, or trafficking in merchandise of obviously shoddy quality. *See generally* IP Manual at 122-24.

In the context of counterfeit semiconductors, prosecutors can also hope to find circumstantial evidence of knowledge from two additional sources: (1) falsified test reports or certificates of conformance, and (2) industry reporting. As to the first, purchasers of semiconductors on the secondary market are increasingly aware of the need to protect against counterfeits and have been asking vendors to provide test reports or certificates of compliance for the products they sell. In response, traffickers in counterfeit semiconductors have been producing fraudulent documentation, as seen in *VisionTech* (falsified certificates of compliance signed by non-existent "Quality Representative"), *MVP Micro* (falsified certificates of compliance allegedly signed by "lowest paid employee [who] reportedly spent most of his days at work smoking marijuana"), and *Epic* (falsified test reports from non-existing test laboratory).

A second potential source of evidence is industry reporting. Industry reports concerning suspected counterfeit parts are collected by the Government-Industry Data Exchange Program (GIDEP) and by industry associations such as ERAI (formerly known as Electronic Resellers Association International). The reports can be used to identify customers of a company that is suspected of trafficking in counterfeit parts in order to ascertain, for example, how the company responds to its customers when its products are found to be counterfeit.

As a practical matter, however, prosecutors should be cautious about relying too heavily on circumstantial evidence of knowledge when it comes to counterfeit semiconductors because the widespread availability of counterfeits in the secondary market provides a ready and obvious basis for a plausible defense. This lesson was made clear in *Zayyad*, a case involving counterfeit pharmaceuticals. In Zayyad's initial prosecution, the defense was able to secure testimony from government witnesses about "gray market" pharmaceuticals, *i.e.*, drugs purchased overseas that were then re-sold in the United States. *See* 741 F.3d at 457. The jury deadlocked, resulting in a mistrial, but a second jury returned a guilty verdict on "the same basic evidence" of knowledge after Zayyad failed to introduce evidence of the gray market during his re-trial. *Id.* at 457-58. In short, circumstantial evidence may be helpful in establishing probable cause for warrants and the like, but direct evidence of knowledge would be much preferred if the case ends up before a jury.

C. Mail fraud and wire fraud

As noted previously, the term "counterfeit" is generally used more broadly than the term "counterfeit mark"; indeed, to some, it even includes "previously used parts that are made to look new, and are sold as new." Senate Report at 1. It is not a violation of 18 U.S.C. § 2320, however, to sell refurbished semiconductors. *See generally* IP Manual at 133-34 ("Congress carefully considered 'gray market' goods and intended that those who traffic in them not be prosecuted.").

An appropriate charge to consider when semiconductors are falsely sold as new, or falsely described as originating from a certain country or as having certain characteristics, may be mail fraud or wire fraud.

IV. Prosecutions involving counterfeit military goods

When prosecuting a case involving counterfeit semiconductors that are falsely identified as military-grade, or are intended for use in a military or national security application, consideration should also be given to charging the defendant under 18 U.S.C. § 2320(a)(3). The elements of the offense are:

- First, that the defendant trafficked in goods
- Second, that the defendant knew that such goods were counterfeit military goods
- Third, that the use, malfunction, or failure of such goods was likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or to national security, and
- Fourth, that the defendant acted intentionally

Pattern Jury Instructions (Criminal Cases) for the Fifth Circuit, § 2-90C (2015). A conviction under § 2320(a)(3) carries higher maximum penalties, as well as an offense-level enhancement under the Sentencing Guidelines. *See* U.S.S.G. § 2B5.3(b)(7) (2015).

Section 2320(a)(3) can be thought of as "an enhancement of the traditional § 2320(a)(1) 'counterfeit goods' charge" with two added requirements. *See* IP Manual at 127. The added requirements are: (i) that the counterfeit goods are falsely identified as military-grade or are intended for use in a military or national security application, and (ii) that the use, malfunction, or failure of the goods would likely cause one or more enumerated harms.

Yang and *Epic* have been the only two cases prosecuted to date involving counterfeit military goods, and both were resolved through guilty pleas to one count of conspiracy to violate section 2320(a)(3). Nevertheless, it is clear that the first of the added requirements is rather easy to satisfy, as every prosecution involving counterfeit semiconductors thus far has included an allegation that some of the semiconductors were either military-grade or destined for the military (and that the defendant or defendants knew of that fact).

The second added requirement—likelihood of a serious consequence—could be more challenging to establish. Given an arbitrarily-selected counterfeit semiconductor used by the military, there could be more than 100 different weapon systems, *see* Senate Report at 63, that would have to be evaluated to determine the consequences if the semiconductor malfunctioned or failed.

A more pragmatic approach, given a company that is known to traffic in counterfeit military components, would be to identify a suitable component, *i.e.*, one whose malfunction or failure in an identified system or application would have a known, serious consequence, and to pursue an undercover

purchase of that component from the company under investigation. Done in that way, it would be relatively easy to prosecute the case under the new provision concerning counterfeit military goods.

V. Conclusion

This article has focused on protecting the military supply chain, but there are obviously consumer applications—both today and in the easily-imagined, near future—where counterfeit semiconductors would present an obvious danger. *See, e.g.*, Adrienne LaFrance, *The High-Stakes Race to Rid the World of Human Drivers*, THE ATLANTIC (Dec. 1, 2015). Strong criminal enforcement of 18 U.S.C. § 2320 is an important tool that prosecutors can use to ameliorate that risk. ❖

ABOUT THE AUTHOR

❑**Edward Chang** is an Assistant United States Attorney in the District of Connecticut. He has been involved in several investigations and prosecutions involving counterfeit semiconductors and has a deeply-rooted fear of autonomous vehicles. ✠

Intellectual Property Enforcement Programs: Helping State and Local Law Enforcement Combat Intellectual Property Crime

Kristie Brackens
Senior Policy Advisor
Office of Justice Programs
Bureau of Justice Assistance

I. Introduction

As stated by President Obama, "our single greatest asset is the innovation and the ingenuity and the creativity of the American people. It is essential to our prosperity, and it will only become more so in this century." *Remarks by President Barack Obama at the Export-Import Bank Annual Conference*, FEDERAL NEWS SERVICE TRANSCRIPTS, Mar. 11, 2010, *available at* 2010 WLNR 27821275. However, this crucial asset is threatened by the increasing perpetration of illegal and damaging acts of intellectual property theft. Not only do these crimes cost the U.S. economy tens of billions of dollars per year, deprive individuals of their livelihoods, and pose a public health threat, but research has shown that intellectual property crimes are closely related to, and support, other crimes, including violent crime. A report by the Rand Corporation found that:

> Counterfeiting is widely used to generate cash for diverse criminal organizations. In the case of DVD film piracy, criminal groups are moving to control the entire supply chain, from manufacture to distribution to street sales, consolidating power over this lucrative black market and building substantial wealth and influence in virtually every region of the globe. Counterfeiting is a threat not only to the global information economy, but also to public safety and national security.

Film Piracy, Organized Crime, and Terrorism, RAND CORPORATION, 2009, *available at* http://www.rand.org/pubs/monographs/MG742.html.

In February 2010, then-Attorney General Eric Holder announced the formation of the U.S. Department of Justice (DOJ) Task Force on Intellectual Property as part of a Department-wide initiative to confront the growing number of intellectual property (IP) crimes. "The rise in intellectual property crime in the United States and abroad threatens not only our public safety but also our economic wellbeing. The Department of Justice must confront this threat with a strong and coordinated response," said Holder. Press Release, Office of the Attorney General, Justice Department Announces New Intellectual Property Task Force as Part of Broad IP Enforcement Initiative (Feb. 12, 2010), *available at* http:// www.justice.gov/opa/pr/justice-department-announces-new-intellectual-property-task-force-part-broad-ip-enforcement.

In coordination with the DOJ Task Force on Intellectual Property, the Office of Justice Programs (OJP) initiated the Intellectual Property Theft Enforcement Program (IPEP) in 2009. The program is designed to build the capacity of state and local criminal justice systems to address criminal IP enforcement through increased prosecution, prevention, training, and technical assistance availability. The program is administered by the Bureau of Justice Assistance (BJA), a component of OJP.

II. Three-prong approach

Since the inception of the program, OJP has awarded $22,077,022 in the IP Theft Enforcement Program, which is informed by Section 404 of the *Prioritizing Resources and Organization for Intellectual Property Act of 2008* (PRO IP Act). Pub. L 110–403, §122 Stat 4256 (2008). This legislation authorizes OJP to make grants to eligible state or local law enforcement entities for training, prevention, enforcement, and prosecution of intellectual property theft and infringement crimes. Under the program, grant recipients establish and maintain effective collaboration and coordination between state and local law enforcement, including prosecutors and multijurisdictional task forces, and appropriate federal agencies, including the FBI and United States Attorneys' offices (USAOs). The information shared under the program includes information about the investigation, analysis, and prosecution of matters involving IP offenses as they relate to violations of state and local criminal statutes. State and local enforcement agencies have received $16,785,348 in federal support. Dept. of Justice, PRO IP Act Annual Report (2014) *available at* http://www.justice.gov/iptf/file/477261/download.

In addition to supporting and increasing coordination and cooperation of enforcement efforts among federal, state, and local law enforcement entities, IPEP funds national training and technical assistance (TTA) and public education campaigns. The National White Collar Crime Center (NW3C) is the TTA provider for IPEP. TTA for state and local law enforcement focuses on supporting the training needs of the local IP sites and providing continuing education for the greater law enforcement community on promising IP crime investigative and prosecutorial practices, health and safety issues resulting from counterfeit products, negative economic ramifications of IP crime, and the connection between IP crime and organized crime, gangs, and terrorism.

Finally, the National IP Theft Public Education Campaign, launched in November 2011 in partnership with the National Crime Prevention Council (NCPC), seeks to raise the public's awareness of the impact of counterfeit and pirated products, change the widely accepted belief that purchasing

counterfeit and pirated products is not harmful, and reduce demand for counterfeit or pirated products by influencing the behaviors of at-risk consumers. The campaign is continuously updated and features television, print, and radio public service announcements, as well as Internet banners and videos.

III. Success of IPEP

IPEP has enhanced the capacity of jurisdictions across the United States to detect and respond to IP crimes in their communities. Since the program's inception, BJA has awarded over $16 million to fund over 41 local/state task forces, resulting in the arrest of 5,247 individuals for violation of IP laws, the disruption or dismantling of 2,844 piracy/counterfeiting organizations, and the seizure of $351,473,399 in counterfeit property, other property, and currency in conjunction with IP enforcement operations. Dept. of Justice, PRO IP Act Annual Report (2014) *available at* http://www.justice.gov/iptf/file/477261/download. In fiscal year (FY) 2014 alone, the 13 active local/state funded task forces arrested 634 individuals for violation of IP laws, served 213 local/state IP-related warrants, disrupted or dismantled 527 piracy/counterfeiting organizations, and seized $4,327,989 in counterfeit property, other property, and currency in conjunction with IP enforcement operations. *Id.* Most recently, the Los Angeles Police Department's Anti-Piracy Unit served 15 search warrants and arrested 24 individuals for IP-related crimes, and recovered over $4 million in evidence value. *Id.* The Anti-Piracy Unit received awards and recognition from the Underwriter Laboratory Corporation and the Emirate Intellectual Property Association. The Anti-Piracy Unit's enforcement action was aired on "ABC 20/20" and "Good Morning America" in May 2015. *Id.*

Figure 1. *Intellectual Property Theft Enforcement Grant Program*

OJP has seen similar success with the national training and outreach. In FY 2015, NW3C conducted training sessions for 198 attendees from 108 agencies in Atlanta, GA; Avon Park, FL; Boca Raton, FL; Bronx, NY; Carson City, NV; Gadsden, AL; Georgetown, TX; Hazard, KY; Helena, MT; Las Vegas, NV; Louisville, KY; Manchester, NH; Maywood, IL; Meriden, CT; Meridian, ID; Middletown, VA; Nashville, TN; New York, NY; Newark, DE; Philadelphia, PA; Phoenix, AZ; Pierre, SD; Ponoma, NY; Rancho Cordova, CA; San Diego, CA; San Francisco, CA; Sandy, UT; Santa Fe, NM; and St. George, UT. In order to improve their IP investigative and prosecutorial approaches, NW3C also conducted 6 tailored seminars for 181 attendees representing 79 agencies, and engaged in an additional 13 technical assistance visits involving 35 agencies with 137 participants.

Additionally, since launching in November 2011, the Department's National IP Theft Public Education Campaign has garnered more than $96.4 million in donated media, including more than 88,479 total airings on television in 209 of 210 nationwide markets, and 27,618 airings on radio. Dept. of Justice, PRO IP Act Annual Report (2014) *available at* http://www.justice.gov/iptf/file/477261/download. A total of 1,841 digital mall posters have been displayed in 43 nationwide markets. Print support for the campaign continues to be strong, adding another $412,000 in donated media for this past year. *Id.* The latest intellectual property theft PSA, "I'm a Phony," was featured on a digital billboard in Times Square, courtesy of the CauseWay Agency (which developed and produced the TV PSA) from September 7 – October 4, 2015. The total estimated donated media value of the Times Square digital billboard is $12,500. The total estimated impressions for the 4-week period were 1,849,860. *Id.*

Figure 2. *Intellectual Property Theft PSA*

Tracking research data indicates that the public education campaign is increasing public awareness of IP theft and is influencing more people to not purchase counterfeit products.

IV. Current IP sites

On October 2, 2015, Attorney General Loretta E. Lynch reaffirmed her commitment to confronting the growing number of IP crimes. "The digital age has revolutionized how we share information, store data, make purchases, and develop products, requiring law enforcement to strengthen

our defenses against cybercrime—one of my top priorities as Attorney General," said Attorney General Lynch. Press Release, Office of the Attorney General, Justice Department Announces New Strategy to Combat Intellectual Property Crimes and $3.2 Million in Grant Funding to State and Local Law Enforcement Agencies, (Oct. 2, 2015) *available at* https://www.fbi.gov/news/pressrel/press-releases/justice-department-announces-new-strategy-to-combat-intellectual-property-crimes-and-3.2-million-in-grant-funding-to-state-and-local-law-enforcement-agencies. Attorney General Lynch then announced the Department's IPEP FY 2015 new awards to state and local jurisdictions to cover expenses related to performing criminal enforcement operations; educate the public to prevent, deter, and identify criminal violations of IP laws; establish task forces to conduct investigations, forensic analyses, and prosecutions; and acquire equipment to conduct investigations and forensic analyses of evidence.

Award Number	Grantee	Amount
2015-ZP-BX-0001	City of Austin Police Department	$400,000
2015-ZP-BX-0003	City of Hartford Police Department	$399,545
2015-ZP-BX-0005	Cook County State Attorney's Office	$400,000
2015-BE-BX-0003	Baltimore County Police Department	$120,174
2015-ZP-BX-0004	North Carolina Department of Secretary of State	$367,076
2015-ZP-BX-0002	New Jersey State Police	$269,619
2015-BE-BX-0004	City of Phoenix Police Department	$253,129
2015-BE-BX-0005	City of Portland Police Department	$373,569
2015-BE-BX-0001	Virginia State Police	$253,128
2015-IP-BX-0012	City of San Antonio Police Department	$400,000

V. Conclusion

Intellectual property crime is not a victimless crime. Intellectual property crime takes away jobs from everyday citizens. It infringes on copyrights, thus suppressing innovation in the United States. Faulty products are made without safety standards. Improperly prepared counterfeit drugs often contain dangerous elements, such as antifreeze, floor wax, and even lighter fluid. Not only do these items jeopardize the health and safety of consumers, they are often used to fund dangerous or even violent criminal enterprises and organized crime networks. The continued investment of the Department into IPEP is helping state and local law enforcement agencies reduce the threat posed by intellectual property crime and increase public safety through enhancing their ability to aggressively investigate and prosecute intellectual property crime. ❖

ABOUT THE AUTHOR

❑**Kristie Brackens** is a Senior Policy Advisor in the Office of Justice Programs, Bureau of Justice Assistance. She leads the Violence Reduction Network that works to deliver customized training and technical assistance, and leverage assets across the Department of Justice to assist cities experiencing high rates of violent crime. Additionally, she oversees the Intellectual Property Enforcement Program that provides support to local and state IP task forces and aims to increase public knowledge on the dangers of intellectual property crime. She began her service with the Department in 2007 and is an adjunct faculty with the University of Phoenix. ✠