Published by *Intellectual Property Law360*, *International Trade Law360*, and *Competition Law360* on July 8, 2010.

What Counterfeiting Crackdown Means For IP Owners

Law360, New York (July 08, 2010) -- On May 6, 2010, the U.S. departments of Justice and Homeland Security announced the results of Operation Network Raider — a two-year law enforcement initiative targeting the illegal distribution of counterfeit network hardware manufactured in China.

The operation was astonishingly successful, resulting in 30 felony convictions and over 700 seizures of counterfeit Cisco network hardware and labels with an estimated retail value in excess of $143 million.

As John Morton, assistant secretary of homeland security for immigration and customs enforcement, explained, counterfeit and substandard computer hardware "pose a triple threat to our nation by stealing from our economy, threatening U.S. jobs and potentially putting the safety of our citizens at risk."

Commenting on the success of the operation, FBI assistant director Gordon M. Snow observed, "This [operation] illustrates how effectively the private sector and law enforcement organizations work together to combat fraudulent goods and preserve the integrity of U.S. computer networks and infrastructure."

Operation Network Raider provides just one example of an ever-growing trend — the coordination between law enforcement and private companies to invoke criminal law to enforce IP rights, particularly in situations in which health, safety or national security are implicated. As discussed below, this trend presents both significant opportunities, as well as some challenges for IP owners.

Making IP Crimes a Top Priority

The past nine months have seen a steady drumbeat of activity reflecting the Obama administration's commitment to aggressively prosecuting IP crimes. For example:

- On Sept. 25, Obama nominated Victoria Espinel as the first U.S. intellectual property enforcement coordinator, a position "charged with drafting an administrativewide strategic plan on intellectual property."

- On Feb. 12, Attorney General Holder announced the formation of the DOJ Task Force on Intellectual Property, chaired by acting Deputy Attorney General Gary G. Grindler, which will "identify and implement a multi-faceted strategy with our federal, state and international partners to effectively combat [IP crimes]."

- On Feb. 24, Holder, during a speech to the Rio de Janeiro Prosecutor General's Office, stated that the theft of IP "is a priority concern for President Obama and for me."

- On March 29, the DOJ's Office of Justice Programs, Bureau of Justice Assistance, announced its solicitation of applications for funding under the Intellectual Property Enforcement Program. Pursuant to this program, the OJB-BJA will award $4 million in grants to fund state, local and tribal criminal investigations, prosecutions, and prevention and education efforts related to IP enforcement.

- On April 26, 2010, the DOJ created 15 new assistant U.S. attorney positions within the Computer Hacking and Intellectual Property Program, and dedicated 20 additional FBI special agents to "combating domestic and international IP crimes."

- On May 3, Grindler stated in an op-ed piece in the National Law Journal that "aggressive intellectual property law enforcement is crucial to our continued success and safety, and is a top priority of the Department of Justice."

- On June 22, the IPEC released its 2010 Joint Strategic Plan on Intellectual Property Enforcement, identifying "33 enforcement strategy action items" reflecting "the U.S. government's coordinated approach to strengthening intellectual property enforcement."

Throwing the Book at Traffickers of Counterfeit Cisco Products

Among the 30 felony convictions arising out of Operation Network Raider were those of Ehab Ashor and Yongeai Li.

Ashor, a Saudi citizen residing in Texas, was the owner of a Houston-based entity specializing in the provision of technology goods and services to the federal government. The evidence at trial established that Ashor knowingly purchased counterfeit Cisco Gigabit Interface Converters from a China-based online vendor, intending to sell the GBICs to the U.S. Department of Defense for a computer network "used by the U.S. Marine Corps to transmit troop movements, relay intelligence and maintain security for a military base west of Fallujah, Iraq."

On January 22, 2010, a federal jury in the U.S. District Court for the Southern District of Texas found Ashor guilty of trafficking in counterfeit GBICs. On May 6, Ashor was sentenced to 51 months in prison and ordered to pay $119,400 in restitution to Cisco.

Li, a resident of China, was convicted in the U.S. District Court for the Central District of California of trafficking in counterfeit Cisco computer networking equipment. Operating through a China-based company, Li knowingly procured counterfeit Cisco products in response to orders received, ultimately shipping the counterfeits to the U.S.

On Sept. 17, Li pled guilty to trafficking in counterfeit Cisco computer networking equipment, and on Jan. 25, he was sentenced to 30 months in prison and ordered to pay $790,683 in restitution to Cisco.

These recent cases are not the first time traffickers of counterfeit Cisco products have been hit with stiff sentences. On July 30, 2008, Charles Lacy-Thompson was sentenced in the U.S. District Court for the Southern District of New York to 30 months in prison, and was ordered to pay $2.2 million in forfeiture to the U.S. for trafficking in computer equipment and packaging bearing counterfeit Cisco marks.

And more recently, on May 28, Robert Cimino of New York was sentenced in the U.S. District Court for the Eastern District of Virginia to 18 months in prison for manufacturing and distributing pirated software via the Internet, and ordered to pay $272,655 in restitution to the copyright owners.

Implications for IP Owners

The administration's commitment to combating IP crimes, and, more specifically, the DOJ's announcement that "[a]ggressive intellectual property law enforcement ... is a top priority," provides considerable opportunities for IP owners looking to law enforcement to assist them in combating counterfeiters.

The intensified enforcement environment may well make it more advantageous for an IP owner to package a criminal counterfeiting case for the government to prosecute, rather than pursue a civil action itself.

Alternatively, IP owners increasingly may seek to supplement their civil anti-counterfeiting strategies with parallel criminal actions. In any event, IP owners who are serious about exploiting all tools at their disposal should evaluate the potential advantages and disadvantages of incorporating criminal law enforcement into their anti-counterfeiting strategies.

Potential Advantages of Using Criminal Law to Enforce An IP Owner's Interests

The government possesses broad powers and extensive resources that no private civil litigant can match. If the U.S. Attorney's Office takes an interest in an IP crime — which is most likely if health, safety or national security interests are implicated — it can invoke its broad powers and formidable resources to help protect the IP owner's interests.

For instance, whereas civil litigants often get mired down in costly discovery practice, the U.S. Attorney's Office holds the power to issue grand jury subpoenas and obtain search warrants. These tools enable the government to acquire evidence that may never surface in a civil proceeding.

Federal criminal law also affords the victims of federal crimes, including IP owners harmed by criminal trafficking of counterfeit goods, with the right to timely restitution in the full amount of their loss.

Restitution orders may even require a counterfeiter to pay the victim's costs and expenses incurred in connection with its participation in the investigation or prosecution of the offense, including expenses incurred by forensic accountants, private investigators, outside lawyers hired to assist the prosecution, and the like.

Potential Disadvantages of Using Criminal Law to Enforce an IP Owner's Interests

Using law enforcement and criminal law to enforce an IP owner's interests is not without its potential pitfalls. First and foremost, upon turning over a matter to the government for prosecution, an IP owner typically relinquishes all control over the matter.

This may prove frustrating to an IP owner in the event the prosecutor adopts a different view of the case or how it should be prosecuted.

In addition, before bringing a case to the government, an IP owner would do well to take stock of its own conduct, and that of its employees, both generally and in connection with any investigation into the alleged criminal conduct.

The failure of an IP owner to maintain a clean house may not only irreparably tarnish the government's case, but it also may expose an IP owner to unanticipated criminal charges itself.

In the same vein, it is crucial to remember that, when dealing with the government, honesty is not only the best policy, but the law. Lying to an AUSA or a federal agent is a serious offense punishable by up to five years imprisonment.

Potential Advantages of Parallel Civil and Criminal Proceedings

Law enforcement prosecution of a criminal counterfeiter does not prevent an IP owner from also pursuing that counterfeiter in a parallel civil proceeding. Indeed, the Lanham and Copyright acts, as well as state and common law, provide civil IP complainants with many remedies, including injunctive and monetary relief against infringers and counterfeiters, not all of which are available to the victim in a criminal proceeding.

For example, a plaintiff in a civil counterfeiting action may be entitled to: (i) a temporary restraining order or preliminary injunction; (ii) an ex parte seizure of goods and records; (iii) an order freezing the defendant's assets to ensure the availability of final relief; (iv) an enhanced monetary award, including statutory damages of up to $2 million per counterfeit mark per type of goods sold; and (v) attorneys' fees.

A potential advantage in pursuing parallel civil and criminal proceedings is that the discovery obtained in the civil proceeding may be used by the prosecution in the criminal case and discussed with the victim without the restrictions imposed by grand jury secrecy or operational concerns.

In addition, although a victim's exchange of information with the AUSA generally is considered a one way street, the Touhy doctrine often makes it possible for a civil litigant to obtain the government's evidence. Such evidence may be otherwise unobtainable by a civil litigant, and, therefore, can prove extremely valuable.

Potential Disadvantages of Parallel Civil and Criminal Proceedings

There are some potential disadvantages to pursuing parallel civil and criminal IP actions. Most significantly, the government may obtain a stay of the civil litigation, perhaps to limit the criminal defendant's ability to compel discovery, which the government may believe will interfere with the criminal matter.

Also, in certain instances, a criminal defendant may obtain a stay of a parallel civil proceeding. Such a stay would bring the parallel civil action to a halt, regardless of how far the action may have progressed.

Even if the civil action is not stayed, an IP owner pursuing a parallel civil proceeding may face certain obstacles in discovery. For instance, an IP owner may be prevented from effectively obtaining discovery from the government's not-yet-sentenced cooperating witnesses.

Moreover, there is a risk that the actions of an IP owner, or its private counsel and investigators, in a parallel civil proceeding may adversely impact the criminal case, possibly rendering a potential criminal action less attractive to the AUSA, or worse yet, tarnishing a pending criminal investigation or proceeding.

Packaging a Case for the U.S. Attorney's Office

An IP owner who decides to seek the assistance of law enforcement in combating a counterfeiter must package the matter in such a way as to make it attractive to the U.S. Attorney's Office.

When bringing a counterfeiting case to the government, an IP owner should explain and emphasize how the particular matter falls within the U.S. Attorney's Office's or DOJ's announced priorities — including IP crimes that implicate health, safety or national security concerns.

Counsel for an IP owner should be prepared to explain the strength of the case and the quality of the investigation conducted, as well as address the government's likely concerns about the presence of

any bias, the availability of corroboration, the proper preservation of documents and other evidence, and the segregation of potential witnesses.

Many of these concerns may be diminished when the matter has been investigated and presented to the government by an experienced former prosecutor familiar with the rules of criminal procedure and evidence.

--By Marcus A. Asner (pictured), Louis S. Ederer and Matthew T. Salzmann, Arnold & Porter LLP

Marcus Asner and Louis Ederer are partners at Arnold & Porter in the firm's New York office. Matthew Salzmann is an associate in the firm's New York office.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients or Portfolio Media, publisher of Law360.