

# Connecticut **LawTribune**

MAY 17, 2010  
VOL. 36, NO. 20 • \$10.00

An ALM Publication



CTLAWTRIBUNE.COM

## KNOCK IT OFF

IP attorneys hope feds send message to counterfeiters

By DOUGLAS S. MALAN

It takes little effort for consumers to get their hands on the hottest designer fashion items these days. There's no shortage of web sites where these products are literally just a click away.

But depending on the web site, there's no guarantee that the product is legitimate. And transactions involving counterfeit goods are a major headache for companies and their attorneys.

"The simple volume of people of people marketing these [counterfeit] products and wanting to buy these products makes it impossible to eradicate," said Curtis Krechevsky, a trademark and copyright law partner at Cantor Colburn in Hartford.

But it's not just counterfeiting that's worrisome to businesses.

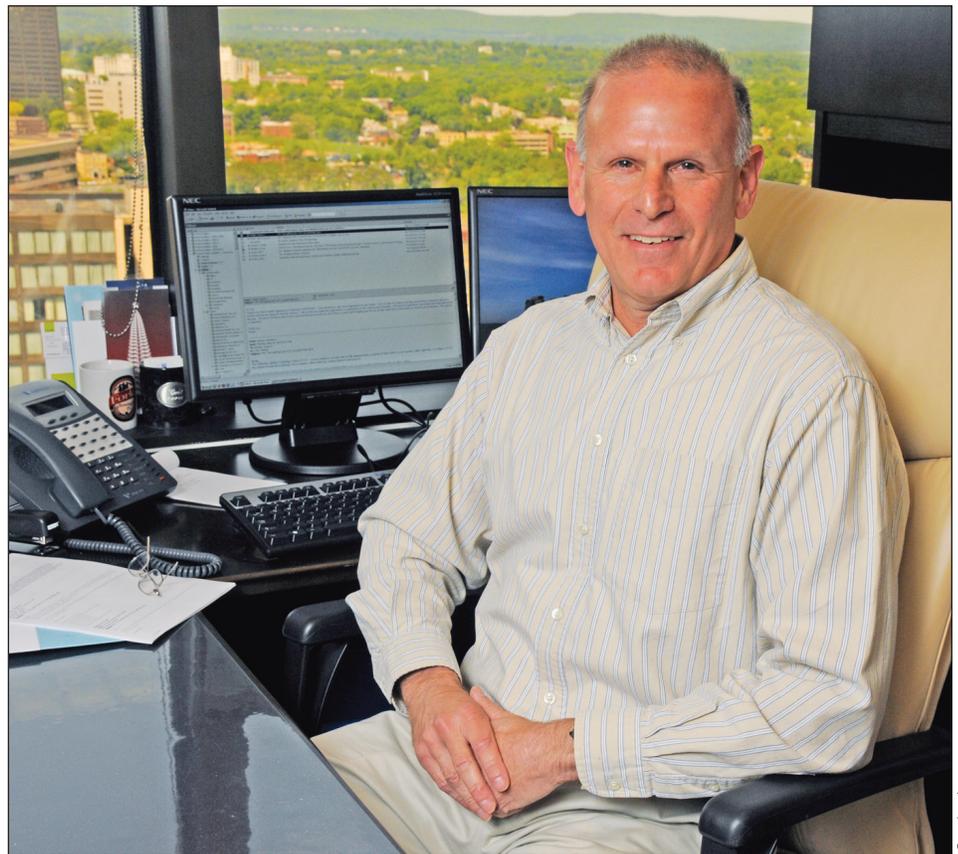
There's concern about the loss of trade secrets from computer hackers or employees who leave the company. And piracy of digital music, movies and software remains an ongoing threat for some companies.

A congressional report released earlier this year revealed that U.S. officials alone seized more than \$73 billion in counterfeit goods between 2004 and 2009, and the study doesn't include the value of pirated digital products.

"Increasingly, the value of U.S. businesses is found in their intellectual property," said Jonathan B. Tropp, a Stamford-based litigator at Day Pitney who focuses on IP cases. "Protecting that value is more important than ever."

The Department of Justice responded to that sentiment in late April when it added 15 new assistant U.S. attorneys and 20 FBI agents to focus on IP crimes in the department's Computer Hacking and Intellectual Property program.

The 15 new prosecutors will be spread among Washington, D.C., Pennsylvania, New Jersey, New York, Massachusetts and Califor-



Gary Lewis

**Attorney Curtis Krechevsky said private companies welcome the addition of federal agents to combat IP crimes because online retailers of counterfeit goods are difficult to identify and trace.**

nia. The FBI agents will be centered in Washington, D.C., New York, San Francisco and Los Angeles, but will not be limited to cases in those four cities. Previously, there were about 30 federal agents dedicated to IP crimes nationwide.

In Connecticut, Assistant U.S. Attorney Edward Chang is part of the Justice Department's national Computer Hacking and Intellectual Property Unit and has handled IP cases involving software piracy and tampering with trade

secrets. A spokesman for the Connecticut U.S. attorney office said some of the new agents appointed to investigate IP crimes will cross into Connecticut to assist with investigations as needed.

"Intellectual property law enforcement is central to protecting our nation's ability to remain at the forefront of technological advancement, business development and job creation," said Acting Deputy U.S. Attorney General Gary Grindler in a statement.

## Conducting Raids

Krechevsky said the explosive growth of the Internet has made IP crimes easier to carry out. A decade ago, for instance, someone interested in purchasing counterfeit goods would go to certain areas of New York City known as hot spots for buying knock-off merchandise.

While those locations still exist, sellers can now set up web sites in a matter of hours registered using fake names and contact information, making them harder for authorities to identify and trace.

Additionally, the Internet “has lowered the transaction cost,” Krechevsky said. “[Sellers] don’t have to keep as much inventory on hand. They can have their suppliers on tap and fill orders as they’re made.”

And these illicit operations can be based anywhere in the world. “It gets very tough to find culpable parties,” Krechevsky said. “You can and should be able to have the government help you go after these people.”

Krechevsky spent 13 years as in-house counsel with sneaker manufacturer Reebok before going into private practice in 2000. He said Reebok goes to great lengths to deter counterfeiters from selling knock-off versions of their shoes. As an in-house lawyer, Krechevsky set up raids in which undercover investigators posed as buyers arranging deals with known suppliers of counterfeit sneakers. Entire cargo containers full of knock-offs would arrive in a port city to be delivered to the undercover investigators. The investigators arranged for celebratory meetings at local hotels with the supplier’s representatives in the U.S.

Law enforcement officials would have the hotel room bugged, monitoring next door, and then burst in to make arrests when they had the incriminating evidence they needed.

“A few of those and you get people’s attention,” Krechevsky said.

With online counterfeit operations, companies are able to shut down web sites selling fake goods by filing complaints with the Internet Corporation for Assigned Names and Numbers. That is a non-profit corporation that works with the U.S. Department of Commerce to manage the assignment of domain names and IP addresses.

But new online outlets for the fake goods can pop up overnight, and the web site owner usually can’t be tracked down quickly. “It’s like the old Whac-A-Mole game,” Krechevsky said. “You knock out one site and another appears. But you have to do something.”

A recent landmark court case in this area could have put the squeeze on counterfeiters who use auction sites to sell their goods.

High-end jeweler Tiffany Co. sued eBay, claiming that the online auction site knew



Gary Lewis

some of its auctions included counterfeit Tiffany jewelry. The jeweler believed eBay should have done more to stop those transactions, from which eBay profited.

But in April, the 2<sup>nd</sup> Circuit Court of Appeals affirmed a New York trial court’s decision that the burden was on Tiffany to identify and alert eBay to auctions involving counterfeit merchandise. Once alerted, eBay must take steps to remove the auction.

The decision was considered a setback to businesses in the fight against IP crime.

“[Businesses] still have to do the self-help,” Krechevsky said, which can be expensive. “But if the government dedicates resources to enforce the laws, as they’ve done now, you offload some of those costs.”

Depending on the offense, IP crimes prosecuted in the U.S. can carry multi-year prison sentences and fines reaching into the millions. Laws also allow for the seizure of inventory and the means of creating that inventory.

But not all misuse of intellectual property is considered criminal. Patent infringements, for example, generally do not carry criminal penalties.

## Piracy And Secrets

Eric Osterberg, an IP litigator in the Stamford office of Fox Rothschild, has handled some counterfeiting cases in his career, though none big enough to get the government involved. But many of his clients in the music and publishing industries are more worried about piracy.

“There’s a general concern that IP needs to be moved up on the hierarchy of worries on the criminal side,” Osterberg said. More investigative and prosecutorial muscle in the government is a welcome change, he added, but he’s not convinced it will be effective.

“I’ll take a let’s-see approach,” he said. “[IP crimes] are a big problem. I don’t know if this will be enough to make a noticeable difference.”

Brian Roche, of Roche Pia in Shelton, serves as Connecticut counsel for software giant Microsoft and has been involved in dozens of lawsuits filed against people who allegedly sold pirated versions of Microsoft’s products.

“The digital products such as movies, music and software continue to be a favorite target,” he said, mainly because the cost to copy and re-distribute the material is low.

Another growing area of his firm’s practice is cracking down on trade-secret theft, and it normally doesn’t involve a sophisticated scheme where a third party hacks into a company’s computer system to steal information. “We do a lot of work combating trade secret abuses, usually involving former employees going to competitors,” Roche said.

In many of these cases, Roche’s clients will investigate online activities of former workers during the final days of their employment. That often leads to forensic analyses of laptops and other company-issued electronic devices to determine if any privileged information was transmitted outside the company.

Clients also look for evidence that workers copied sensitive information onto small, portable hard drives. “That type of activity likely would lead to a lawsuit,” Roche said, adding that his firm has a few of those cases going on now.

In the past, companies have chosen to file civil lawsuits against people who steal their intellectual property, especially with the government focusing resources on counterterrorism and Internet crimes such as child pornography and financial scams, Roche said.

But the government now appears serious about fighting IP crimes against businesses, he said. “Private industries won’t have to carry the ball with a civil prosecution when a criminal prosecution is possible,” Roche said. “It’s not like the government hasn’t been taking on these cases, but now there appears to be a real focus on it.”