IP LAW & BUSINESS
iplawandbusiness.com

FEATURE

Policing the Internet

Helping trademark owners to fight counterfeiters on the Internet is a growth business for law firms and consultants alike.

By Xenia P. Kobylarz
IP Law & Business/June 2007

Reprints & Permissions

On the Internet, no one knows if you're a dog. Or a well-tailored investigator in the London office of Covington & Burling. That fact has guided Peter Anaman's entire career over the last seven years. The 33-year-old British-trained law school grad is the head of Covington's Internet monitoring and investigation unit, and he uses multiple online personas to nail bad guys: sellers of counterfeit goods and pirated software, hackers, phishers, you name it.

One time Anaman was hired by several software companies to investigate a group of Lithuanian students who were suspected of selling some 2,000 different pirated software programs for $10-$20 apiece on the Web. For years the group had eluded Lithuanian police. Anaman, a 6-foot-plus lieutenant reservist in the French Army, managed to infiltrate the ring in a matter of months by pretending to be a flirtatious 27-year-old female programmer who complained a lot about her boss in online chat rooms. After a few months, he was able to befriend members of the group and obtain encryption codes and other personal information while chatting with them online. The information helped the software companies to shut down the Web sites and led to the arrest of the pirates. "I help send people to prison, and they don't even know me," Anaman says.

The rise of the Internet as a major place of commerce has been both a curse and a boon to owners of brands and other intellectual property. Online business sales are booming, but so are the sales of fake goods and pirated software. Though estimates of the size of the problem vary, all agree it's big. One estimate posits that 14 percent--or $84 billion--of last year's $624 billion global counterfeit trade was derived from Internet sales. MarkMonitor, a provider of online brand protection, projects that Internet counterfeit and piracy sales will soar to $119 billion this year.

As a result, Internet policing has become a major cost of doing business for many companies. Last year the six major movie studios in the United States spent an estimated $40 million on countermeasures to foil illegal downloads of movies. Some individual luxury brand owners such as Tiffany & Co. spend well over $1 million annually tracking and pulling down counterfeit auctions from different auction sites. Where once companies relied on a a few retired law enforcement agents and private detectives, the immensity of the problem has led businesses to hire Internet-savvy professionals like Anaman, and to a burgeoning field of consulting and enforcement firms. "The Internet has changed the way bad guys do their business," says Harley Lewin, head of Greenberg Traurig's global brand enforcement practice. "It now takes enormous effort and resources to track down and identify counterfeiters. They could be anyone and be anywhere in the world."

Some law firms have chosen to enter full bore into Internet enforcement, both as a new line of business that generates legal work and as a way to serve existing clients. Covington, for instance, offers a full-service Internet monitoring and enforcement staff that includes 24/7 online brand monitoring, Internet investigators, and enforcement and litigation support. Evan Cox, the partner in charge of the group, says that the firm originally created the department to assist business software clients in online piracy investigations. It has since expanded to include monitoring and investigating other cybercrimes, such as phishing and virus attacks. Its clients include financial institutions, pharmaceutical companies, and online security companies.

The daily routine of a cyber-investigator is quite different from that of a typical lawyer. In London, Anaman regularly eavesdrops on chat rooms and message boards where software hackers and coders go, as a way of keeping his pulse on the community. There he finds out if, say, an ambitious teenager is attempting to decode the encryption of a software program or plans to release a counterfeit product before the bona fide version has been launched.

However, much of his time is spent notifying auction sites, such as eBay and iOffer, that counterfeit or pirated products are up for sale on their sites and asking them to take down the auctions and put a stop to the sale. He then searches for contact details of sellers in order to send them warning letters. The responsibility of the auction sites themselves is a key legal question that is being argued out in many courtrooms around the world [see "Looking for Deep

Pockets"].

But until the law is settled, companies protecting valuable intellectual property have no other option but to take on the enormous burden of policing the Internet auctions themselves. For instance, the two-lawyer IP team at Los Angeles-based jeans maker 7 For All Mankind manages to knock down 10,000 auctions off eBay every month, according to general counsel Barbara Kolsun. "We work very hard," she says, while using a consultant to do the lion's share of the online monitoring.

The software and entertainment sectors have grown quite savvy in foiling would-be online infringers. The movie studios and music labels, for example, have deployed file sharing software that is designed to disrupt file searches and downloads on peer-to-peer networks such as LimeWire and Gnutella. But many luxury goods companies are simply relying on software designed to help them automate the process of tracking down fakes and other trademark abuses online. Lawyers say that using technology is just the very first step in stopping offenders. "At the end of the day, all you get is this huge report and a lot of information," says Lewin of Greenberg Taurig.

And it's not just the auction sites causing the problems. In December The McGraw-Hill Companies, Inc.'s education unit enlisted Covington's help in taking down seven Russian Web sites that were selling scanned copies of hundreds of McGraw-Hill's books. Covington's group discovered three more infringing Web sites hosted by three different Internet service providers based in Russia. Within a week, almost all of the Web sites were shut down after Covington contacted the ISPs hosting the sites. Shutting down the other sites required more investigation, according to Lisa Peets, Covington's London partner in charge of the case. "We found out that the people operating the sites were connected to the largest organized crime group in Russia, and the ISPs knew what was going on," she says. Peets's group finally located and took down the group's central file server. The investigation is still under way for possible criminal and civil litigation. McGraw-Hill has since retained Covington to conduct ongoing Internet monitoring and enforcement actions. The company is also continuing to do some monitoring in-house, according to associate general counsel Suzanne Tesley.

As fast as the business of Internet investigations is growing, some service providers-naturally--think that it should be growing faster. "There are some Fortune 500 companies that still don't have an Internet policing program," says Rob Holmes, president of icybercrime.com, a ten-year-old company that conducts online counterfeiting investigations. "I guess some businesses don't see the return on investment," Holmes says. "They think that for every ten counterfeiters they stop, there are a dozen more that pop up, so why bother?" Monitoring and enforcement companies try to convince corporations to allocate resources by documenting their tally of the seizure of counterfeit goods and of favorable court judgments.

Online monitoring and enforcement is more an art than a science, says Karen Kitterman, a trademark partner at Fenwick & West in Mountain View, California, who handles auction monitoring for many of the firm's technology clients. She advises against relying on automated software that sends cease-and-desist letters by the hundreds. Sending a threatening letter that makes the client sound overly zealous is a no-no, she says. "We send each demand letter with the client's reputation in mind, knowing our letter could be posted on blogs around the world. Or appear in the evening news," she notes. "Trademarks are symbols of goodwill, so while we enforce trademarks and copyrights on the Internet, we also seek to enhance the client's goodwill in the Internet community."

It's also important not to cry wolf. Sending take-down notices for content that isn't really infringing is a quick way to lose credibility with ISPs and auction sites, notes Covington's Anaman.

But practitioners say the job of protecting IP online may soon get even more difficult and expensive. Political pressure is building from privacy advocates and the general public to push back and outlaw tools and methods that Internet investigators have often used to identify online offenders. For instance, Anthony Keats, a partner at IP boutique Keats MacFarland & Wilson in Los Angeles, points to a California legislative proposal that would prohibit impersonations, fictitious or fraudulent statements, and false representations to obtain personal information--so goodbye to Anaman's flirtatious programmer in that jurisdiction. Meanwhile, an international council that oversees domain name registration is expected to soon change its policies to give more privacy to people who put up Web sites.

Another worrisome trend is the migration of online counterfeiters to countries with less established IP laws, such as China. China now has five auction sites and more than 800,000 Web sites. Internet use among Chinese citizens is exploding.

But the tactic by trademark owners of asking ISPs to take down offending sites, which usually works in the U.S. and Europe, is often futile in China. Hong Kong-based Baker & Mc-Kenzie partner Loke Khoon Tan says that of the 67 Web sites he tried to shut down recently on behalf of a luxury brand client, 16 were taken down, six Web sites removed infringing content, and 45 are

still in operation.

"I expect to see a lot more Internet infringement litigation," says Tan. "This will be a growth area for law firms in China."

Copyright © 2007 ALM Properties Inc. All rights reserved.