CORPORATE counsel

ALM Properties, Inc.
Page printed from: *Corporate Counsel*

Back to Article

Don't Blame China for Trade Secrets Theft

IP Insider
When it comes to stolen trade secrets and digital espionage, the culprits are more likely to be homegrown.

Jan Wolfe
Corporate Counsel
December 22, 2011

Consider the following two court cases involving Motorola's claimed trade secrets:

The first is the criminal espionage prosecution of software engineer Hanjuan Jin. When she quit her job at Motorola, Inc.'s offices outside Chicago in 2007, Jin took with her two bags full of confidential company documents, according to the U.S. Department of Justice. She then tried to board a plane for her native China with more than 1,000 Motorola documents and a one-way ticket in hand. Had U.S. Customs agents at O'Hare Airport not stopped her, Jin would have sold Motorola's trade secrets to a Chinese rival, prosecutors allege. At press time a federal district court judge was mulling a verdict. Jin, a naturalized U.S. citizen, maintains her innocence.

The second is Motorola's drawn-out trade secrets fight with Lemko Corp., a small crosstown rival founded by former Motorola employees. Motorola sued Lemko's founders in 2008, claiming that they assisted Jin in her ill-fated caper. In 2009 Motorola amended its original complaint to add new allegations that Lemko's founders themselves stole confidential trade secrets when they left Motorola years earlier. In November, Lemko execs fired back with a lawsuit accusing Motorola of making frivolous allegations in order to destroy their reputations. They named Motorola's senior corporate counsel Jeffrey Johnson and his outside lawyers at Nixon Peabody as defendants in the case. A week later, Lemko turned the tables further, alleging in a separate complaint that Motorola stole its trade secrets when it hired away a Lemko engineer.

Jin's dramatic espionage charges have garnered considerable media attention, and for good reason. They underscore the U.S. government's recent crackdown on IP theft by the Chinese government and related businesses, which a government agency called "the world's most active and persistent perpetrators of economic espionage" in a recent report. In 2010 the Justice Department hired 15 assistant U.S. attorneys and 20 Federal Bureau of Investigation agents to focus exclusively on IP crimes. They secured guilty pleas from Chinese scientists at some of the United States's most innovative companies, including Ford Motor Company, Dow AgroSciences LLC, and E.I. du Pont de Nemours and Company.

But, without diminishing the seriousness of Chinese economic espionage, IP lawyers say the Lemko subplot is more representative of trade secrets litigation for most U.S. companies. "Incidents involving China grab most of the headlines," says Darin Snyder, a partner in O'Melveny & Myers's San Francisco office specializing in trade secrets litigation. Far more common than Chinese spying, he says, is employees taking trade secrets with them when they move to a new company, often a start-up looking to gain ground on more established rivals. "It happens that China has been the fastest-growing economy in the world and has thousands of up-and-coming businesses," he says.

"Day in and day out, changing jobs occurs at a much higher volume than true economic espionage," agrees Russell Beck, a partner at Beck Reed Riden who teaches trade secrets law at Boston University School of Law. The "vast majority" of Beck's trade secrets cases involve employees moving between domestic competitors, he says.

Beck breaks down his enforcement practice like this: A significant number of cases involve employees or business partners stealing data for their own gain. But more commonly, businesses try to gain ground on rivals by hiring away their employees—who often have misguided and easily exploited assumptions about what information they can disclose. And sometimes nobody intended for proprietary information to change hands, but it happened anyway because safeguards weren't put in place. Embarrassing and expensive litigation follows.

Flooded with calls from clients concerned about trade secrets theft, Snyder and O'Melveny counsel David Almeling decided to investigate whether such cases are up nationwide. After poring through court opinions and consulting with statisticians, they concluded in two recent law review articles that trade secrets litigation in federal court had doubled between 1995 and 2004, and is on pace to double again by 2017. Meanwhile, trade secrets litigation has grown by 36 percent in state court in the last 15 years. For comparison, state court litigation in general was up 9 percent during roughly the same period.

That explosive increase correlates with a rise in employee mobility. Burlingame, California–based employment consultant Jobvite, Inc., recently asked 800 U.S.–based human resources professionals how long they expect their average new employee to stay with the company. A third responded two years or less. Only 14 percent predicted that new workers would stick around for more than five years. "Gone are the days of the company employee working for the same employer for 40 years," says Almeling.

To make matters worse, 60 percent of workers admit to having stolen confidential company information when they've left a job, according to a 2009 study by the Ponemon Institute, a Traverse City, Michigan–based research center dedicated to data protection.

The explosion in trade secrets litigation also reflects the ever-increasing importance of IP to the modern business. "There's been a doubling down on IP protection, and trade secrets in particular," says Thomas Sager, senior vice president and general counsel at DuPont, which recently won a $920 million jury verdict in a trade secrets battle with South Korea–based Kolon Industries over its Kevlar product. "We've seen a dramatic increase on trade secret protection in the corporation," he says.

IP lawyers say the trade secrets boom also correlates closely with the rate of technological advancement. "It's much easier to steal the proverbial secret sauce now, because that recipe isn't just sitting in a notebook in a shelf somewhere," says David Walton, a trade secrets litigator at Cozen O'Connor in Philadelphia.

Seemingly every new technology provides a new way for employees to snag files, says Walton. The defendants in his last two cases were both accused of stashing company documents on Dropbox.com, a popular cloud-based file-storage Web site. Walton plans to subpoena Dropbox for critical evidence, he says. "It used to be in these types of cases, you would just check the e-mails and flash drives to see if they were taking any documents. It's a lot more complicated now, and it's only going to get more complicated," he says.

Technology may lead to leaks, but it also makes it easier to catch the culprit, says Walton. Every electronic transfer leaves a footprint that can be uncovered by forensic computer analysts. High-level tech support doesn't come cheap, though. Walton advises clients to expect to pay a minimum of $30,000–$50,000 for an investigation, and possibly much more.

But while data theft is on the rise, IP lawyers say it's a bad idea to get paranoid. Witness the embarrassing scandal at the French carmaker Renault SA. In August 2010 an investigator in its security department accused three senior managers of leaking details of Renault's electric-vehicle program to a foreign competitor. The company publicly suspended the employees and lodged a criminal complaint against them in January 2011.

But the employees, who maintained their innocence, were exonerated last March when prosecutors announced that they had found no evidence of espionage. Renault quickly shifted the investigation toward "a possible swindle" by the in-house investigator, who was arrested at Charles de Gaulle Airport as he was boarding a plane bound for Guinea. One of the first heads to roll was that of Christian Husson, Renault's general counsel.

Back in Chicago, Lemko's strategy may be to turn its battle with Motorola into an American version of L'Affaire Renault. Its complaint accuses Motorola of launching a "witch hunt" against Jin, manipulating the media, and "racially profiling" Asian American employees as trade secrets thieves. Motorola declined to comment.

Walton says he's seen paranoia grip smaller businesses. He says he once exculpated a client accused of trade secrets theft by showing that the supposed data breach was just the company's IT guy working after hours.

Where Renault executives went wrong, says Walton, was in following their worst suspicions of Chinese spying, and not letting the evidence speak for itself. "You always have to look for innocent explanations and be careful," he says. "When I work with computer forensics experts, I say to them, just find the evidence and tell me what the evidence means. You have to let the evidence be its own advocate."

As is often the case, IP lawyers say that preventive measures, like screening new employees and conducting exit interviews with old ones, can go a long way. That's particularly true of trade secrets, because to win a case, you actually have to show that you took reasonable measures to protect the information in the first place. Says Beck: "The more you do on the front end to protect your trade secrets, the more likely a court is to rule in your favor."

Copyright 2011. ALM Media Properties, LLC. All rights reserved.