


THE AMERICAN LAWYER

An **ALM** Publication

americanlawyer.com

FEBRUARY 2016



CROWELL & MORING'S MICHAEL
SONGER FLEW TO KOREA WITH
VIDEOGRAPHERS IN TOW.

To Catch an IP Thief

Lawyers for DuPont and the Justice Department teamed up to protect Kevlar, the iconic body armor—and redefined trade secrets law.

By Michael D. Goldhaber

HALF A CENTURY AGO, CHEMIST STEPHANIE KWOLEK spun a liquid polymer into a fiber five times stronger than steel. She not only won a place in the National Inventors Hall of Fame, but inspired the children's book "The Woman Who Invented the Thread that Stops the Bullets: The Genius of Stephanie Kwolek." Despite initially being dubbed "a miracle in search of market," Kevlar found its way into cleats, canoes and hockey sticks; space shields, flak helmets and body armor. It has reputedly saved 3,000 law enforcement officers from serious injury or death.

Lately, Kevlar has also inspired an epic trade secrets case that has transformed the crime's prosecution, helping to enact the Cybersecurity Information Sharing Act this December, and goosing a debate over two other significant proposals. Trade secrets theft and Chinese hacking are epidemic; PricewaterhouseCoopers pegs their cost at 1 to 3 percent of U.S. gross domestic product. But lawyers are rising to meet the challenge. Thanks in part to Kevlar, foreign IP thieves are no longer bulletproof.

THE KEVLAR CASE BEGINS WITH MICHAEL MITCHELL, AN ENGINEER and 24-year employee of E.I. du Pont de Nemours & Co., who acrimoniously left his position as head of Kevlar marketing in 2006. The next year the South Korean textile conglomerate Kolon Group, which had tried in vain to reverse-engineer Kevlar since 1980, hired Mitchell as a consultant. This account of their adventures in crime and law relies on the voluminous civil and criminal record, and on interviews with half a dozen lawyers opposed to Kolon.

There's no record of the Koreans' overture to Mitchell. But here's how they subtly approached another man who worked on Kevlar's main competing product, Twaron: "It is my pleasure to introduce me to you. ... We are reviewing your resume. ... You are an engineer. Do you know details about Twaron production equipments/facilities and Twaron production processes? ... Please advise."

Mitchell shared confidential lists of Kevlar costs, prices and customers for \$128,000. And just in case he held anything back, his partners in crime secretly copied the contents of his laptop while he was at a restaurant. Still, if Kolon wished to go further and copy Kevlar, it needed to corrupt a scientist.

Mitchell clumsily fished for information with former colleagues on the Kevlar team, who duly reported it to their supervisors. DuPont asked the FBI to investigate. FBI agents swiftly found incriminating evidence on Mitchell's computer, and pressed him to cooperate in a sting.

Wearing an FBI wire at a Richmond hotel, Mitchell in 2008 introduced a DuPont employee posing as a corrupt scientist to Kolon managers who were eager to learn more. "This is very proprietary information that you're talking about," said the lure. "We're talking about DuPont trade secrets ... [and] I know DuPont does not want to give this information up."

A Kolon executive replied cagily: "This kind of conversation must be confidential. OK? We don't want to—we don't want to leave out some kind of evidence."

The FBI planned to arrest the Koreans on U.S. territory once they got more definitive evidence. But Mitchell got greedy before they could spring the trap. Playing a treacherous triple game, he told Kolon he was taping their conversations on his own—and threatened to "go to the FBI" unless the Koreans paid him more money. Kolon dropped Mitchell, and the U.S. charged him with obstruction of justice. "It was completely unethical," says lead prosecutor Kosta Stojilkovic. "And it completely changed the course of the criminal case. We were back at square one."

But for a civil case, DuPont's lawyers at Crowell & Moring and McGuireWoods had enough to file in early 2009. And the civil lawyers made a series of breakthroughs.

First, Crowell & Moring noticed in discovery that Kolon managers marked sensitive files in their inbox "Need to Delete" or "Get Rid Of." A trial judge in the Eastern District of Virginia ordered the seizure of Kolon's hard drives and, after systematic destruction came to light, ruled that a jury could infer intent to steal trade secrets.

Second, Crowell & Moring discovered that Kolon had corrupted others. Most vitally, it had recruited retired engineer Edward

One tip-off to the extent of copying was the company's huge new plant. It was a precise replica of DuPont's cramped floor plan—down to a notch to work around a nonexistent pillar.

Schulz to share specifications for the Kevlar polymer, and for the devices that spin and purify the fiber. In Schulz's words, he shared "everything you would ever want to know" about cooking Kevlar.

Alarmed, Crowell & Moring partner Michael Songer traveled to South Korea with a DuPont technician and videographers. They saw at once that Kolon's new plant, built in a wide open field, was a precise replica of the cramped factory that DuPont retrofitted in an old Richmond building dating from the 1920s. "We show up in this shiny, cavernous new facility," says Songer, "and the equipment is in the same configuration for no reason." There was even a notch to work around a nonexistent pillar.

AFTER A SEVEN-WEEK CIVIL TRIAL, SONGER AND BRIAN RIOPELLE OF McGuireWoods won a \$920 million jury verdict in 2011. But then it was the civil case's turn to derail. The U.S. Court of Appeals for the Fourth Circuit ruled that the jury should perhaps have evaluated whether DuPont had revealed its trade secrets at an old patent trial. While a civil retrial loomed, the criminal lawyers came to the fore.

The U.S. persuaded the Fourth Circuit that it had a right to subpoena the civil discovery. And conviction on that evidence was a slam dunk, thanks to the care with which Crowell & Moring

criminal partner Stephen Byers built the record. Yet it took two-plus years for the U.S. to serve Kolon with criminal process.

The hitch was that the federal criminal rules say that a party must have a U.S. address to be served. The U.S. instead invoked the Mutual Legal Assistance Treaty and, using the leverage of free trade talks, Crowell & Moring's consulting arm, C&M International, lobbied the White House IP czar to get the Korean Justice Ministry on board. Kolon objected to using an MLAT as an end-run on the criminal rules, and hired former solicitor general Paul Clement of Bancroft. But in February 2015, the Fourth Circuit declined to hear an emergency appeal.

For the first time in history, a foreign company with no U.S. address had been served with process over its objection. "The criminal case against Kolon Industries and its successor companies was groundbreaking," says U.S. Attorney for the Eastern District of Virginia Dana Boente. "Foreign corporations with no direct presence in the U.S. were forced to answer for criminal acts committed here, based on service of process pursuant to the provisions of a treaty between the U.S. and a foreign country. Kolon was the first criminal case to test the permissibility of such service under the U.S. Constitution and laws, and sets an important precedent at a time when intellectual property crimes increasingly involve international and corporate elements."

In April, Kolon settled all litigation by pleading guilty to trade secrets theft and obstruction of justice with a payment of \$360 million: \$275 million in restitution to DuPont and \$85 million in criminal fines. (In separate pleas, Mitchell received an 18-month sentence for trade secrets theft and obstruction, while Schulz received nine months' probation for conspiracy to commit trade secrets theft.) The DOJ touted it as proof that the United States "will aggressively investigate and prosecute intellectual property crimes, regardless of whether the perpetrators are foreign or domestic."

To make prosecution easier next time, the Kevlar case has been invoked to support three changes in law.

Most directly, the case has inspired a pending amendment to Federal Criminal Rule of Procedure 4, to clarify that a U.S. mailing address is not a requirement for legal service. U.S. Department of Justice officials are hopeful that the Supreme Court and Congress will approve the revision by December.

Second, DuPont is among the companies whose experience helped to justify the Cybersecurity Information Sharing Act of 2015. Recently enacted by Congress over the objection of privacy advocates, CISA encourages general counsel to report cyberattacks by clarifying that it won't subject reporting companies to liability.

Third, DuPont is among the most vocal advocates of the proposed Defend Trade Secrets Act. Co-sponsored by Sen. Chris Coons of Delaware, where DuPont is based, the bill would create a private cause of action for trade secrets theft, which would for the first time allow corporate victims to sue trade secrets thieves for damages under a harmonious federal law rather than a patchwork

of state laws. Even more important, it would provide for an ex parte injunction to preserve evidence and prevent disclosure. A group of more than 40 academics who fear anti-competitive abuses wrote a public letter calling it "the most significant expansion of federal law in intellectual property since the Lanham Act in 1946." But to practitioners like Songer, "this type of theft has become so common that a procedure allowing a company to say, 'Help me now!' would be much appreciated."

THE KEVLAR CASE, BUILT ON KOREAN CORRUPTION OF A COMPANY mole, may seem an odd symbol for a crime, IP theft, reputedly dominated by Chinese hackers. After all, the number of global cyberattacks reported to PwC soared from fewer than 4 million in 2009 to more than 40 million in 2014. In November, Moody's Investors Service announced that it would start downgrading companies for cyber risk.

But while foreign hackers get all the attention, the biggest IP theft risk may still be posed by disgruntled employees walking out the door with hot files. The threats from "insiders" and outsiders can't be disentangled, as one often works for the other. According to the 2013 Administration Strategy on IP theft, "Foreign competitors of U.S. corporations, some with ties to foreign governments, have increased their efforts to steal trade secrets through the recruitment of current or former employees." As FBI official Randall Coleman told Congress in 2014, "Economic espionage and theft of trade secrets are increasingly linked to the insider threat and the growing threat of cyber-enabled trade secrets theft."

PARTNER STEPHEN BYERS FOCUSED ON THE CRIMINAL ENDGAME.



While cyberwar has many origins, China's outsize role is not a myth. Former director of national intelligence Dennis Blair estimated in 2013 that China accounts for 50-80 percent of American IP theft. Even as he indignantly denies every attack, President Xi Jinping announced in 2014 that China aims to be a cyberpower. This spring, China declared cyberspace to be the "new commanding heights in strategic competition." As Obama counterterrorism czar Lisa Monaco has noted, "Today's espionage also involves nation states like China focused on stealing research and development, sensitive technology, corporate trade secrets and other materials to advance their economic and military capabilities."

In 2014, the U.S. dramatically charged five alleged Chinese army hackers with, among other things, stealing a nuclear reactor plan from Westinghouse Electric Co. and trade litigation secrets from U.S. Steel Corp. "Whenever we talk about cyberattacks

state-owned Pangang Group allegedly recruited DuPont employees to steal the secrets of titanium dioxide, a white pigment with a \$14 billion worldwide market for uses ranging from automotive paint to Oreo cookie filling. The U.S. businessman who recruited the DuPont scientists was convicted of trade secrets theft after a 2014 jury trial, and sentenced to 15 years in prison; Pangang was charged in San Francisco federal court in January after delays in the service of process.

The contrast between DuPont's Korean Kevlar case and the Chinese pigment case is instructive. The Justice Department is optimistic about extraditing Korean executives, but has little hope of nabbing those in China. And while the U.S. and DuPont were able to extract \$360 million from the Korean company, Pangang is unlikely to pay, because Chinese courts don't enforce U.S. judgments.

Spies are hard to prosecute, and the U.S. indictment of Chinese army suspects is purely symbolic. Since the Economic Espionage Act was passed in 1996, the DOJ's national security division has handled only about a dozen out-and-out espionage cases, which are prosecuted under Section 1831 of the act. By contrast, DOJ officials say, its computer crimes and IP section has enforced between 200 and 300 run-of-the-mill trade theft cases under Section 1832 of the statute. That pace is apt to accelerate after passage of the Cybersecurity Information Sharing Act, the impending revision of Federal Criminal Rule of Procedure 4 and the debate over the Defend Trade Secrets Act.

"We're proud of what the *Kevlar* case has done for trade secrets enforcement," says Kent Gardiner, who recently stepped down as Crowell & Moring's chair and heads its litigation group. "But it doesn't solve the China problem. ... This discussion has always been about China."

South Korea has begun to enforce IP against both foreign and domestic companies, says Gardiner, even including the previously off-limits chaebols like Kolon, family-owned business conglomerates that serve as national champions. The willingness of Korean courts to permit service of process on Kolon by the U.S. was a major sign that it wishes to be accepted as a sophisticated international player in IP creation and enforcement.

China will never be a satisfactory partner in enforcement of trade secrets, he says, until it develops a culture of respect for such assets. Unlikely as that may seem in an age of cyberwar, Gardiner sees rays of hope in China's economic maturation. "China's courts have begun to entertain litigation involving trade secrets theft and related claims. Those cases will help educate Chinese judges on the legal and business implications of trade secrets protection," he says, "which gradually will produce more respect for IP."

WANTED BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets



Huang Zhenyu Wen Xinyu Sun Kaijiang Gu Chunhui Wang Dong

IN 2014, THE FBI ISSUED THIS POSTER FOR FIVE CHINESE ARMY OFFICERS WANTED FOR ECONOMIC ESPIONAGE.

by nation states," says Shane McGee, chief privacy officer of the cybercrime consultancy FireEye Inc., "trade secrets are most of what's being stolen."

AS HUBS OF VALUABLE TRADE DATA, LAW FIRMS ARE HARDLY immune to hacking. Cyberattacks in the legal sector only rarely become public, as when China reportedly hacked the Permanent Court of Arbitration during the South China Sea arbitration last summer. But a 2014 report by Benjamin Lawsky, then New York superintendent of financial services, concluded that third-party vendors such as law firms are especially vulnerable. "When hackers go after law firms," says McGee, whose consultancy has responded to multiple Chinese attacks on U.S. law firms, "they're going after business information, like plans to bid on contracts or buy corporate assets." The problem is so pervasive that this summer saw the launch of a clearinghouse known as the Legal Services Information Sharing and Analysis Center.

DuPont itself says it's been victimized by Chinese actors in three high-profile cases, including two pending indictments. A nanochemist pleaded guilty in 2010 to stealing organic light-emitting diode technology on behalf of Peking University. Executives from China's DBN Group allegedly plotted to steal genetically modified seeds by digging in an Iowa cornfield. And

Email: mgoldhaber@alm.com.