Chapter 2

When Insiders and/or Competitors Target a Business's Intellectual Property

Introduction

By definition, an insider can come in many forms, be it an employee, a member of the management team, a corporate board member, a vendor, a third-party contracted manufacturer, or a collaborative partner in a joint venture.

The newspapers are replete with countless examples of the damage an insider can do to a business.

The following is a selection of some particularly insightful cases, which serve to illustrate the various motivations of the offenders, as well as the damage done to the enterprises they undermined.

Lightwave Microsystems

Let us begin with the case of an employee at a privately held firm (Lightwave Microsystems), who occupied a trusted position within that company, that of Director of Information Technology, and who acted alone in his attempt to illegally share Lightwave's intellectual property. The individual, Brent Woodward of Oakland, CA, chose to exercise his venial needs, as well as obtain some solace via revenge when faced with circumstances that he believed were unjust—two very powerful motivators in an individual contemplating a malevolent act.

In late 2002, the owner of Lightwave Microsystems, a California firm, announced that the company would cease operations due to the firm's inability to make a profit, but Lightwave Microsystems was not without value—it owned patents and had evolved trade secrets that could be sold. (Lightwave was subsequently purchased by NeoPhotonics of San Jose, CA.) When faced with the prospect of unemployment and upside-down stock options, Woodward made copies of the company's trade secrets from the firm's backup tapes and created a plan to sell these secrets to a competitor. He would feather his own nest monetarily and get revenge for the abruptness of his CEO's actions.

No one at Lightwave Microsystems detected the unauthorized copy activity. Why would they? Woodward's access was both natural and unencumbered. Furthermore, as Director of Information Technology, it was Woodward's responsibility to protect this very data—to discover, neutralize, and mitigate any and all attempts to steal Lightwave Microsystems' intellectual property.

Admittedly, Woodward's methodology was very sophomoric, but worthy of sharing nonetheless. He created an alias name, "Joe Data," and also set up a Web-based e-mail account, lightwavedata@yahoo.com, from which he executed his crime. Woodward

contacted JDS-Uniphase's (JDS) chief technology officer and offered to provide Lightwave Microsystems' data to JDS in return for a significant sum of money.

JDS did the absolute right thing: the firm immediately contacted the U.S. Federal Bureau of Investigation (FBI), and at their request, JDS consented to the monitoring of communications between JDS and "Joe Data," which was to occur via e-mail. The FBI, with a consensual monitoring permit provided by JDS, was able to observe the controlled negotiations between JDS and "Joe Data," as well as trace back these communications via the user's Internet protocol address to the e-mail service provider, Yahoo. The trace activity showed "Joe Data" was connected to the Internet from within Woodward's residence. This discovery enabled the FBI to execute a valid search warrant of the residence, which produced sufficient evidence to ultimately bring about Woodward's arrest. Ultimately, he was charged with one count of theft of trade secrets under 18 U.S.C. § 1832.

In August 2005, the United States Attorney's Office for the Northern District of California announced that Brent Woodward had pled guilty to the aforementioned charge. Though he could have been sentenced to ten years imprisonment and fined US$250,000, he received a $20,000 fine and was sentenced to two years in prison, plus three years of supervised release.

Though Woodward found that his vengeful attempt to obtain an illegal bonus to be very expensive in the end—in both defense fees as well as penalties adjudicated—it is important to note that Woodward was acting by himself, and for himself, and thus had no interests other than his own venial needs. What would have happened had Woodward offered the purloined data to a less ethical competitor? Perhaps that competitor would have taken the data and set up the equivalent of a parallel universe. Would the value of Lightwave Microsystems' intellectual property sold to NeoPhotonics have been jeopardized? What of NeoPhotonics, the purchaser of Lightwave Microsystems' technology? If the unscrupulous competitor had taken the trade secrets and capitalized on the technological advances, what recourse would NeoPhotonics have had to recoup their investment/payment to Lightwave Microsystems? Litigation would only be an option IF Lightwave Microsystems knew the intellectual property had been stolen. And this would have come to light when? The purchaser wouldn't have admitted to having purloined the intellectual property, and Woodward certainly wouldn't have advertised his sale. Only during the unscrupulous competitor's developmental, manufacturing, and/or marketing/sales processes would there have been the possibility that the technology acquisition might be revealed.

The best course would have been to initially establish a defense against Woodward's action. Lightwave Microsystems should have had in place multiple audit trails and either human or machine tracking of all users, including the super-user, so that a warning could have been sent that anomalous behavior had occurred.

America Online

Let's now move on to another case in which greed was the motivating factor, inducing an employee to steal his employer's private data. In April and May 2003, American Online (AOL) software engineer Jason Smathers, utilized a colleague's access codes to surreptitiously log on to the AOL server. Then, posing as the colleague, he used his colleague's access to acquire information from each of the then 30 million AOL customers. The data stolen by Smathers comprised 92 million records, which contained the personal identifying information of those 30 million customers. The data included e-mail addresses, screen names, ZIP codes, customer credit card types (not numbers), and telephone numbers associated with AOL customer accounts. Smathers sold the stolen AOL data to Sean Dunaway of Las Vegas. Dunaway paid Smathers US$27,000 for the addresses, and then utilized them to advertise his own online gambling Web site. Dunaway later resold the AOL data to online "spammers" for approximately US$52,000. Clearly, he was an early adopter of the concept of spamming.

The Department of Justice prosecuted this case under the (then new) federal law Can-Spam (Controlling the Assault of Non-Solicited Pornography and Marketing Act). Smathers had pled guilty in February 2005 to the crime. In October 2005, he was sentenced to 15 months in prison and fined US$84,000—triple what he had garnered through the sale of the data. Smathers clearly knew the data had value, but he grossly underestimated the value of the information. Though DOJ recommended to the presiding judge that Smathers be barred from the software profession, the judge noted Smathers' cooperation in the investigation and believed that his cooperation and Smathers' contrite behavior warranted leniency. Smathers noted to the court that AOL had said his theft and subsequent sale had cost the company at least US$400,000—and potentially millions of U.S. dollars.

At first glance, it would seem only AOL and their 30 million subscribers were exposed to unwanted spam. So where's the damage? The user can simply press the Delete key and get on with life. After all, spam is received by virtually every Internet user, and a variety of companies now specialize in filtering spam so only "good" e-mail arrives in their inbox. However, the loss of revenue to AOL was the loss of

time each user experienced while deleting those unwanted e-mails—and time has value. But why was a crime that was committed in 2003 not prosecuted until early 2005? A very good question.

The delay in prosecution is largely due to the fact that until mid-2004, Smathers was still an employee of AOL and had not yet been identified as the source of the data breach. While AOL knew they had a problem and were cooperating with law enforcement, Smathers' use of a colleague's administrative logon was an effective method of bypassing the AOL corporate security apparatus. Smathers' colleague did have authorized access to the data, whereas Smathers did not. Had the colleague perhaps protected his passwords better (there is no evidence to suggest the unidentified colleague colluded or provided Smathers with his login passwords), this crime might never have occurred.

But the real damage may still be looming. What of the collation of e-mail addresses, usernames, and user telephone numbers? What malicious use could this data be to e-mail phishers or unscrupulous telemarketers? The answer: Priceless. That was 2003. Fast forward to 2007 where some spammed e-mail has evolved into what is known euphemistically as *phishing*.

AOL is advertised as a "family-friendly" environment—one where the customer doesn't have to be a technological marvel, nor think in bits or baud, to enjoy the pleasures of the Internet—and AOL works extraordinarily hard to exclude the seedier side of the Internet. As noted earlier, AOL admitted to having spent at least US$400,000 as a result of this incident, but the downside may be much greater as they continue creating software to mitigate the loss of customer data, while simultaneously working to regain the trust of their customer base.

According to the Privacy Rights Clearinghouse, in 2006 alone there were approximately 100,453,730 cases of personal identifying information revealed to those without a need to know. These revelations occurred in government entities, retailers, educational institutes, and consulting firms (www.privacyrights.org/ar/DataBreaches2006-Analysis.htm).

Casiano Communications

Let's look at another instance of personal greed—this in a separate industry where a worker was accused of stealing the intellectual property of his employer and setting up shop as a direct competitor. In mid-October 2005, Casiano Communications, Inc. (CCI), arguably the most prominent publisher within the Caribbean basin with respect to

Caribbean business and travel literature magazines, filed suit against a former employee, John Bynum. The suit alleged that Bynum stole intellectual property from CCI—specifically, CCI's databases, which Bynum then forwarded to his personal e-mail account from CCI's computers. According to the CCI complaint, Bynum stole client and advertiser information, violating CCI's Electronic Mail and Company Resources and Equipment policy, which is a condition of employment with CCI.

San Juan, Puerto Rico Superior Court issued a temporary restraining order against Bynum that required him to cease and desist from utilizing, transmitting, selling, or reproducing any form of database or other trade secrets obtained during the course of his employment with CCI. The injunction granted CCI the right to seize all materials contained in any computers, disks, or other information-technology items in the personal possession of the defendant. CCI alleged that Bynum had been selling a database of key island (Puerto Rico) business contacts to companies to market their products and services.

Again, this is an example of personal greed, motivated as much by circumstances as opportunity. It is not beyond the pale to assume your employees know who your competitors are and how to reach out to these firms to sell your intellectual property should the opportunity present itself and the competitor be unscrupulous enough to accept it (unlike the Lightwave Microsystems case).

Corning and PicVue

A case that hit the public eye in 2005, and that was settled in 2006, has these very circumstances present, where an opportunity presented to a low-level employee, coupled with the identification of an interested party, created a temptation for instant financial gain that was simply too great for a weak-willed employee to ignore.

This was the case of Corning Incorporated and PicVue Electronics, the latter a Taiwanese corporation. On October 20, 2005, the Department of Justice charged Jonathan Sanders, an employee of Corning's Harrodsburg, KY plant, with the theft of trade secret material belonging to Corning. Specifically, material pertaining to an "overflow down draw fusion glass-making process used to produce Thin Filter Transistor (TFT) Liquid Crystal Display (LCD) flat panel glass."

In the DOJ complaint, it is alleged that Sanders began his theft of Corning's IP in December 1999 and continued to perpetrate the crime through December 2001. Sanders allegedly took, without authorization, trade secret material belonging to Corning and subsequently sold that same material to PicVue Electronics Ltd.,

a Taiwanese corporation. This case of Economic Espionage, not only involved PicVue Electronics, the corporation, but also the former president of PicVue.

When arrested, Sanders waived his right to a preliminary hearing, was indicted, and pled guilty. He was sentenced to 48 months imprisonment and ordered to pay a fine of US$20,000 on April 18, 2006.

He told the FBI that he found blueprints containing the Corning trade secrets within a Corning warehouse in 1999. The blueprints were within a container of sensitive corporate material awaiting destruction. He said he simply took the blueprints instead of destroying them.

In December 1999, Sanders then traveled to California and met with PicVue's company president, Jacob Lin, as well as Yeong C. Lin, a consultant to PicVue. Sanders claimed he only described the fusion draw process, and did not show the drawings to the PicVue president nor his consultant. Subsequent to this meeting, Sanders was allegedly offered a job by PicVue, but declined the position.

Then around September 2000, Yeong C. Lin, the consultant, informed PicVue that Sanders was now offering Corning's blueprints/drawings via an oral description. PicVue authorized the payment of US$30,000 and wired the funds to a California bank account, where apparently the PicVue consultant took control of the funds. The consultant then enlisted the aid of a college roommate, Danny Price, who carried US$25,000 to a meeting with Sanders outside of Atlanta, GA, so as to obfuscate the connection between PicVue and Sanders.

Sanders met with Price as planned, outside of Atlanta, and accepted the money from Price. In exchange, he provided Price with the Corning blueprints he had stolen from the corporate sensitive data destruction bin. Price apparently gave the documents to consultant, Lin, who met with PicVue engineers in California. The PicVue engineers took digital pictures of the blueprint documents and transferred the images to a digital storage device. The engineers hand-carried the digital storage device back to Taiwan, and the blueprints were then, allegedly, destroyed.

Two months later (November 2000), engineers from PicVue traveled to Kentucky and met with Sanders directly to discuss the blueprints he had sold to PicVue. Sanders claims the conversations were centered on providing clarification to PicVue on details contained within the blueprints.

PicVue representatives then traveled to the offices of Saint-Gobain glass, Niagara Falls, NY in September 2001 to purchase a part specific to the fusion process. Given the prior commercial relationship between Corning and Saint-Gobain, the latter recognized the utility of the part as being only applicable to the fusion draw process

and alerted Corning to the possibility that their trade secrets had been compromised to PicVue.

Corning representatives visited Saint-Gobain's offices, reviewed the specifications provided by PicVue and concluded that Corning trade secrets were involved. Corning contacted the FBI, who opened an investigation October 2001.

In this instance, Corning apparently had a set of procedures in place to destroy company confidential documents, but it would appear no mechanism existed to ensure that documents put into the "to-be-destroyed" bin were, in fact, subsequently destroyed. Again, the company was ignorant of the theft of their intellectual property until the recipient—PicVue, in this case—approached one of the few firms in the world able to create the parts necessary to make the purloined documents effective in the marketplace. If there is a bright side to the entire episode, it is the strength of the relationship between Corning and Saint-Gobain, which brought this illegal activity to light, not internal procedures.

Let us assume you have appropriate checks and balances in place to protect yourself against the opportunistic and greed-driven employee. What defense do you have to protect yourself when the theft of your technology is premeditated by individuals who are the leaders, and literally in the driver's seat of one of your main competitors? Can't happen, you say? Think again.

Avery Dennison and Four Pillars

Let's now review the well-documented and publicized instance of intellectual property theft that was encountered by Avery Dennison, the firm that makes labels, and by extension, the firm that spends a great deal of money on the research and development of adhesives. Unbeknownst to the company, they had had their intellectual property stolen from them from 1989 through 1997. The theft of their IP was literally a textbook example of the methodical harvesting of a firm's technological advances and research by a competitor.

Avery Dennison, whose headquarters is in Pasadena, CA, is one of the United States largest manufacturers of adhesive labels, and retains intellectual property for these formulas. The firm's adhesives and methodologies give Avery Dennison their market advantage within the global adhesive label market. Because of this, a competitor, Four Pillars Enterprise Limited of Taiwan, specifically targeted their research facility in Concord, OH.

Four Pillars is a manufacturer of pressure-sensitive products in Taiwan, with market share both in the United States and the Far East. Prior to 1989, Four Pillars CEO had identified his competition and had noted the competitive advantage held by

market-sector leader Avery Dennison and so had set out as a corporate goal to capitalize on Avery Dennison's advance research in adhesives. A very determined individual, he was successful in stealing the formulas for Avery Dennison's adhesives—some might say very successful.

Successful that is, until 1997, when one of his Four Pillars' employees applied for work with Avery Dennison, and during the course of the interview(s) revealed that for the preceding eight years, Avery Dennison's adhesive formulas were being provided to Four Pillars by an employee of Avery Dennison.

Avery Dennison had not previously detected this theft of their IP. The firm took the correct action and contacted the FBI, and together with Avery Dennison, the two contrived a sting operation to identify the employee who was supplying Four Pillars with company secrets. The sting operation was fruitful and identified Mr. Ten Hong Lee—a.k.a., Victor Lee—a U.S. citizen and senior research engineer at Avery Dennison's Concord, Ohio research facility, who was stealing the intellectual property of his employer.

Lee was confronted and admitted his guilt, confessing to having stolen the formulas and methodologies of his employer from 1989 to 1997. He was later persuaded to act as a cooperative witness for the Department of Justice (DOJ), who wished to prosecute this theft of the intellectual property of a United States corporation by a foreign national, under the powers of the Economic Espionage Act (EEA) of 1996.

The ensuing investigation revealed Lee—who received his undergraduate degree at the National University of Taipei, his Masters degree in polymer science from Akron University, and his Ph.D. in chemical engineering from Texas Tech—had been invited to Taiwan by the Industrial Technology Research Institute to give a lecture at one of their conferences. While there, he was asked to present a technical lecture to Four Pillars by the company's technical director.

During this visit to Taiwan, Lee was enticed to covertly enter into a relationship with Pin Yen Yang—a.k.a., P.Y. Yang—President and CEO of the Taiwanese firm, Four Pillars Enterprise Company, Ltd as a "secret consultant." For this, he was paid $25,000 for his first year. Lee, Yang, and Yang's daughter, Hwei Chen Yang—a.k.a., Sally Yang—conspired to provide the Yangs with Avery Dennison's intellectual property and business methodologies. In exchange, Lee would be paid substantial sums of money—to be deposited with Lee's relatives, who were resident in Taiwan.

Following the discovery by Avery Dennison, the covert relationship continued under FBI scrutiny until early September 1997, when Lee provided to the Yangs proprietary information of Avery Dennison origin during a meeting monitored and controlled by the FBI in a room within the Holiday Inn located in Westlake, Ohio. Lee indicated on the video coverage of the meeting to the Yangs that the papers he

was providing were the intellectual proprietary property of Avery Dennison. The Yangs acknowledged such, and following the meeting, the Yangs were observed cutting, with a knife, the headers and footers off the documents provided by Lee. Subsequently, the Yangs were arrested by the FBI as they attempted to board a plane and return to their corporate headquarters with the data.

The relationship between Lee and the Yangs' Four Pillars was a clear case of "economic espionage." During the prosecution of this case, it was learned that Lee was paid more than $150,000 over a period of eight years in exchange for sharing the intellectual property of his employer, Avery Dennison. In 1999, U.S. District Court Judge Peter C. Economus convicted both Yang and his daughter for stealing trade secrets and also convicted Four Pillars on economic espionage charges. Yang was sentenced to six months of home confinement and fined $250,000; his daughter was fined $5,000 and received a year's probation. The firm, Four Pillars, was fined $5 million for accepting the pilfered trade secrets. Lee pled guilty to wire fraud and defrauding his employer.

Avery Dennison's discovery of Four Pillars' illegal activity was due to a serendipitous event, the employment application by a former Four Pillars' employee and this employee's willingness to share information concerning Four Pillars' recruitment of an Avery Dennison employee for the sole purpose of compromising the intellectual property of Avery Dennison. In this instance, Four Pillars personnel targeted an individual with whom the Yangs could relate to on the basis of ethnicity, leveraging Lee's desire to help a fellow-countryman. The Yangs stroked Lee's ego, giving him "recognition" for his intellect, and providing him with remuneration in a covert manner—thus, keeping his skullduggery out of the view of the tax authorities, Avery Dennison lenders, or others who may question the increase/addition in Lee's income.

The Yangs' investment of approximately $150,000 resulted in an approximate $30 to 50 million loss to Avery Dennison. It is worth noting that Yang and his firm Four Pillars were acting in their own self-interest and not at the behest of any other entity.

Four Pillars ultimately appealed their conviction to the Supreme Court, hoping for a reduction in the sentence, but the convictions were upheld in October 2002. Four Pillars continues to be an active firm, involved in adhesive and label manufacturing.

Lexar Media and Toshiba

Let's move on to one of those ticklish situations that every company that has ever collaborated with another company encounters: *Is this a win-win scenario, or am I placing my company in a situation of inordinate risk?* The answer could be yes—*It could be a win-win situation*—but you must keep your eye on your property and monitor your partner's actions as well.

Now, let's review the litigation undertaken by Lexar Media (as of June 2006, a wholly owned subsidiary of Micron Technology) and their successful lawsuit in which they claimed the theft of their trade secrets by a foreign competitor and the competitor's U.S. subsidiaries.

In late March 2005, a California Superior Court jury found Toshiba Corporation (a Japanese company) guilty of the theft of trade secrets from Lexar Media and assessed damages of $381.4 million and punitive damages of $84 million for a total of $465.4 million. Lexar had alleged that Toshiba had utilized Lexar's trade secrets in Toshiba's product line, which included NAND flash chips, Compact Flash cards, xD-Picture cards, and Secure Digital cards. The jury agreed and the issuance of punitive damages by the jury indicated that the jury found Toshiba's actions to be oppressive, fraudulent, and/or malicious.

Toshiba petitioned the court in April 2005 to recognize the jury's award as an advisory verdict and asked that the monetary damages be reduced, while Lexar petitioned the court for an injunction against Toshiba so as to prevent the sale of any Toshiba products that incorporated Lexar's intellectual property. On October 14, 2005, the court ruled that the jury findings were not advisory but in fact final. The court also declined to issue an injunction against Toshiba. Lexar's Executive Vice President and General Counsel, Eric Whitaker, noted that Lexar will continue to pursue patent infringement litigation against Toshiba, and remains confident that once patent infringement has been confirmed, that an injunction against Toshiba preventing the sale of their products will be forthcoming. Then in April 2006, Lexar filed a petition with the U.S. International Trade Commission (ITC) to initiate a Section 337 investigation in which Lexar asked that Toshiba's NAND flash memory chips be barred from import into the United States. According to an ITC press release, in May 2006 the ITC voted to institute an investigation of certain flash memory chips, flash memory systems, and products containing the same. In October 2006, Toshiba and Micron (having acquired Lexar) reached a settlement, the details of which were omitted from the public Securities and Exchange Commission filings of November 2006.

A tremendous amount of legal wrangling was involved in the proceedings, and while a settlement occurred, it begs the question: How did it get this far? According to Lexar, in mid-1996 Lexar Media was created by employees of Cirrus Corporation, and its business plan centered on technology created by Cirrus. Prior to the creation of Lexar, Cirrus and Toshiba had been involved in discussions (1994 to 1995) on how Cirrus would collaborate with Toshiba in creating flash memory controllers in support of Toshiba's preferred flash memory technology. Upon creation of Lexar, discussions

between Toshiba and Lexar increased in depth and frequency. Toshiba and Lexar's Toshiba—Toshiba America and Toshiba America Electronic Components (TEAC)—were given access to Lexar's intellectual property under a Non-Disclosure Agreement (NDA) signed on December 1, 1996, which had a five-year expiration date.

Following the signing of the NDA, in-depth discussion between the parties ensued, and Toshiba invested US$3 million in Lexar in May 1997. They also placed a member on the board of directors of Lexar. Throughout 1997, Lexar continued to share intellectual property with Toshiba. In April 1998, Toshiba and Lexar entered into a partnership so as to be competitive in the flash memory market. The joint relationship apparently prospered throughout 1998 and most of 1999. On October 6, 1999, Toshiba and SanDisk announced in a joint press statement that the two firms had entered into a joint agreement to develop and manufacturer Gigabit Scale flash memory. Interestingly, the Toshiba board member apparently missed the October 5, 1999 Lexar board meeting. Lexar felt that their "partner" had sold them out to their main competitor in the flash memory market—SanDisk. Not only had Toshiba been a partner in numerous joint development projects, but Toshiba's presence on the Lexar board of directors provided Toshiba with all the strengths and weaknesses of the firm.

The Lexar board requested an explanation from the board member representing their partner Toshiba. The board member provided assurances that the agreement between Toshiba and SanDisk did not involve Lexar technologies. The board member continued with his assurances, noting the publicized agreement between Toshiba and SanDisk involved a separate division within Toshiba than that involved with Lexar. Less than seven months later, SanDisk and Toshiba announced in a joint press statement that the two had signed a US$700 million deal to create a joint fabrication facility in Virginia to produce multilevel cell (MLC) flash memory chips. Lexar believed that their intellectual property, specifically the multipage write technology was being used in this, and that without this technology, the MLC flash memory initiative would not be financially viable.

Lexar believes that Toshiba and its subsidiaries have incorporated into their product line intellectual property which, when disclosed by Lexar to Toshiba, were not only considered proprietary trade secrets of Lexar, but also were covered under the subsequent NDA. Though suspicious, it was not until Toshiba published in 2001 the technologies used in their MLC smart memory application that proof was evident to Lexar that their IP had been used.

In this instance, Lexar was able to prove what they suspected when Toshiba published the technical specifications of the Toshiba product line. What makes this

case especially noteworthy is the apparent brashness on the part of Toshiba. Toshiba had a seat on the board of the company whose intellectual property they would be purloining. In addition, Toshiba had a number of joint development projects, during which Lexar's intellectual property was fully disclosed to Toshiba, and which Toshiba then leveraged for their own benefit in their own product line.

So, would Lexar not have lost their intellectual property had they chosen their partners more carefully? Probably yes, but did they have a choice in choosing their dance partner? Lexar was a spin-out and a startup and thus required a rock-solid partnership to reduce the unremunerated burn rate and shorten the distance to profitability. The preexisting Lexar/Toshiba relationship at first appears to have given Toshiba the impetus to take advantage of the startup's perceived lack of attention to the protection of their intellectual property, when in reality the importance of the intellectual property was not lost on the Lexar executive team, being that they did pay attention and did notice it, albeit after the theft had occurred and the IP had been incorporated into a competitor's product.

SigmaTel and Citroen

Which brings us to two situations of alleged IP theft involving companies from two separate industries—automotive and audio entertainment devices. So what's the similarity? Both companies allege that their patented methodologies were copied by a competitor located within China and then marketed within the Chinese market—thus, the companies in each case apparently ended up competing against their own product designs, manufactured by companies that had little or no research costs associated with the development of the product design, allowing the companies to market the product for a cost considerably less than the company owning the patent. So, is that the price of doing business in China? The government of China claims to be improving their intellectual property rights protection methodologies, but as we noted earlier, they have a long row to hoe. There will be repeated instances where individual corporations will be victimized. Unscrupulous business practices will always arise when intellectual property protection is lax.

In January 2005, SigmaTel, a developer and manufacturer of audio devices, filed suit against Actions Semiconductor Company of Zhuhai, Guangdong, China (Actions Semi), alleging that Actions Semi's integrated circuits, which are within Action Semi's MP3 players, infringe upon multiple patents related to SigmaTel's portable audio devices. SigmaTel followed in March 2005, with the filing of a complaint with the

U.S. International Trade Commission (ITC), requesting that the ITC initiate a Section 337 investigation on Actions Semi. In the ITC complaint, SigmaTel identified the specific patents that they believe had been infringed upon and requested that the ITC grant a permanent exclusion order, banning the importation into the U.S. of the infringing products and issuing a cease-and-desist order halting sale of these same products. The ITC opened an investigation, and the trial began in November 2005.

Actions Semi claimed no infringement of SigmaTel's patents has occurred. In September 2006, the ITC found that Actions had infringed upon SigmaTel's patents and rendered judgment in favor of SigmaTel. The ITC issued a limited exclusion order protecting SigmaTel in the U.S. market from Actions Semi's importation of products that were found to contain certain identified components. Thus, SigmaTel had their U.S. market protected.

The second case, which occurred in October 2005, involves Citroen's joint venture in China: Dongfeng Peugot Citroen Automobile. Citroen alleged that Shanghai Maple used Citroen's core chassis technology in producing a series of Shanghai Maple models. According to the Chinese press, Shanghai Maple claimed their automobiles were created from their own designs. Citroen, however, claimed their patent on "special chassis technology" had already been filed with the world IP rights organization and had not been licensed to Shanghai Maple. Shanghai Maple, a subsidiary of Geely Automobile, claimed no knowledge of any infringement, stating that they had never received any documentation from Citroen.

Interestingly, the unlicensed use of technology apparently is not an unusual occurrence within the Chinese automotive manufacturing sector. In May 2005, General Motors Daewoo alleged that Cherry QQ copied its "Spark" sedan design and so demanded 80 million RMB (approximately US$10 million) as compensation for patent infringement. Prior to the GM/Cherry suit, Dongfeng Honda and Toyota Auto sued Hebei Shuanghuan Auto and Geely Auto for similar reasons.

Truly remarkable is the perspective of the deputy engineer from within the China Automotive Technology & Research Center, Zhang Zhenzhi, who noted in the *Shanghai Daily News*, "It's inevitable for domestic automakers to imitate other advanced technologies, no matter from other domestic companies or foreign firms. But in the future, we would be able to better our designs after getting more experience on developing our own autos." To the untrained eye, it would appear that loss of IP is expected and will continue to be accepted within the nascent Chinese auto industry.

In both of these examples, the company whose technology has been illegally used did all of the right steps to protect their intellectual property—for example, filing patents, and so on. But in the end, they found themselves caught up in an embryonic legal system,

oftentimes described as a litigation quagmire of quicksand where it is all but impossible to effectively litigate patent violations. In SigmaTel's instance, they took appropriate measures to protect themselves within one of their prime markets—the United States. The fact that they prevailed in the ITC trail speaks volumes, especially given that the overt threat to SigmaTel's market share in the U.S. was successfully mitigated. That said, the injunction, levied against Actions Semi, affects only business within the U.S. and has no effect on the China or European market. While in Citroen's instance, it boils down to what they would call in prohibition-era Chicago—*gettin' the business*—where the deputy engineer from within the official Chinese Automotive Technology & Research Center viewed the apparent "borrowing" of IP as the norm—something to be expected of young companies, and something to be tolerated by the more established new-to-China foreign firms.

3dGEO – China

In 2004, Chinese citizen Yan Ming Shan, 34, of Daqing, China, pled guilty in federal court to a one-count indictment that charged him with the unauthorized access to the computer programs of 3dGEO, where he fraudulently obtained proprietary source code and other software. Shan was sentenced to two years imprisonment.

According to the DOJ press release concerning this case, from April to September 2002 Shan worked for 3dGEO Development, Inc., a Mountain View, California company that develops software used in the survey of land for sources of natural gas and oil. 3dGEO employed Shan under an agreement with one of its customers, PetroChina, a Chinese company with a division named DaQing Oil, which arranged for its employee to travel to California for training on 3dGEO's software. FBI agents arrested Mr. Shan in September 2002 as he attempted to board a flight to China. Ever since, he has been held in custody as a flight risk, pending trial.

Interestingly, in an interview with 3dGEO's president, Dimitri Bevc, which occurred shortly after the arrest of Shan, Bevc said the episode highlighted a dilemma for the company, which was seeking to secure its intellectual property but also expand its business in Asia. "There's incredible demand from Chinese firms that are hungry for technology," said Mr. Bevc. "But we are built on our own intellectual property."

Bevc continued, saying he was afraid his company was being punished in the Chinese marketplace. In addition, with the pending payments from PetroChina for work already completed, Mr. Bevc said his company's Chinese sales prospects had been drying up. "What we heard back was… that 3dGEO did something wrong" by taking action against Mr. Shan, who served most of his sentence while awaiting trial, and has since returned to China, Mr. Bevc related.

This page intentionally left blank