Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

TRADE SECRETS

For the fourth year in a row, lawyers at Gibson, Dunn & Crutcher provide a summary of the key milestones in trade secret litigation over the past year.

2013 Trade Secrets Litigation Round-Up




By Jason C. Schwartz,
Alexander H. Southwell,
Molly T. Senger and
David A. Schnitzer

In 2013, U.S. Attorney General Eric Holder remarked that ''[t]here are only two categories of companies affected by trade secret theft: those that know they've been compromised—and those that don't know it yet.''[1] Over the past year, there have been several significant developments in trade secrets law, amidst growing concern about the devastating effect of trade secret theft on U.S. companies—both by insiders-turned-competitors, and by those working for foreign companies and sovereigns.

Jason C. Schwartz is an employment litigation partner in the Washington, D.C., office of Gibson, Dunn & Crutcher, whose practice includes litigating high-stakes trade secrets and non-compete disputes. Alexander H. Southwell, a litigation partner in Gibson Dunn's New York office, is a former federal computer crimes prosecutor and serves as co-chair of Gibson Dunn's Information Technology and Data Privacy practice group. Molly T. Senger and David A. Schnitzer are litigation associates in Gibson Dunn's Washington, D.C., office.

The White House announced a broad trade secret theft prevention strategy in 2013, and the Department of Justice continued to vigorously prosecute criminal trade secret theft, unsealing an indictment against two former Eli Lilly & Co. scientists alleged to have stolen trade secrets valued at $55 million for the benefit of a Chinese competitor. At the same time, the DOJ occasionally struggled in its attempts to bring foreign corporations accused of trade secret theft under the jurisdiction of U.S. courts, suffering a significant 2013 defeat in its high-profile case against the Chinese government-controlled entity, Panang Group Co. Ltd.

In the legislative arena, Congress enacted a new amendment to strengthen the penalties available for

[1] Attorney General Eric Holder, Remarks at the Administration Trade Secret Strategy Rollout (Feb. 20, 2013), *available at* http://www.justice.gov/iso/opa/ag/speeches/2013/ag-speech-1302201.html.

 ISSN 0148-7965

those convicted under the Economic Espionage Act (EEA), while Texas became the 47th state to adopt the Uniform Trade Secrets Act (UTSA).

In the civil trade secrets realm, 2013 saw important appeals in the long-standing Mattel-MGA Bratz doll trade secrets dispute, and in the blockbuster DuPont-Kolon protective fiber battle. And a trade secret case before the Federal Circuit demonstrated the significance of careful compliance with non-disclosure disagreements, as the court held that a company's failure to properly designate information as ''protected'' under the terms of such an agreement precluded the company from later claiming that information was a trade secret.

We discuss these and other 2013 developments in trade secrets law below. We first address changes in the statutory landscape, followed by criminal developments, and then civil developments.

STATUTORY DEVELOPMENTS

Trade secret law is based primarily on state law, although the EEA provides a basis for federal criminal prosecutions. In 2013, there were several notable developments regarding both the EEA and state laws related to the protection of trade secrets.

Federal Economic Espionage Act Developments

Spurred by rising concerns of foreign actors stealing American trade secrets, Congress in 2013 continued to strengthen the principal criminal statute dealing with such matters—the Economic Espionage Act, 18 U.S.C. § 1832. In January 2013, Congress amended the EEA with the passage of the Foreign and Economic Espionage Penalty Enhancement Act, which increased the maximum fine for individuals convicted under the EEA from $500,000 to $5 million.[2] The Act similarly raised the maximum fine for organizations found to have violated the EEA from $10 million to the greater of $10 million or ''three times the value of the stolen trade secret.''[3] The value of a stolen trade secret is broadly defined under the Act to include not only the ''expenses for research and design'' of the trade secret, but also the ''other costs of reproducing the secret that the organization has thereby avoided.''[4] This strengthening of the EEA has the potential to further deter the theft of valuable trade secret technology and to set damages calculation precedents that may be applied in civil litigation as well.

The EEA does not provide for a private right of action, and companies seeking civil remedies for trade secret theft generally must pursue their misappropriation claims under state law. In 2013, however, the American Bar Association's Intellectual Property Law section asked Congress to create a ''federal civil claim for the misappropriation of a trade secret when certain circumstances are met.''[5] The Commission on the Theft of American Intellectual Property similarly advocated for the amendment of the EEA to provide a federal private right of action for trade secret misappropriation.[6] In response to these and other efforts to federalize trade secret law, several legislators, including Sen. Jeff Flake (R-Ariz.) and Rep. Zoe Lofgren (D-Calif.), introduced measures in 2013 that would provide civil litigants with a federal avenue to pursue trade secret claims. To date, however, none of these measures have emerged from committee.[7]

State Law Developments

In May, Texas became the forty-seventh state to adopt a version of the Uniform Trade Secrets Act (UTSA), leaving Massachusetts, New York, and North Carolina as the only three states that have not yet adopted some form of the UTSA. Texas's version of the UTSA, which became effective on Sept. 1, 2013, made several intellectual-property-owner-friendly changes to the state's prior common law scheme, such as (1) omitting the requirement that information remain in continuous use to be protected as a trade secret; (2) creating new trade secret protection for so-called ''negative know-how'' (i.e., acquired knowledge of what does *not* work); (3) codifying the inevitable disclosure doctrine; (4) providing for injunctive relief for threatened trade secret theft; and (5) easing the requirements for filing materials under seal in trade secret litigation.

CRIMINAL DEVELOPMENTS

There are continued indications that the Obama administration is increasing its criminal prosecution of trade secret theft as part of a broader effort to bolster its protection of U.S. intellectual property. In February, the White House released a white paper entitled, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, which recognized that ''the pace of economic espionage and trade secret theft against U.S. corporations is accelerating.''[8] The Obama Administration's strategy for mitigating trade secret theft includes increased diplomatic efforts to protect intellectual property overseas, and the promotion of voluntary best practices amongst private industry leaders.

In addition, the Obama administration has continued to enhance domestic law enforcement efforts to combat trade secret theft. During the first 10 months of fiscal year 2013, the Department of Justice reported fourteen new prosecutions and three convictions under the Economic Espionage Act—a 30 percent increase from fiscal year 2012 and a 70 percent increase from five years ago.[9] Similarly, in June 2013, the FBI reported a 39 percent increase in trade secrets investigations since fiscal

---

[2] *See* Pub. Law 112–269, 126 Stat. 2442.

[3] *See id*.

[4] *Id.*

[5] *See* Letter to U.S. Intellectual Property Enforcement Coordinator (Apr. 22, 2013), *available at* http://www.americanbar.org/content/dam/aba/administrative/intellectual_property_law/advocacy/aba_ipl_trade_secret_IPEC_april22_2013.authcheckdam.pdf.

[6] *See The Report of the Commission on the Theft of American Intellectual Property* 73 (2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

[7] *See* ''Sen. Flake Introduces Trade Secret Bill to Allow Civil Action Against Foreign Entities,'' 87 *Bloomberg BNA's Patent, Trademark and Copyright Journal* 215 (Nov. 29, 2013) (87 PTCJ 215, 11/29/13).

[8] *See Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* 1 (2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[9] *See Prosecutions for 2013: Lead Charge: 18 U.S.C. 1832—Theft of Trade Secrets*, Transactional Records Clearinghouse (Oct. 2013).

  PTCJ ISSN 0148-7965

year 2009.[10] Investigating cyber-crimes, including trade secret theft, remains the third highest priority for the FBI (after terrorism and counterintelligence).[11]

Trade Secret Theft by Chinese Competitors of U.S. Companies

The vast majority of criminal trade secret cases cited in the White House's *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* involved trade secret theft by (or for the benefit of) Chinese entities.[12] Over the past year, prosecutors brought several indictments against Chinese nationals alleged to have stolen trade secrets for the benefit of Chinese companies, amidst reports that the Chinese government is increasingly engaged in sophisticated economic espionage and cyber-attacks on U.S. interests.

United States v. Cao (S.D. Ind.)[13]

In October, an Indiana federal district court unsealed an indictment against two former Eli Lilly & Co. biologists, who were charged with seven counts of divulging trade secrets valued at more than $55 million to a Chinese competitor. Guoquin Cao and Shuyu Li, who held senior positions with Eli Lilly, have been accused of electronically passing their employer's trade secrets to Jiangsu Hengrui Medicine Co., a major producer of pharmaceuticals in China that recently began to compete in U.S. markets. The trade secrets allegedly misappropriated relate to new treatments for cancer, cardiovascular disease, and diabetes, all of which are in the early stages of development. Trial is currently scheduled for May 2014.

United States v. Huang (W.D. Mo.)[14]

In January 2013, two Chinese nationals pled guilty to stealing trade secrets from Pittsburgh Corning Corp. Ji Li Huang and Xiao Guang Qi attempted to buy what they believed to be Pittsburgh Corning's trade secrets related to the company's cellular glass insulation technology with the goal of beginning their own, competing business in China. After unsuccessful attempts to gather the information by physically accessing Pittsburgh Corning's plant, Huang and Qi placed a newspaper advertisement seeking someone with Pittsburgh Corning experience ''to lead a project to build up a foam glass factory with continuous research on new formulas'' in Asia. A company employee, cooperating with Pittsburgh Corning and federal agents, corresponded with the defendants for several weeks and arranged a meeting, during which the defendants paid for what they believed to be Pittsburgh Corning's trade secrets before they were arrested. After pleading guilty, Huang was sentenced to 18 months imprisonment and a $250,000 fine; Qi was sentenced to time served and a $20,000 fine, and agreed to depart the United States.

United States v. Liu (D.N.J.)[15]**; (3d Cir.)**[16]

In March, Sixing Liu, a Chinese national and a former employee of a U.S. defense contractor was sentenced to 70 months in prison after being convicted on charges that included unlawful possession of trade secrets and violations of the Export Control Act. Prior to leaving his employment, Liu had copied thousands of the defense contractor's electronic files related to guidance systems for missiles, UAVs and other airborne technology, and took them with him to China. Liu appealed, and the case is now pending before the Third Circuit.

United States v. Maniar (D.N.J.)[17]

Of course, corporate concern with foreign economic espionage is not limited to China.

In June, federal authorities arrested Ketankumar Maniar, a former staff engineer at the medical technology company Becton, Dickinson, and Co. According to the indictment, while employed at BD, Maniar downloaded approximately 8,000 BD files, which included highly valuable confidential and trade secret information related to the company's pre-fillable disposable pen injectors.[18] The government has alleged that Maniar was planning to relocate to India at the time he was arrested, and that he intended to use BD's trade secret information to obtain employment there. Maniar is currently in plea negotiations with the government.

Criminal Prosecutions Under the CFAA, Federal Fraud Statutes and State Law

Although most of the 2013 criminal trade secret cases were brought under the EEA, there also have been several prosecutions under the Computer Fraud and Abuse Act (CFAA), and some significant prosecutions related to trade secret theft under federal fraud statutes. In addition, 2013 saw new developments in the high-profile *Aleynikov* trade secret case, involving the prosecution of a former Goldman Sachs programmer under state law, after the Second Circuit reversed his conviction under the EEA.

United States v. Liu (W.D.N.Y.)[19]

In October, the FBI arrested Yi Liu, a former employee of Sprung-brett RDI Inc., a New York company working to develop an ''electric actuation system'' for U.S. military submarines and fighter jets. Liu was charged under the EEA and the CFAA for allegedly stealing trade secrets and unlawfully accessing 277,000 Sung-brett files using a company laptop during the seven months after he left the company. If convicted, Liu could face a maximum penalty of 60 years in prison and a fine of $3.5 million.[20]

---

[10] *See* U.S. Intellectual Property Enforcement Coordinator, *Joint Strategic Plan on Intellectual Property Enforcement* 43 (2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

[11] *See* FBI, ''What We Investigate,'' *available at* http://www.fbi.gov/about-us/investigate.

[12] *See Administration Strategy*, *supra* n.8, *Summary of Dep't of Justice Economic Espionage and Trade Secret Criminal Cases January 2009—Present (Updated January 2013)*, at 1-9.

[13] No. 13 Cr. 00150 (S.D. Ind.).

[14] No. 12 Cr. 00296 (W.D. Mo.).

[15] No. 11 Cr. 00208 (D.N.J.).

[16] No. 13-2282 (3d Cir.).

[17] No. 13 Mj. 06085(D.N.J.).

[18] *See* Press Release, U.S. Dep't of Justice, *Former Engineer for Global Medical Technology Corporation Charged With Stealing Trade Secrets From New Jersey Employer* (June 5, 2013), *available at* http://www.justice.gov/usao/nj/Press/files/Maniar,%20Ketankumar%20Arrest%20News%20Release.html.

[19] No. 13 Cr. 00226 (W.D.N.Y.).

[20] *See* FBI Press Release, *Former Employee of Amherst Technology Firm Indicted for Stealing Trade Secrets*, (Oct. 23, 2013), *available at* http://www.fbi.gov/buffalo/press-releases/

United States v. Zhu (S.D.N.Y.)[21]

A recent criminal case filed in the U.S. District Court for the Southern District of New York illustrates how federal fraud statutes can be used to prosecute theft of confidential, proprietary information.

In October, two researchers at New York University were charged with several bribery counts, as well as honest services fraud,[22] based on their alleged scheme to defraud the University out of ''the intangible right to their honest services.'' Although the Supreme Court narrowed the scope of the ''honest services'' statute in 2010, making clear that it ''criminalizes *only* bribe-and-kickback'' schemes (rather than all types of self-dealing),[23] the conduct alleged here—i.e., ''conspir[ing] to receive bribes . . . in exchange for acquiring and transferring . . . certain research and non-public information''—appears to fall within that now-limited scope.

According to the indictment, Yudong Zhu agreed to provide a Chinese company with non-public information related to the University's new MRI technology. In return, the Chinese company allegedly agreed to provide Zhu with kickbacks in the form of royalty payments worth $2 million, stock options valued at $23 million, and a high-level position with the company. Together with co-defendant Ye Li, Zhu allegedly flew to China to discuss the arrangement with the Chinese company in 2012. In February 2013, Zhu allegedly received an initial payment of $400,000 from the Chinese company before he was arrested.

United States v. Zhao (E.D. Wis.)[24]

On April 11, the Department of Justice announced charges against former research scientist Hua Jun Zhao for tampering with a federally-protected computer and for lying to the FBI in connection with an economic espionage investigation.[25] Zhao was originally charged in a criminal complaint under the EEA for stealing an anti-cancer compound from his former employer, the Medical College of Wisconsin.[26] On February 27, Zhao was allegedly suspended from the Medical College and denied access to the labs in connection with the disappearance of three vials of the anti-cancer compound.[27] The indictment alleged that Zhao later attempted to access his work computer in an effort to delete information relating to the compound and obstruct the economic espionage investigation. Zhao ultimately pled guilty to the computer fraud charge.[28] On August 6, he was sentenced to time served and two years of supervised release.

People v. Aleynikov (N.Y. Sup. Ct.)[29]***; Aleynikov v. Goldman Sachs Grp., Inc. (D.N.J.)***[30]***; (3d Cir.)***[31]

As discussed in last year's *Trade Secrets Litigation Round-Up*,[32] the Second Circuit in 2012 reversed the conviction of Sergey Aleynikov, a former computer programmer for Goldman Sachs Group Inc. who had been found guilty of stealing computer source code for Goldman's high-frequency trading program in violation of the National Stolen Property Act (NSPA) and the EEA. After the reversal of his federal conviction, Aleynikov was arrested in August 2012 and arraigned on state felony charges for unlawful use of secret scientific material and unlawful duplication of computer related material.[33] Aleynikov entered a plea of not guilty in New York County Criminal Court, where the case against him remains pending.

Aleynikov also initiated a federal action against Goldman in the U.S. District Court for the District of New Jersey, seeking indemnification for the attorneys' fees and expenses that he incurred in the federal criminal action, and an advancement of the attorneys' fees and expenses that he is incurring in the state criminal case.[34] Goldman filed a counter-claim against Aleynikov, alleging breach of contract, trade secret misappropriation, and conversion, and seeking a declaratory judgment that Goldman is not liable for malicious prosecution (in response to alleged statements by Aleynikov's counsel that he intended to file such a claim).

In October 2013, the court granted in part Aleynikov's motion for summary judgment, ordering Goldman to pay Aleynikov's legal fees and expenses incurred to date in connection with the New York state criminal case, and to advance Aleynikov all such fees and expenses related to the state criminal case ''as they are incurred going forward.'' In a subsequent opinion, the court denied Aleynikov's motion to dismiss Goldman's counter-claims.

Goldman has appealed the district court's summary judgment ruling on the advancement of attorneys' fees and expenses to the Third Circuit, arguing, in part, that Aleynikov was not an ''officer,'' entitled to indemnification and advancement.[35] The Third Circuit is heard oral argument on Jan. 21, 2014.

2013/former-employee-of-amherst-technology-firm-indicted-for-stealing-trade-secrets.

[21] No. 13 Cr. 00761 (S.D.N.Y.).

[22] *See* 18 U.S.C. §§ 1343 and 1346.

[23] *See Skilling v. United States*, 561 U.S. 358, 130 S. Ct. 2896, 2932-33 (2010).

[24] No. 13 Cr. 00058 (E.D. Wis.).

[25] *See* Press Release, U.S. Dep't of Justice, *Defendant Charged with Attempting to Damage a Protected Computer* (Apr. 11, 2013), *available at* http://www.justice.gov/usao/wie/news/2013/pr20130411_Protected_Computer_Damage_Charge.html.

[26] *Id.*

[27] *See* Bruce Vielmetti, ''Suspended Medical College Researcher Indicted on Computer Fraud, Lying Charges,'' *Wis. Milwaukee J. Sentinel* (Apr. 11, 2013), *available at* http://www.jsonline.com/news/crime/suspended-medical-college-researcher-indicted-on-computer-fraud-lying-charges-n99h67m-202599901.html.

[28] *See* Andrew Harris, ''Researcher Accused of Espionage to Admit to Lesser Crime,'' *Bloomberg* (July 3, 2013), *available at* http://www.bloomberg.com/news/2013-07-03/cancer-drug-researcher-to-plead-guilty-to-computer-crime.html.

[29] No. 60353/2012 (N.Y. Sup. Ct.).

[30] No. 12 Cv. 05994 (D.N.J.).

[31] No. 13-4237 (3d Cir.).

[32] *See* Jason C. Schwartz, Alexander H. Southwell, Molly T. Senger and Sue J. Bai, ''2012 Trade Secret Litigation Round-Up,'' 85 *Bloomberg BNA's Patent, Trademark & Copyright Journal* 392, (85 PTCJ 392, 1/18/13) (''2012 TS Round-Up'').

[33] *See People v. Aleynikov*, No. 60353/2012 (N.Y. Sup. Ct.).

[34] *See Aleynikov v. Goldman Sachs Group, Inc.*, No. 12 Cv. 05994 (D.N.J.).

[35] *See* No. 13-4237 (3d Cir.).

  PTCJ ISSN 0148-7965

Prosecutors Face Increasing Difficulties Serving Foreign Companies

During 2013, federal prosecutors faced increasing difficulties effecting service on foreign corporations alleged to have stolen U.S. companies' trade secrets. Federal Rule of Criminal Procedure 4(c), which governs service on organizational defendants, provides that ''[a] copy [of the summons] must also be mailed to the organization's last known address within the district or its principal place of business elsewhere in the United States.''[36] Although the rule arguably only requires the mailing of a summons as a supplemental means of providing service, foreign corporations have successfully argued that the mailing of a summons to a defendant's place of business in the United States is, in fact, *required* to properly effect service. Thus, these defendants have argued, where no such place of business exists in the United States, service cannot be accomplished, and the case cannot proceed.

At the behest of the Department of Justice, the federal judiciary's rulemaking body is currently considering an amendment to clarify the meaning of Fed. R. Crim. P. 4(c)(3)(C).[37] In the meantime, however, prosecutors continue to struggle in proving that service has been properly made on foreign corporations in criminal trade secrets cases.

United States v. Liew (N.D. Cal.)[38]

In February 2012, the Department of Justice charged four individuals and five corporations, including Panang Group Co. Ltd.—an entity controlled by the Chinese government—with theft of trade secrets related to DuPont's titanium dioxide products, which are used to produce specialized coatings and plastics. As noted in last year's *Trade Secrets Litigation Round-Up*,[39] the case was significant not only because it represented the first foreign economic espionage prosecution against a corporation, but also because it directly asserted that representatives of the Chinese government were involved in the trade secret theft.

In April, however, Panang won a motion to quash service, on the grounds that Rule 4(c) requires mailing of the summons to an address within the district or elsewhere in the United States. The court concluded that ''the drafters [of Rule 4(c)] intended the mailing requirement to be a mandatory component of effective service.''[40] The court also held that the government had failed to establish that the individuals and entities whom it had properly served in the United States were the agents or alter egos of Panang.[41]

Despite the lack of proper service on Panang, the case has continued against the individual named defendants and the U.S. corporate defendant. In a subsequent ruling in June, the court denied a motion to dismiss filed by three of the individual defendants and the U.S. corporate defendant (U.S.A. Performance Technology Inc.), who argued that the charges against them were unconstitutionally vague because the trade secrets they allegedly attempted to steal were not described with the requisite level of specificity. Rejecting this argument, the court found that since the defendants were charged with ''*attempted* economic espionage and *attempted* theft of trade secrets,'' these charges did ''not require proof of an actual trade secret.''[42] As the Court explained, ''it is the Defendants' intent and their actions that form the 'core criminality' of these charges, rather than the existence of the asserted trade secret.''[43] Thus, because the defendants' guilt depended ''upon their intent and their actions, rather than on 'a specific identification of fact,' ''—i.e., the allegedly stolen trade secrets—the charges against them were deemed sufficient to withstand a motion to dismiss.[44]

On Jan. 7, 2013, the court concluded voir dire for the jury trial against defendants Walter Liew, Robert J. Maegerle, and U.S.A. Performance Technology Inc. and the trial began. As of the date this review was written, the trial was still underway.

United States v. Kolon Indus., Inc. (E.D. Va.)[45]

In late 2012, prosecutors indicted the South Korean company Kolon Industries Inc. and five of its executives for theft of trade secrets related to the Kevlar technology produced by DuPont. This indictment followed civil litigation (discussed below), currently on appeal to the Fourth Circuit, in which a federal jury awarded DuPont a $920 million verdict.

In contrast to the court's decision in *Liew*, the U.S. District Court for the Eastern District of Virginia in *Kolon Industries* held that mailing under Rule 4(c) ''is not a component of effective service of a summons. Nor is mailing a necessary prerequisite to the exercise of jurisdiction over a foreign corporation which does not have a 'last known address within the district or to its principal place of business elsewhere in the United States.' ''[46] Nonetheless, the court found that the government needed to satisfy Rule 4's requirement of delivery to ''an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process.''[47] According to the court, the government failed to establish that any of the U.S. entities it served were the alter egos or general agents of Kolon, and the service that had been made pursuant to a mutual legal assistance treaty (MLAT) arrived two days after the scheduled appearance, rendering it ineffective.[48]

The court did not, however, dismiss the indictment, thereby suggesting that service still could be accomplished under the MLAT or otherwise. Over the past year, there has been a flurry of briefing on this issue, culminating in a recent Sur-Sur-Sur-Reply filed by the government. On Jan. 9, the government filed a notice of additional service, which was effected in Korea. As of the date this review was written, the court has not yet

[36] Fed. R. Crim. P. 4(c)(3)(C).
[37] *See* Memo to Criminal Rules Advisory Committee from Reporters (Sept. 24, 2013), *in* Advisory Committee on Criminal Rules, Salt Lake City, Utah (Oct. 18, 2013), at 104-156, *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2013-10.pdf.
[38] No. 11 Cr. 00573 (N.D. Cal.).
[39] *See* 2012 TS Round-Up, *supra* n.32.
[40] Slip op. at 10 (April 8, 2013).
[41] *Id.* at 10-11.
[42] *See United States v. Liew*, 2013 BL 153735, at *5 (N.D. Cal. June 11, 2013) (emphasis added).
[43] *Id.* at *6.
[44] *Id.* (citation omitted).
[45] No. 12 Cr. 00137, 926 F. Supp. 2d 794, 2013 BL 49906 (E.D. Va.).
[46] *Id.* at 802.
[47] *Id.*
[48] *Id.* at 820.

ruled on what is required to properly effect service on Kolon.

United States v. Sinovel Wind Grp. (W.D. Wis.)[49]

In one of the highest-profile EEA cases of 2013, the Department of Justice indicted the Chinese company Sinovel Wind Group and several of its employees for stealing trade secrets valued at $800 million from an American wind-turbine company, American Superconductor Corp.[50]

One of the individual defendants, Dejan Karabasevic, formerly headed the automation engineering department at an AMSC facility in Austria. The other two individual defendants—Su Liying and Zhao Haichun—were Sinovel managers. According to the indictment, Sinovel and its employees recruited Karabasevic to leave AMSC and join Sinovel, and bring with him the source code for software for part of AMSC's wind turbine electrical control system (PM3000). Sinovel allegedly then commissioned several turbines in Massachusetts using the trade secrets at issue. Upon the announcement of the charges, U.S. Attorney for the Western District of Wisconsin John W. Vaudreuil called the plan ''nothing short of attempted corporate homicide,'' and Acting Assistant Attorney General Mythili Raman commented that ''[s]tamping out intellectual property theft is a top priority for this administration, and we will continue to work with our IP Task Force partners to ensure that American ingenuity is protected.''[51]

Sinovel contends that Rule 4's mailing provision is mandatory to perfect service, and that none of the individuals or entities that were served in the United States was a proper agent of Sinovel authorized to accept service. The court has not yet ruled on Sinovel's motion.

Appellate Decisions on the EEA

Both the Sixth Circuit and Seventh Circuit issued significant decisions interpreting the EEA, which may serve to lessen the burden on prosecutors seeking to prove EEA violations and damages resulting therefrom.

United States v. Jin (7th Cir.)[52]

The Seventh Circuit Court of Appeals recently had occasion to consider the nature of the ''injury'' required to sustain a trade secret conviction under the EEA.

Hanjaun Jin, formerly a Motorola Inc. software engineer, was arrested at Chicago's O'Hare International Airport in February 2007 while attempting to board a flight to China, carrying $31,000 and thousands of proprietary Motorola documents detailing the company's ''push-to-talk'' iDEN technology. After being convicted and sentenced to four years in prison, Jin appealed, arguing that the information at issue was not a trade secret under the EEA, and that she could not be convicted under the EEA because ''she neither intended nor knew that the theft would harm Motorola.''[53]

The trade secret misappropriation provision of the EEA requires ''intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof,'' as well as intent or knowledge that the offense will injure the owner of the trade secret.[54] The EEA further defines a trade secret as information that ''derives independent economic value, actual or potential, from not being generally known.''[55]

In *Jin*, Judge Richard Posner, writing for the court, concluded that the ''government doesn't have to prove that the owner of the secret actually lost money as a result of the theft'' to sustain a conviction under the EEA.[56] Thus, the court found, it was sufficient that the misappropriated iDEN technology at issue had potential economic value, and that Motorola was injured by the revelation that it ''couldn't keep secrets or prevent rivals from stealing its technology.''[57] Even assuming that iDEN was outdated and had diminishing commercial value at the time it was misappropriated, Posner explained that Motorola still would have had ''to warn its customers of the risk that privacy of communications over the iDEN network had been or would be compromised. And it would have had to take countermeasures at some expense to itself.''[58] Moreover, the court found, Jin would have known that such warnings and countermeasures on the part of Motorola would be necessary.[59] Accordingly, the court held there was sufficient injury and intent to injure to support the EEA conviction.

United States v. Howley (6th Cir.)[60]

The U.S. Court of Appeals for the Sixth Circuit made clear in 2013 that sentencing for the theft of trade secrets under the EEA, which is tied to the amount of the loss sustained, does not require the government to establish an ''exact figure for the loss a victim suffered or the amount of harm a defendant caused or intended to cause''; instead, the Sixth Circuit found, a ''reasonable estimate will do.''[61]

Howley involved the conviction of two former Wyko Tire Technology employees for trade secret theft. A jury found the two defendants—Sean Howley and Clark Roberts—guilty of stealing trade secrets related to Goodyear Tire & Rubber Co.'s tire manufacturing process for large earth-moving equipment. The defendants had accessed a Goodyear plant under the pretext of repairing Wyko equipment in the facility, and, while there, took photographs of Goodyear's manufacturing technology. The photographs were intended to assist Wyko in designing items needed for a contract with a Chinese competitor to Goodyear.

At sentencing, the government contended that the theft had cost Goodyear between $305,000 and $520,000, but the district court held that the estimates were not sufficiently well-grounded. As a result, the court refused to increase the offense level under the

[49] No. 13 Cr. 00084 (W.D. Wis.).
[50] *See* DOJ Press Release, *Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets* (June 27, 2013), *available at* http://www.justice.gov/opa/pr/2013/June/13-crm-730.html.
[51] *Id.*
[52] 733 F.3d 718, 2013 BL 260373 (7th Cir. 2013).
[53] *Id.* at 720.
[54] *See* 18 U.S.C. § 1832(a).
[55] *Id.* § 1839(3)(B).
[56] 733 F.3d at 721.
[57] *Id.* at 722.
[58] *Id.* at 720.
[59] *Id.*
[60] 707 F.3d 575, 2013 BL 28430, 105 U.S.P.Q.2d 1886 (6th Cir. 2013) (85 PTCJ 472, 2/8/13).
[61] *Id.* at 582 (internal quotation marks omitted).

   ISSN 0148-7965

Sentencing Guidelines, and sentenced Howley and Roberts as if there had been no loss at all.[62]

Reversing and remanding the judgment of the district court, the Sixth Circuit explained that a finding of no loss was at odds with an EEA trade secrets conviction, which requires that the stolen property have some ''independent economic value.''[63] According to the court, ''On remand, the district court need not be exacting. The guidelines require only a 'reasonable' estimate of actual or intended loss within broad ranges. But the court must at least provide an estimate and reasons for it.''[64]

On remand, the district court sentenced both defendants to four years of probation and 150 hours of community service, rejecting the government's renewed request for imprisonment based on the value of the loss sustained.

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) provides both federal civil and criminal causes of action against any person who, in relevant part, ''intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer,'' or who ''intentionally accesses a protected computer without authorization and as a result of such conduct, causes damage and loss.''[65] Claims of trade secret misappropriation are often brought together with claims under CFAA, since employees attempting to steal their employers' trade secrets frequently do so by accessing confidential information on their employers' computers. In order for an employee's conduct to violate CFAA, however, the employee must not be authorized to access the computer, or he must have ''exceed[ed] authorized access.'' In 2013, courts continued to debate what it means to ''exceed authorized access'' under CFAA.

Continued Debate Over ''Authorized Access''

The Second, Fourth, and Ninth Circuits all have taken the ''narrow'' view, holding that merely accessing information in violation of an employer's computer usage policy is insufficient to state a claim under CFAA, as CFAA was not intended to criminalize ''minor dalliances'' such as ''g-chatting with friends, playing games, shopping or watching sports highlights'' on a computer that an individual had a right to access.[66] In contrast, the Fifth, Seventh, and Eleventh Circuits all have taken the ''broad'' view, holding that any type of access that furthers an interest adverse to the employer violates the statute, even when access to the computer itself is authorized.

Entering 2013, many speculated that the Supreme Court would resolve this circuit split by granting certiorari in the Fourth Circuit case, *WEC Carolina Energy Solutions, LLC v. Miller*.[67] However, on Jan. 2, 2013, the parties stipulated to the dismissal of the petition for certiorari.[68]

There was also legislative interest in clarifying CFAA in the wake of the tragic suicide of MIT student Aaron Schwartz, whom federal authorities had charged under CFAA for accessing thousands of articles from a database of academic articles. For example, the proposed ''Aaron's Law,''[69] would have removed the ''exceeds authorized access'' language from CFAA, and redefined ''access without authorization'' to require ''knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information.'' Aaron's Law, however, was not reported out of committee in 2013.

In 2014, litigants in the First, Third, Sixth, Eighth, Tenth and D.C. Circuits continue to lack controlling precedential guidance on the scope of CFAA. And, as the latest *Nosal* decision shows, even within one side of the existing circuit split, there remain significant unresolved questions regarding CFAA's intended scope.

United States v. Nosal (N.D. Cal.)[70]

Nosal involves a long-running criminal CFAA prosecution of David Nosal, a former executive search firm employee. Nosal was charged with conspiring to violate CFAA by allegedly enlisting several of his former firm's employees to obtain confidential information from the firm's ''Searcher'' database, which Nosal intended to use to start a competing executive search firm. At the first trial, the district court held that there had been no violation of CFAA because the employees who accessed the database on Nosal's behalf were authorized to do so, even though the purpose of their actual use violated their employer's computer usage policy. A panel of the Ninth Circuit reversed, taking the ''broad'' view that violating an employer's terms of use is sufficient to violate CFAA. In 2012, the Ninth Circuit, sitting en banc, reversed the panel, adopting the ''narrow'' view that the phrase ''exceeds authorized access'' in CFAA does not extend to mere violations of an employer's computer use restrictions.

Returning to district court, Nosal moved for dismissal of the CFAA conspiracy counts against him, arguing that the en banc Ninth Circuit decision required the government to allege ''the circumvention of technological access barriers''—i.e., hacking—since a mere violation of computer use restrictions is insufficient to prove a CFAA violation. Rejecting that argument, the district court explained that the en banc opinion did not ''explicitly hold that the CFAA is limited to hacking crimes,'' and, in fact, did not address ''the *manner* in which access is limited, whether by technological barrier or otherwise.''[71] As the court explained, ''*Nosal* holds only that it is not a violation of the CFAA to access a computer with permission, but with the intent to use the information gained thereby in violation of a use agreement.''[72] But conduct that falls short of ''hacking'' may still constitute unauthorized access or access that ''exceeds authorization'' within the meaning of CFAA.[73]

The court then went on to reject what it characterized as Nosal's ''constrained and hypertechnical definition

[62] *See id.*
[63] 18 U.S.C. § 1839(3)(B).
[64] 707 F.3d at 583.
[65] *See* 18 U.S.C. § 1030(a)(2)(C), (a)(5)(C), (g) (2012).
[66] *United States v. Nosal*, 676 F.3d 854, 860, 2012 BL 89201 (9th Cir. 2012) (en banc).
[67] 687 F.3d 199 (4th Cir. 2012).
[68] 133 S. Ct. 831.
[69] H.R. 2454/S.1196, 113th Cong. (2013).
[70] No. 08 Cr. 00237, 930 F. Supp. 2d 1051, 2013 BL 65962 (N.D. Cal.).
[71] 930 F. Supp. 2d at 1060.
[72] *Id.*
[73] *See id.*

of 'access' in which access focuses solely on the moment of entry and nothing else.''[74] Nosal had argued that an initial employee—J.F.—''accessed'' the Searcher database when she logged in using her password, and that a second employee—M.J.—*used* the system after it had been *accessed* by J.F. Under Nosal's theory, then, M.J. did not engage in ''unauthorized 'access' within the meaning of the statute,'' since J.F., rather than M.J., had accessed the files.[75] Dismissing this argument, the court explained that such a reading of the CFAA would ''produce a non-sensical result,'' since it would permit an individual to evade prosecution by looking ''over the shoulder of the authorized user to view password protected information or files.''[76] Thus, the court found, the government had sufficiently stated a claim against Nosal based on M.J.'s unauthorized access of the Searcher database for Nosal's benefit, after J.F. had logged into the database with her password.[77]

At the subsequent trial, Nosal was again convicted by a jury. He moved for a new trial and/or an acquittal, again alleging that the underlying conduct at issue was outside the scope of CFAA. Nosal argued that because he was still working for his firm as an independent contractor with access to the underlying information at issue at the time that it was retrieved, it was irrelevant who had actually accessed the ''Searcher'' database or how he or she had done so. In an Aug. 15 order, the court rejected this argument, explaining that the ''text of the statute . . . is concerned not with permission to access *information*, but rather with permission to access a protected *computer*.''[78] As the court explained, ''[j]ust because a person is authorized generally to receive information from a database does not mean that person can deputize any other person, including one without authorization, to access the computer in clear violation of an employer's rule.''[79] Moreover, the court emphasized, the evidence presented at trial demonstrated that Nosal ''did *not* actually have unqualified access to all of the information on [his former employer's system]'' in his capacity as an independent contractor.[80] The Court thus upheld Nosal's conviction under CFAA.[81]

On Jan. 8, 2014, the court sentenced Nosal to a year and a day in prison, followed by three years of supervised release, 400 hours of community service, and $60,000 in fines. Nosal has filed a motion for release pending appeal, which is set for hearing on Feb. 12, 2014.

CIVIL DEVELOPMENTS

Outside of situations in which CFAA may provide a civil right of action, state law continues its traditional dominance in trade secret civil suits. As discussed above, 47 states and the District of Columbia all have adopted a version of the Uniform Trade Secrets Act (UTSA). But despite the thousands of decisions across these jurisdictions interpreting the UTSA, courts in 2013 continued to confront novel questions related to the types of information that can qualify for trade secret protection and the steps that a trade secret owner must take to protect information in order for it to qualify as a trade secret.

Information Eligible for Trade Secret Protection

First Express Servs. Grp., Inc., v. Easter (Neb.)[82]

A recent decision by the Nebraska Supreme Court on the meaning of a ''trade secret'' underscores the significance of changes that certain states have made to their versions of the UTSA. *Easter* involved a crop insurance agent who left her prior agency and took with her a customer list ''which was available only by logging in using . . . a password.''[83] The list included customer names, contact information, location and types of crops, types of insurance coverage, and size of commission.[84] After joining her son's competing insurance firm, the defendant-agent sent her customers a letter ''informing them of her resignation and soliciting their business,'' and in some cases, she prepared draft forms transferring her former clients' insurance policies for their signature.[85] The defendant's former employer brought suit, alleging trade secret misappropriation under Nebraska law.

The state's high court concluded that the customer list at issue was not a trade secret under Nebraska's version of UTSA. In most states, a trade secret is defined as information that derives independent economic value ''from not being *generally* known . . . and not being *readily* ascertainable by proper means.''[86] Nebraska, however, deleted the words ''generally'' and ''readily'' from its version of the UTSA, thereby greatly narrowing its definition of a trade secret.[87] The court found that the customer list at issue was not protected under this narrowed definition, because all of the information included in the list was available by proper means: the Internet provided most of the information about the customers' crops and contact information; the agent could recite much of it from memory; and the information regarding prior coverage could be obtained either from the customers themselves or from the prior agency with the customers' authorization.[88] As a result, the court held that the customer list was not a trade secret, and reversed the jury's verdict on the misappropriation claim.[89]

Wellington Resource Grp., LLC v. Beck Energy Corp. (S.D. Ohio)[90]

A federal district court in Ohio recently considered when knowledge of a business opportunity can qualify for trade secret protection.

Wellington Research Group LLC had a contract with Beck Energy Corp. to identify possible buyers of Beck's oil-and-gas assets, pursuant to which Beck agreed to pay Wellington 5 percent of the total purchase price, if

[74] *Id.* at 1063.
[75] *Id.* at 1062.
[76] *Id.*
[77] *Id.* at 1057, 1063.
[78] 2013 BL 245007, at *6.
[79] *Id.*
[80] *Id.* at *7.
[81] *Id.* at *11.

[82] 286 Neb. 912 (Neb. 2013).
[83] *Id.* at 916.
[84] *Id.*
[85] *Id.* at 918.
[86] *Id.* (emphases added).
[87] *See id.* at 925.
[88] *Id.* at 925-26.
[89] *Id.* at 927.
[90] No. 12 Cv. 00104, 2013 BL 254028 (S.D. Ohio Sept. 20, 2013).

  PTCJ ISSN 0148-7965

and when Wellington successfully identified a purchaser for Beck. Wellington, in turn, contracted with Marcellus Shale Land Acquisition Group LLC to leverage MSLAG's resources to find a buyer for Beck's assets, and agreed to provide MSLAG with half of Wellington's finder's fee in exchange for MSLAG's services. MSLAG subsequently identified XTO Energy Inc. as a potential buyer, and introduced XTO to Wellington, which, in turn, introduced XTO to Beck. XTO eventually bought approximately $86 million of Beck's assets. After the sale, Wellington requested its 5 percent compensation from Beck, but Beck refused to pay Wellington its finder's fee. MSLAG, in turn, requested its agreed-upon percentage of Wellington's fee, but was refused (as Wellington had received no compensation from Beck). In addition to other claims, MSLAG alleged that Beck had misappropriated a trade secret under Ohio's version of the UTSA. Beck moved to dismiss, and the court denied the motion, finding that ''confidential, proprietary information regarding business opportunities in the oil and gas development industry, including the opportunity with XTO,'' could qualify for trade secret protection as information that derives ''independent economic value . . . from not being generally known.''[91]

Cent. Trust & Invest. Co. v. Kennedy (Mo. Ct. App.)[92]

In a case demonstrating the importance of well-drafted non-competition agreements, a Missouri appellate court recently held that a financial services firm's client list did not qualify for trade secret protection under that state's version of the UTSA.

Central Trust & Investment Co. sued Kennedy, a former employee who started a competing firm, alleging that he misappropriated Central Trust's client lists. The appellate court upheld the trial court's grant of summary judgment for the employee, emphasizing the multiple ways in which the company had allowed free access to its client information by its employees and affiliates. The court also noted that ''attached to Kennedy's employment contract was a list of his clients with no matching provision that such information was to remain confidential in any way.''[93] In addition, the court found that Central Trust had failed to meet its burden of establishing that the client information had ''any recognizable extrinsic or intrinsic value.''[94] Nor was Central Trust protected by the non-competition agreement that Kennedy had signed, as the agreement specifically stated that it would be rendered void upon a change in control of the Central Trust—which was, in fact, the event that precipitated Kennedy's departure.[95]

Sarkissian Mason v. Enter. Holdings, Inc. (S.D.N.Y.)[96]***; (2d Cir.)***[97]

Another court applying Missouri law—this one in New York, under choice-of-law rules—recently held that a marketing idea for the sale of used cars was not a protectable trade secret because it did not meet the UTSA requirement of having ''independent economic value, actual or potential, from not being generally known . . . and not being readily ascertainable by proper means.'' Subject to a Non-Disclosure Agreement, Sarkissian Mason Inc. presented Enterprise Holdings Inc. with a proposal that would enable customers to use their mobile devices to obtain price quotes for used cars and to contact dealers. The parties ultimately could not reach agreement on whether Enterprise would exclusively use Sarkissian's system, and Enterprise later announced the launch of its own mobile device service.

Sarkissian sued for trade secret misappropriation, and the court granted summary judgment for Enterprise. Analogizing to Internet search engines, the court explained that while ''Google's search algorithms most certainly are a trade secret and have value . . . the idea of a search engine is not.''[98] As the court noted, the components of the mobile device system at issue were ''widely known,'' and the ''unexecuted concept'' of the mobile device was thus of ''limited value because it is readily ascertainable.''[99] The court similarly held that there had not been a misappropriation, because the two systems were ''different concepts created from a similar collection of publically available ideas concerning the use of mobile devices to connect consumers to information about products they are using or considering purchasing.''[100] Sarkissian appealed the decision to the Second Circuit, and the appeal remains pending.

Sw. Energy Prod. Co. v. Berry-Helfand (Tex. App.)[101]

A Texas appellate court recently discussed the circumstances under which public information can be transformed into a protectable trade secret. The plaintiff, Toby Berry Helfand, took public and semi-public logs from 600 wells and with ''thousands of hours of work over a period of several years'' analyzed the data to identify and map a geological formation likely to produce valuable amounts of natural gas. Helfand's analysis also specifically identified a number of so-called ''sweet spots'' for drilling.[102] In 2005, Helfand presented her findings to Southwestern Energy Production Co., pursuant to a confidentiality agreement that required Southwestern to include Helfand in any projects that it pursued to develop the ''sweet spots.'' Acting alone, Southwestern later participated in the successful development of over eighty wells clustered around the spots that had been identified by Helfand.

Helfand sued Southwestern for theft and misappropriation of trade secrets, as well as for breach of fiduciary duty, fraud, and breach of contract. Southwestern argued that the geological information could not qualify for trade secret protection. The jury disagreed, finding that the material at issue was a trade secret, and awarding approximately $40 million to Helfand in actual damages, disgorgement and interest.[103] Southwestern appealed, and in 2013, the appellate court upheld the verdict, explaining that while ''the raw data was drawn from public or semi-public sources, there is abundant evidence to support the jury's finding that this massive

[91] *Id.* at *17.
[92] No. SD31658 (Mo. Ct. App. Feb. 19, 2013).
[93] *Id.* at *5.
[94] *Id.*
[95] *Id.* at *6.
[96] No. 11 Cv. 09472, 2013 BL 185823 (S.D.N.Y. July 15, 2013).
[97] No. 13-3052 (2d Cir.).
[98] 2013 BL 185823 at *10.
[99] *Id.*
[100] *Id.* at *11.
[101] 411 S.W.3d 581 (Tex. App. 2013).
[102] *Id.* at 597.
[103] *Id.* at 590.

compilation and analysis was a trade secret.''[104] The court also upheld the finding of misappropriation, concluding that it was reasonable for the jury to find misappropriation when ''[d]espite a well recorded aversion to . . . drilling [in specific areas] before meeting Helfand, shortly thereafter [Southwestern] zealously pursued . . . opportunities that coincided with Helfand's sweet spots.''[105]

Adequacy of Steps to Protect Secrets

Convolve, Inc. v. Compaq Computer Corp. (Fed. Cir.)[106]

A recent decision of the Federal Circuit illustrates the importance of complying with non-disclosure agreements in order for information to merit protection as a trade secret.

Convolve Inc. executed a non-disclosure agreement with Seagate during the parties' negotiations regarding the potential licensing of Convolve's hard drive manufacturing technology. The NDA required, among other things, that the disclosing party designate protected, confidential information as such at the time of disclosure and in a follow-up written notice. The Federal Circuit held that because Convolve had not provided the written notice required by the terms of the NDA, and because there had been no waiver of the NDA's written notice or marking requirements, ''Seagate did not breach the NDA to the extent that it may have appropriated the information disclosed.''[107]

Having thus affirmed the dismissal of Convolve's breach-of-contract claims, the Federal Circuit also went on to reject Convolve's trade secret misappropriation claim under the California UTSA. According to the court, the NDA had the effect of superseding any other implied duty of confidentiality in the materials covered by the agreement.[108] Thus, because the NDA with Seagate ''cover[ed] the substance of the information disclosed . . . the NDA control[led] the entirety of the parties' relationship regarding those disclosures,'' and Convolve's failure to ''follow the procedures set forth in the NDA to protect the shared information'' was fatal to Convolve's trade secret misappropriation claim.[109]

State ex rel. Luken v. Corp. for Findlay Market of Cincinnati (Ohio)[110]

The Ohio high court also recently considered the nature of the efforts required to protect the secrecy of information in order for that information to qualify as a trade secret.

Luken involved a citizen's attempt to obtain unredacted copies of certain subleases under a state public records law. The subleases at issue were for tenants in a market that was owned by the city of Cincinnati, and which was operated by and leased to a public-private corporation. The state argued that it was not required to produce the requested subleases as a result of their trade secret status, since the state public records law exempts ''trade secrets'' from disclosure. The citizen countered that the market had not taken sufficient steps to protect the information in the subleases for them to qualify as a trade secret. The court conceded that ''the leases do not require tenants to keep the information secret,''[111] but went on to note that the corporation retained its ''unredacted copies of the leases in a locked filing cabinet and allows access only to employees who need the information.''[112]

On balance, the court concluded that while ''the corporation could have taken more care in keeping the information secret,'' the trial court was within its discretion to hold that the measures undertaken were adequate, given that they were ''standard for the industry.''[113]

Damages

2013 bore witness to Kolon's challenge to the $920 verdict entered against it in its high-profile trade secrets battle with DuPont, and to a Ninth Circuit decision vacating a $172 million award to MGA in its longstanding Bratz doll trade secret dispute with Mattel. Below, we discuss these and other significant 2013 trade secret cases involving blockbuster verdicts.

E.I. DuPont De Nemours & Co. v. Kolon Indus., Inc. (4th Cir.)[114]

As discussed above, in 2012, the South Korean company Kolon Industries Inc. and five of its executives were indicted for criminal trade secrets theft, based on their alleged misappropriation of trade secrets related to DuPont's Kevlar technology. In a parallel civil action brought by DuPont against Kolon, a federal jury found that Kolon had, in fact, misappropriated trade secrets relating to the manufacture of Kevlar, and awarded DuPont $920 million in damages. The court also entered a 20-year worldwide injunction, barring Kolon from manufacturing Heracron—its product allegedly made with DuPont's trade secrets. The Fourth Circuit granted a stay of the injunction pending appeal.

In the spring of 2013, Kolon argued that the judgment was flawed in several respects. First, it claimed that the trial court should have required DuPont to more specifically address each of the 149 trade secrets at issue. It also argued that the $920 million verdict was excessive and not connected to any harm DuPont incurred, and that the injunction was inconsistent with the damages award. According to Kolon, DuPont should not receive both full compensation for its research and development costs and the benefit of the court blocking Kolon from competing in the marketplace.[115]

The case was argued before the Fourth Circuit on May 17, 2013. Although DuPont requested that the courtroom be closed during oral argument, the Fourth Circuit denied that request. As of this writing, the Fourth Circuit has not yet issued an opinion on Kolon's appeal. However, when handed down, the Fourth Circuit's opinion likely will significantly impact the future availability of post-judgment injunctions.

[104] *Id.* at 597-98.
[105] *Id.* at 600.
[106] 527 F. App'x 910, 2013 BL 175065 (Fed. Cir. 2013) (87 PTCJ 73, 11/8/13).
[107] *Id.* at 922.
[108] *Id.* at 925.
[109] *See id.*
[110] 988 N.E.2d 546 (Ohio 2013).
[111] *Id.* at 552.
[112] *Id.* at 551-52.
[113] *Id.* at 552.
[114] No. 12-1260 (4th Cir.).
[115] *See* Redacted Final Opening Brief, Doc. No. 90 (Feb. 22, 2013).

  PTCJ ISSN 0148-7965

Mattel, Inc. v. MGA Entm't, Inc. (9th Cir.)[116]***; MGA Entm't Inc. v. Mattel Inc. (Cal. Sup. Ct.)***[117]

The Ninth Circuit's 2013 decision vacating the $172 million award to MGA in its longstanding dispute with Mattel underscores the significance of careful pleading in trade secrets litigation.

This decision is only the latest in a hard-fought trade secrets battle that began ten years ago, when Mattel—the maker of the Barbie doll—sued MGA, alleging that Mattel employee Carter Bryant had designed the successful line of Bratz dolls while working for Mattel, and that MGA therefore had misappropriated Mattel's trade secrets by producing Bryant's design. Mattel won a jury trial on that claim, but the jury verdict was subsequently vacated by the Ninth Circuit. Before the second trial, the court granted MGA's motion to add a trade secret misappropriation counterclaim against Mattel. MGA alleged that Mattel had engaged in corporate espionage at trade fairs to view MGA's as-not-yet-released Bratz dolls. MGA styled its new claim as a compulsory counterclaim-in-reply under Federal Rule of Civil Procedure 13(a)(1)(A), which allows certain claims to be brought in a reply that otherwise would be time-barred.

The second jury found that Mattel was liable for misappropriating MGA's trade secrets, and entered an award of $172 million against Mattel. Mattel appealed the verdict, and the Ninth Circuit agreed with Mattel that MGA's counterclaim ''should not have reached the jury.''[118] Under Rule 13, a respondent can add a compulsory counterclaim-in-reply that ''arises out of the transaction or occurrence that is the subject matter of the opposing party's claim.''[119] According to the court, the fact ''[t]hat both Mattel and MGA claimed they stole each other's trade secrets isn't enough to render MGA's counterclaim compulsory.''[120] The court went on to explain that ''Mattel's specific allegations regarding trade secrets were that several of their employees . . . defected to MGA and disclosed Mattel's trade secrets.'' That allegation did not involve the ''same aggregate core of facts'' as MGA's ''allegations that Mattel's employees stole MGA trade secrets by engaging in chicanery (such as masquerading as buyers) at toy fairs.''[121] Because the claim was not mandatory, it did not qualify for special treatment under Rule 13, and was therefore time-barred as outside the three-year statute of limitations under California law.

Most recently, on Jan. 14, 2014, MGA filed a new action against Mattel in Los Angeles Superior Court, seeking $1 billion in damages for trade secret misappropriation.[122] In its complaint, MGA contends that the Ninth Circuit ''vacated without prejudice the $170 million judgment against Mattel . . . [d]ue to a technical procedural issue having nothing to do with the merits of [MGA's] claims,'' and that, ''[b]ecause of the lack of ongoing federal jurisdiction for this matter, the retrial of MGA's California Uniform Trade Secret Act claim must now take place in this Court.''[123] According to news reports, Mattel intends to defend, at least in part, on the ground that MGA's claim is barred by the statute of limitations.[124]

Wellogix, Inc. v. Accenture, LLP (5th Cir.)[125]

In 2013, the Fifth Circuit upheld a $44.4 million verdict against Accenture LLP, including $18.2 million in punitive damages, based on a jury's finding that Accenture had maliciously misappropriated the trade secrets of Wellogix Inc.

Wellogix sued Accenture and several other companies, alleging that they had misappropriated Wellogix's trade secrets, which they obtained in connection with an earlier joint project related to oil well drilling software. The suit against Accenture proceeded to trial, and a jury in the Southern District of Texas concluded that the company had, in fact, misappropriated Wellogix's trade secrets. The jury awarded Wellogix $26.2 million in compensatory damages and $68.2 million in punitive damages. Wellogix then accepted a remittitur of the punitive damages to $18.2 million, reducing the total award to $44.4 million.[126]

On appeal, Accenture argued, in part, that the damages award was unwarranted, but the Fifth Circuit rejected this argument. With respect to the compensatory damages award, the Fifth Circuit found that the jury's conclusion that Wellogix was entitled to $26.2 million was reasonable under Texas law, which allows consideration of a plaintiff's lost profits, a defendant's actual profits, the value that a third party would have paid for the secret, saved costs by the defendant, and a reasonable royalty.[127] As to the punitive damages, the court concluded that the jury was reasonable in finding malice—a prerequisite to an award of punitive damages. The panel rejected Accenture's argument that ''a defendant's supportive comments about a plaintiff, or, conversely, a plaintiff's supportive comments about a defendant, preclude a jury's finding of malice.''[128] Nor did the court find the punitive damages award, after remittitur, to violate due process by being grossly excessive.[129]

An Alternative Venue: The International Trade Commission

The International Trade Commission is an increasingly popular forum for certain types of trade secret misappropriation claims.

In 2011, the Federal Circuit found that the ITC has jurisdiction under Section 337 of the Tariff Act of 1930 over actions involving unfair trade practices that occur exclusively overseas, but that cause domestic injury.[130]

---

[116] 705 F.3d 1108, 2013 BL 20955, 105 U.S.P.Q.2d 1574 (9th Cir. 2013) (85 PTCJ 453, 2/1/13).

[117] No. BC532708 (Cal. Sup. Ct.).

[118] 705 F.3d at 1110.

[119] Fed. R. Civ. P. 13(a)(1)(A).

[120] 705 F.3d at 1110.

[121] *Id.*

[122] *See MGA Entm't Inc. v. Mattel Inc.*, BC532708 (Cal. Sup. Ct.).

[123] *Id.*, Compl. ¶ 3.

[124] *See* Edvard Pettersson, ''MGA Sues Mattel for Trade-Secret Theft, Seeks $1 Billion,'' *Bloomberg News* (Jan. 13, 2014), *available at* http://www.businessweek.com/news/2014-01-13/mga-sues-mattel-for-trade-secret-theft-seeks-1-billion-1.

[125] 716 F.3d 867, 2013 BL 129992, 106 U.S.P.Q.2d 1796 (5th Cir. 2013) (86 PTCJ 187, 5/24/13).

[126] *Id.* at 874.

[127] *Id.* at 879-81.

[128] *Id.* at 884.

[129] *Id.* at 886.

[130] *TianRui Group Co. v. Int'l Trade Comm'n*, 661 F.3d 1322 (Fed Cir. 2011).

That decision also created a uniform common law for such cases, replacing the use of state law.[131]

For plaintiffs seeking injunctive relief for trade secret misappropriation, the ITC can provide a speedier venue with more relaxed evidentiary standards than federal district courts. Although the ITC cannot issue monetary damages, it can bar imports of offending articles into the United States—which is often a major market for offending goods.

In 2013, several U.S. plaintiffs pursued trade secrets claims before the ITC, such as those discussed below.

In re Certain Paper Shredders (ITC)[132]

In January 2013, the ITC voted to open an investigation into a complaint by paper shredder manufacturer Fellowes Inc. against several respondents with Chinese ties. The company alleged that the entities and one individual misappropriated Fellowes's trade secrets and were importing competing products into the United States, which used the misappropriated technology. Fellowes alleged that the respondents took physical possession of equipment and documents and that they had hired employees of Fellowes' Chinese joint venture. In November, the parties settled their dispute, and an Administrative Law Judge initially approved a consent decree, which included a five-year ban on the importation of shredders using the trade secrets at issue. The commission approved the settlement in late December 2013.[133]

In Re Robotic Toys and Components Thereof (ITC)[134]

In January 2013, Texas-based Innovation First International Inc. a manufacturer of robotic toys including the Robo Fish and Aqua Pet, alleged that Zuru Inc. had hired a former Innovation First employee, subject to a non-competition agreement, and that Zuru and the employee had used Innovation First trade secrets to manufacture a competing product, which they sold to CVS. The ITC ordered an investigation in February, and in June 2013, the parties agreed to a settlement and consent decree, under which Zuru and CVS agreed not to import products containing the asserted trade secrets. In July, the ITC approved the settlement.

In Re Certain Rubber Resins (ITC)[135]

The ITC is currently considering a case initiated by SI Group Inc.—a manufacturer of rubber tackifiers, which are a component of rubber tires. SI Group alleges that certain companies in China, Hong Kong and Canada hired a former SI Group employee and have used SI Group's trade secrets in their own manufacturing of rubber tackifiers. In June 2013, an administrative law judge found a violation, and the ITC has ordered further investigation in conjunction with its review.[136] Notably, on the same day the ALJ issued his decision, a Chinese court rejected essentially the same argument in a parallel case. However, the commission's staff maintains that the Chinese decision is irrelevant, because the ''respondents' do not appear to argue that the Chinese Judgment makes any findings under the legal standards of 19 U.S.C. § 1337, or under U.S. federal common law of trade secret misappropriation, as applied by the Commission.''[137] The issue of the preclusive effect of other judicial determinations on an ITC proceeding has not been resolved.

Another Alternative: State Government Civil Actions

California v. Ningbo Beyond Home Textile Co. (L.A. Sup. Ct.)[138]; ***California v. Pratibha Syntex Ltd. (L.A. Sup. Ct.)***[139]

Although private litigants in trade secret cases have long relied on state unfair competition statutes, state governments have begun bringing their own civil lawsuits to combat intellectual property theft. In January 2013, California joined this recent trend. State Attorney General Kamala D. Harris filed lawsuits under the state's unfair competition law against two foreign apparel manufacturers—Ningbo Beyond Home Textile Co., which is based in China, and Pratibha Syntex Ltd., which is based in India. The lawsuits allege that Ningbo and Pratibha gained an unfair competitive advantage over American companies by using pirated software in the production of clothing imported to and sold in California. According to the complaints, the two companies combined shipped over 730,000 pounds of apparel into California from 2010 through 2012.

California alleges that Ningbo and Pratibha used pirated software from Microsoft and Adobe, among others, to lower their production costs. The state is seeking a bar on imports into California by Ningbo and Pratibha until they comply with licensing requirements. In addition, the state is seeking civil penalties and court orders, which would require the companies to certify their compliance with all software licensing requirements; to provide a bi-annual software inventory to the state for five years; and to submit to court-appointed trustees, who would to verify compliance.

Both suits are sequels to Microsoft's private litigation in foreign courts. In the case of Ningbo, Microsoft had pursued copyright infringement claims against Ningbo in a Chinese court, and during a court-ordered inspection, allegedly discovered that the company was using pirated software Microsoft valued at $351,326. The complaint against Pratibha builds on similar Microsoft litigation in India.

With these cases, California is following in the footsteps of Massachusetts, which filed a similar action in 2012 against a Thai seafood-processing company, and Washington, which used the threat of an unfair competition suit to reach a settlement with a Brazilian aircraft manufacturer in 2012.

CONCLUSION

Developments in 2013 made clear that U.S. companies in all industries continue to be vulnerable to trade secret theft from both domestic and foreign actors. Although high-profile incidents of theft tied to foreign interests dominate the headlines, companies face equally

[131] *See id.*

[132] Investigation No. 337-TA-863 (Int'l Trade Comm'n Nov. 20, 2013).

[133] *See* 78 Fed. Reg. 79,006 (Dec. 27, 2013).

[134] Investigation No. 337-TA-869 (Int'l Trade Comm'n July 9, 2013).

[135] Investigation No. 337-TA-849 (Int'l Trade Comm'n).

[136] *See* 78 Fed. Reg. 56,734 (Sept. 13, 2013).

[137] Office of Unfair Import Investigation's Response to Respondents' Notice of New Authority (Oct. 30, 2013) at 4.

[138] No. BC 499771 (L.A. Sup. Ct.).

[139] No. BC 499751 (L.A. Sup. Ct.).

   ISSN 0148-7965

significant threats from trusted employees seeking to start new businesses or defect to domestic competitors.

To guard against both types of threats, U.S. businesses should regularly assess the adequacy of their safeguards—legal, practical, physical and technological—for intellectual property. Judicial decisions in 2013 also demonstrated that well-crafted workplace policies and non-disclosure agreements can mean the difference between success and failure in a subsequent action for misappropriation of trade secrets or other valuable intellectual property.

As the legal environment continues to evolve, U.S. companies confronting the loss of trade secrets should consider the growing range of forums and types of actions available to them and to prosecutors. As demonstrated by this year's developments, the federal and state governments are increasingly sensitive to the harm done by trade secret theft, and can be valuable allies in this battle.