Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

TRADE SECRETS

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

2011 Trade Secrets Litigation Round-Up



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

INTRODUCTION

Information security has become one of the top priorities for corporate executives and board members in 2012, according to a November 2011 survey from the Corporate Executive Board Co. *See* Emily Chasen, *Information Security Jumps to Top Priority for Audit Committees* (Nov. 28, 2011), *available at* http://blogs.wsj.com/cfo/2011/11/28/information-security-jumps-to-top-priority-for-audit-committees/.

Jason C. Schwartz is an employment litigation partner with Gibson, Dunn & Crutcher, Washington, D.C., His 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 is a litigation associate in Gibson Dunn's Washington, D.C., office.

And with good reason.

A recent report by the U.S. Office of the National Counterintelligence Executive found that ''FIS [Foreign Intelligence Services], corporations, and private individuals increased their efforts in 2009-2011 to steal proprietary technologies, which cost millions of dollars to develop and represented tens or hundreds of millions in potential profits.'' *See* U.S. Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* (Oct. 2011), *available at* www.dni.gov/reports/20111103_report_fecie.pdf.

Indeed, a survey published in *USA Today* in November found that as many as 17 percent of persons polled admitted that they would disclose their company's secrets for money, while another 8 percent confessed that they had already done so. *See* USA TODAY Snapshots® (Nov. 20, 2011) (citing Monster.com survey), *available at* http://www.scoop.it/t/snapshots.

The growing need for U.S. companies to protect their trade secrets and other confidential, proprietary information is illustrated by the increasing number and significance of trade secret and related litigation over the past year. 2011 saw several high-stakes jury trials resulting in substantial damages awards to victims of

trade secret misappropriation, such as the $920 million award to DuPont in its suit against Kolon Industries over Kevlar-related technologies, and the $310 million award to MGA Entertainment in its long-standing dispute with Mattel over the successful line of Bratz dolls.

The Department of Justice also brought a number of significant criminal prosecutions for trade secret theft and economic espionage in 2011, many involving defendants allegedly acting on behalf of foreign state-owned entities. In addition, 2011 bore witness to several significant judicial decisions impacting trade secret law, including a noteworthy ruling from the U.S. Court of Appeals for the Ninth Circuit regarding the scope of the Computer Fraud and Abuse Act— which is currently being reconsidered by the Ninth Circuit en banc—and a December 2011 decision from the Eighth Circuit, which may serve to expand what constitutes a protectable trade secret under the Uniform Trade Secrets Act.

We highlight these and other significant 2011 developments below, first addressing civil developments and then criminal developments.

CIVIL DEVELOPMENTS

Courts in 2011 addressed a host of complex legal issues impacting trade secret law, ranging from the circumstances under which compilations of publicly-available information may be entitled to trade secret protection, to the meaning of ''authorized access'' under the CFAA. This section describes some of the most notable civil actions involving allegations of trade secret misappropriation over the past year.

Compilations as Trade Secrets

Three courts of appeal issued opinions this year reaffirming the viability of trade secret protection for valuable compilations of information, notwithstanding claims that the components of the compilations were publicly available.

■ ***Design Insights Inc. v. Sentia Group Inc.***, No. 09-2300, 416 Fed. App'x 324 (4th Cir. 2011).

In March, the Fourth Circuit provided guidance on the circumstances under which a compilation containing publicly-available information may warrant trade secret protection.

This unpublished case involved a dispute over a software application belonging to Design Insights Inc. DII brought suit against Sentia Group Inc. and four of Sentia's founders—three of whom were formerly affiliated with DII—alleging, in part, that the defendants had misappropriated DII's trade secrets related to its ''Dynamic Expected Utility'' Model (''EU Model'') software in order to create a competing application.

The district court granted summary judgment for the defendants, finding that DII's EU Model software did not qualify as a trade secret under Virginia law. On appeal, the Fourth Circuit reversed and remanded, with instructions to the district court to consider ''whether or not the software program, as a *total compilation*, could qualify as a trade secret.'' *Id.* at 327 (emphasis added).

On remand, the district court again granted summary judgment for the defendants, this time finding that ''DII failed to satisfy its burden to show that DII's software, as a compilation, was not generally known or readily ascertainable by proper means.'' *Id.* at 328.

The Fourth Circuit disagreed. On appeal for the second time, the appeals court explained that ''a trade secret may be composed of publicly-available information if the method by which that information is compiled is not generally known.'' *Id.* at 329. For this reason, the court explained, ''a trade secret 'might consist of several discrete elements, any one of which could have been discovered by study of material available to the public.' '' *Id.* (citation omitted).

The court then pointed to the testimony and reports submitted by two DII witnesses, who stated that ''elements'' of the DII EU Model software were, in fact, proprietary, and that ''many aspects of the source code, and hence the compilation of the source code as a whole, were not public knowledge or readily ascertainable by proper means.'' *Id.* at 330. Based on this testimony, the court found that DII had adduced sufficient evidence to create a genuine issue of material fact as to whether its software was not generally known or readily ascertainable by proper means and, therefore, DII was entitled to proceed beyond summary judgment.

■ ***Tewari De-Ox Systems Inc. v. Mountain States/Rosen LLC***, 637 F. 2d 604, 98 USPQ2d 1741 (5th Cir. 2011) (82 PTCJ 47, 5/13/11).

The Fifth Circuit in April examined whether combinations of elements can warrant trade secret protection even if *all* elements of that combination have been publicly disclosed. *See id.* at 611.

In *Tewari*, the owner of an oxygen meat-packing method brought suit against a meat wholesaler, alleging, in part, that the wholesaler had misappropriated its trade secrets. The district court found that the publication of information related to the plaintiff's meat-packing method in patent applications had destroyed that information's status as a trade secret, and that none of the plaintiff's other claimed trade secrets warranted protection, as their ''elements were known in the industry.'' *See id.* at 610.

On appeal, the Fifth Circuit affirmed in part and reversed in part. The appeals court agreed with the district court's determination that any information that had been publicly disclosed in patent applications did not qualify for trade secret protection.

Applying Texas law, the court explained that while ''no post-2000 Texas case directly addresses whether a published patent application destroys the secrecy of its contents for trade secret purposes, the weight of authority from other jurisdictions holds that it does.'' *Id.* at 612. With respect to the plaintiff's other claimed trade secrets, however, the court reversed, noting that it had, on prior occasions, ''specifically rejected the contention that a combination of disclosed technologies cannot itself constitute a trade secret.'' *Id.* at 613.

Rather, the court explained, '' 'a trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process, design and operation of which in unique combination, affords a competitive advantage and is a protectable secret.' '' *Id.* at 613 (citation omitted).

■ ***AvidAir Helicopter Supply Inc. v. Rolls-Royce Corp.***, No. 10-3444, 101 USPQ2d 1069 (8th Cir. Dec. 13, 2011) (83 PTCJ 266, 12/23/11).

Finally, a recent Eighth Circuit decision on this topic serves as an important reminder of the distinctions between patent and trade secret law—and may prove useful to would-be plaintiffs seeking trade secret protection for information that has not been kept ''absolutely secret.'' *See id.* at *5.

  PTCJ ISSN 0148-7965

In *AvidAir*, the Eighth Circuit examined whether Rolls-Royce documents relating to the repair of helicopter engines—referred to as Distributor Overhaul Information Letters, or ''DOILs''—qualified for trade secret protection under the UTSA. The court first emphasized that even if the DOILs were comprised almost entirely of publicly-available information, they could nonetheless constitute protectable trade secrets.

As the court explained, ''[c]ompilations of non-secret and secret information can be valuable so long as the combination affords a competitive advantage and is not readily ascertainable.'' *Id.* at *3.

Rejecting the plaintiff's contention that the DOILs lacked value because they contained ''only a trivial amount of information that was not readily ascertainable,'' the court explained that the value of a compilation does not stem from the ''merit of its technical improvements.'' *Id.* at *4. As distinguished from ''patent law, which predicates protection on novelty and nonobviousness, trade secret laws are meant to govern commercial ethics,'' the court pointed out. *Id.* at *5.

In other words, '' 'the effort of compiling useful information is, of itself, entitled to protection even if the information is otherwise generally known.' '' *Id.* at *3 (citation omitted). Thus viewed, the court found the value of the DOILs to be readily apparent, given the significant research and testing that Rolls-Royce had conducted in order to create them. *See id.* at *4.

Moreover, the court noted, the plaintiff's ''repeated attempts to secure the . . . DOILs without Rolls-Royce's approval belie[d] its claim that the information in the documents was readily ascertainable or not independently valuable.'' *Id.* at *5.

With respect to the secrecy of the DOILs, the court found that Rolls-Royce had undertaken sufficient efforts to protect the DOILs from disclosure by labeling them as proprietary. ''Reasonable efforts to maintain secrecy need not be overly extravagant, and absolute secrecy is not required'' to gain trade secret protection, the court explained. *Id.* at *5.

Hence, the mere fact that the plaintiff was able to obtain the DOILs did not negate their status as trade secrets, since the evidence indicated that the plaintiff had ''either acquired the documents from others who were not authorized to provide [the plaintiff] with the documents, or acquired the documents from others who had themselves misappropriated the documents.'' *See id.*

Intersection with the Computer Fraud and Abuse Act

Trade secret misappropriation claims are frequently raised in federal court in conjunction with claims under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

The CFAA establishes federal criminal penalties and provides a federal civil cause of action for various offenses related to unauthorized computer access. For example, the act creates a cause of action against any person who ''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.'' *See* 18 U.S.C. § § 1030(a)(2)(C), (a)(5)(C), and (g).

A protected computer is broadly defined by the act to include all computers ''used in or affecting interstate or foreign commerce or communication,'' *id.* Section 1030(e)(2)(B), which, practically speaking, means any computer connected to the internet.

Because trade secret misappropriation often involves employees' illicit downloading of information from their employers' computers, and because the CFAA serves as a basis for federal court jurisdiction, many trade secret cases also include claims brought under the CFAA.

In order for an employee's conduct to be actionable under the CFAA, however, the employee must not have been authorized to access the computer, or he must have ''exceed[ed] authorized access.'' Courts remain divided over what it means to ''exceed authorized access'' or to access a computer ''without authorization,'' as the following two cases illustrate.[1]

■ ***WEC Carolina Energy Solutions LLC v. Miller***, No. 10-CV-2775, 2011 WL 379458 (D.S.C. Feb. 3, 2011).

A federal district court in South Carolina recently had occasion to examine the meaning of ''without authorization'' under the CFAA.

The case involved a suit by WEC Carolina Energy Solutions LLC against its former employee, Willie Miller, and his assistant, Emily Kelley. WEC alleged that Miller and Kelley had downloaded WEC's confidential documents and e-mailed them to Miller's personal e-mail account, so that Miller could use them for the benefit of his new employer and WEC's competitor, Arc Energy.

In addition to bringing various claims against Miller and Kelley under state law, WEC alleged that Miller and Kelley violated the CFAA when they accessed WEC's computers to send Miller the confidential WEC documents. Miller and Kelley acted ''without authorization'' or ''exceed[ed] authorized access,'' WEC argued, because their actions violated the company's policies prohibiting ''(1) downloading confidential and proprietary information to a personal computer or (2) using any confidential information or trade secrets unless authorized by WEC.'' *Id.* at *3-4.

Rejecting this argument, the court explained that ''[t]he company policies at issue in this case do not restrict an employee's ability to *access* data,'' but only establish limitations on ''how a WEC employee may *use* confidential information after accessing it.'' *Id.* at *3. Hence, the fact that Miller and Kelley may have violated WEC's computer *use* policies was irrelevant in examining whether they had *access* to the computers at issue.

Because Miller and Kelley, as a WEC employees, were, in fact, authorized to access the computers containing WEC's confidential information, they did not act ''without authorization'' under the CFAA.

Moreover, the court explained, Miller and Kelley also did not ''exceed[] authorized access'' within the meaning of the CFAA by violating company policies or acting on behalf of Arc Energy. *See id.* at *4. The CFAA defines ''exceeds authorized access'' as ''to access a computer with authorization and to use such access to obtain or alter information on the computer that the accessor is not entitled so to obtain or alter.'' *See* 18 U.S.C. § 1030(e)(6).

[1] For a fuller discussion of this issue, *see* Jason C. Schwartz and Michael Murray, ''Recent Developments in Trade Secret Law: the Computer Fraud and Abuse Act,'' *Society for Human Resource Management* (June 6, 2011), *available at* http://www.shrm.org/LegalIssues/FederalResources/Pages/TradeSecretLawCFAA.aspx.

Citing this definition, the court found that Miller and Kelley could not have ''exceed[ed] authorized access,'' because that determination ''depends on whether the employee accessed information he was not entitled to access.'' *Id.* Because Miller and Kelley were, in fact, entitled to access the information, they did not ''exceed authorized access'' simply by *using* that information for a purpose that was prohibited by company policy.

Accordingly, the court granted the defendants' motion to dismiss.

■ ***United States v. Nosal***, No. 10-10038, 642 F.3d 781 (9th Cir. 2011), *reh'g en banc granted* (Oct. 27, 2011).

The Ninth Circuit in *Nosal*, a criminal prosecution under the CFAA with implications for civil litigation under the statute as well, took a different view of the meaning of authorized access.

There, the court examined whether David Nosal, a former employee of the executive search firm Korn/Ferry International, violated the CFAA by enlisting several Korn/Ferry employees to assist him in obtaining confidential information from the Korn/Ferry ''Searcher'' database, which Nosal allegedly planned to use to establish his own, competing executive search firm. After he was indicted for violating the CFAA, Nosal filed a motion to dismiss the indictment, arguing that the Korn/Ferry employees did not act ''without authorization'' or ''exceed[] authorized access'' when they accessed the Searcher database on his behalf, since they ''had permission to access the computer and its information under certain circumstances.'' *Id.* at 783.

The district court agreed, citing the Ninth Circuit's decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) for the proposition that an employee's authorization to access a computer does not cease simply because ''an employee resolves to use the computer contrary to the employer's interest.''

Hence, the district court found, the employees did not exceed their authorized access to the Searcher database because they ''had authority to obtain information from the Searcher database for legitimate Korn/Ferry *business purposes*,'' and ''intent is irrelevant in determining whether a person exceeds authorized access.'' *Id.* at 784-85.

On appeal, the Ninth Circuit reversed, holding that ''an employee 'exceeds authorized access' under § 1030 when he or she violates the employer's computer access restrictions—including *use* restrictions.'' *Id.* at 789 (emphasis added). Because all Korn/Ferry employees were subject to a formal computer usage policy, which placed ''clear and conspicuous restrictions'' on access to the Searcher database—and because the employees' use of the database to defraud Korn/Ferry was in clear violation of the company's usage policies—the employees did, in fact, ''exceed'' their authorized access within the meaning of the CFAA. *See id.* at 787.

In reaching this conclusion, the Ninth Circuit rejected the approach adopted by the Seventh Circuit in *International Airport Centers LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). There, the court found that an employee does not have authorization to access a computer within the meaning of the CFAA when he violates a duty of loyalty owed to his employer by acting in a manner that is inconsistent with his employer's interests.

In *Nosal*, however, the court made clear that liability under the CFAA does not depend on whether an employee acts with an improper purpose; rather, it is ''the *employer* that determines whether an employee is authorized to access the computer''—i.e., through the adoption of usage restrictions. *Nosal*, 642 F.3d at 78.

Many have criticized the Ninth Circuit's decision in *Nosal* on the ground that it unduly broadens the scope of potential liability under the CFAA, as even minor violations of employer-instituted computer usage policies can now arguably give rise to federal prosecution under the Act. Since the panel issued its decision in *Nosal* in April, the Ninth Circuit granted Nosal's motion for a rehearing en banc.

Chief Judge Alex Kozinski presided over the en banc hearing in December; no en banc decision has yet been issued.

Noncompetition and Nondisclosure Agreements

Trade secret misappropriation claims often accompany noncompete or nondisclosure agreement claims, and the same interests are often asserted to support enforcement of such agreements.

Although a fuller treatment of the law of noncompete and nondisclosure agreements is beyond the scope of this article, a few significant 2011 cases in this arena are highlighted below.

■ ***IBM Corp. v. Giovanni Visentin***, No. 1:11-CV-00399, 2011 WL 672025 (S.D.N.Y. Feb. 16, 2011); No. 11-902 (2d Cir.).

In February, a federal district court issued a 62-page decision holding that IBM was not entitled to a preliminary injunction to enforce a non-competition agreement with its former executive, Giovanni Visentin.

The decision is noteworthy both because of the skepticism with which the court viewed IBM's broad noncompetition agreement, and because of the court's narrow approach to the doctrine of inevitable disclosure.

Visentin worked for IBM for 26 years as a business manager, eventually serving as the general manager of IBM's Integrated Technology Services business. When Visentin resigned from IBM in January 2011 to accept a new position with Hewlett-Packard, IBM brought suit, alleging breach of contract and trade secret misappropriation, and seeking a preliminary injunction to prevent Visentin from working for HP for 12 months.

While at IBM, Visentin had signed a noncompetition agreement, which provided, in part, that for a year following the termination of his employment, he would not associate with any entity that ''engages in competition with any business unit or divisions of [IBM] in which [he] worked at any time during the three (3) year period prior to the termination of [his] employment.'' *Id.* at 3.

IBM argued that HP was its competitor in the emerging market of ''cloud computing,'' and that Visentin possessed confidential and trade secret information relating to IBM's cloud computing business and associated strategies, as well as information regarding IBM's general business strategies, its potential and ''troubled'' clients, and its acquisition targets. According to IBM, it would be irreparably harmed if Visentin were permitted to accept his new position at HP, given ''the risk that he will inevitably disclose confidential information that he learned at IBM.'' *Id.* at 7.

Rejecting this argument, the district court—after conducting a four-day evidentiary hearing—held that most of the categories of information that IBM sought to protect did not qualify as trade secrets. The court emphasized that Visentin was not employed as a computer ex-

   ISSN 0148-7965

pert at IBM, and that his ''primary job was to be a 'general manager.' '' *Id.* at 8.

''Although trade secrets may have lurked somewhere on the periphery, the real thrust of [Visentin's] position was to manage his teams to make them as efficient as possible,'' the court explained. *Id.* Moreover, with respect to the categories of information that did merit trade secret protection, the court found that IBM had failed to demonstrate any likelihood of inevitable disclosure.

In reaching this finding, the court stressed that Visentin's new position at HP—though involving some of the same responsibilities as his previous position at IBM—was not ''nearly identical'' to his former position, as Visentin would have ''significantly larger'' responsibility at HP, and would be working in areas to which he had ''no prior exposure'' at IBM. *Id.* at 17.

The court also emphasized that Visentin had agreed to ''circumscribe the nature of his responsibilities at HP'' to mitigate any risk of disclosure of confidential information, and that there was no evidence of any prior wrongdoing on Visentin's part. *Id.* at 20.

Given its inability to find that ''Visentin's position at HP would require him to disclose any confidential IBM information he might remember,'' the court held that IBM did not have a ''likelihood of success'' on the merits in its suit to enforce its non-competition agreement, as needed to justify the imposition of a preliminary injunction. *See id.* The court characterized IBM's non-competition agreement—which lacked any geographic limitation, and was not tailored with respect to specific IBM employees—as ''greater than necessary to protect IBM's legitimate interests.'' *Id.* at 23.

In fact, the court explained, the evidence presented during the hearing indicated that the agreement was ''designed not to protect a legitimate business interest, but rather, to keep the leadership talent of IBM from leaving.'' *Id.* at 22. Having found that the noncompetition agreement was overbroad and thus invalid under New York law, the court nonetheless went on to find that it also imposed an undue hardship on Visentin's future employment prospects.

Accordingly, the court denied IBM's motion for a preliminary injunction. The Second Circuit affirmed the district court's decision in a summary order.

■ ***Marsh USA Inc. v. Cook***, No. 09-0558, 2011 WL 6378834 (Tex. Dec. 16, 2011).

This year, the Texas Supreme Court issued a decision that substantially eases the showing necessary for employers to compel enforcement of noncompetition agreements in Texas.

The court in *Marsh* held that under Texas's Covenants Not to Compete Act, an award of stock options to an employee in exchange for the employee's agreement not to compete constitutes adequate consideration to support enforcement of the agreement, as stock options are ''reasonably related'' to the employer's interest in protecting its goodwill.

Marsh involved a Stock Award Plan that Marsh USA Inc. had designed to provide its key employees with the opportunity to become part-owners of the company.

In order to exercise their stock options, employees had to sign an agreement, promising that if they left the company within three years of exercising their options, they would not for the following two years ''solicit or accept business of the type offered by [the company]'' and in which they were involved from the company's clients, former clients, or prospective clients. *Id.* at *1. Employees also had to promise that they would not disclose the company's trade secrets or confidential information. *Id.*

Rex Cook, a managing director at Marsh, signed the agreement in order to exercise his stock options in February 2005, and then, less than three years later, began to work for Marsh's direct competitor, Dallas Series of Lockton Cos. When Marsh brought suit for breach of contract and breach of fiduciary duty, Cook defended on the ground that the non-solicitation/noncompetition agreement ''constituted an unenforceable contract because it was not ancillary to or part of an otherwise enforceable agreement.'' *Id.* at *2.

Under Texas law, a covenant not to compete is enforceable only if there is an ''otherwise enforceable'' agreement between the parties and the covenant is ''ancillary to or part of'' that otherwise enforceable agreement. *Id.* at *6. Prior to *Marsh*, Texas courts had interpreted this to mean that '' 'the consideration given by the employer in the otherwise enforceable agreement must *give rise* to the employer's interest in restraining the employee from competing.' '' *Id.* at *7 (quoting *Light v. Centel Cellular Co. of Texas*, 883 S.W.2d 643, 647 (Tex. 1994) (emphasis added)).

In *Marsh*, however, the Texas Supreme Court explained that consideration for a non-competition agreement need only be ''*reasonably related* to an interest worthy of protection, such as trade secrets, confidential information or goodwill''; there is no requirement, said the court, that the consideration actually ''give[] rise to the interest in restraining the employee from competing.'' *Id.* at *9. The court therefore found that the award of stock options to Cook was sufficient to support enforcement of the noncompetition agreement.

As the court explained, ''By awarding Cook stock options, Marsh linked the interests of a key employee with the company's long-term business interests''—including its interest in protecting goodwill by preventing former employees from usurping the company's relationships with its customers. *Id.* at *11.

Because the stock options were thus ''reasonably related'' to the protection of ''business goodwill''—a protectable interest under the act—the court found that the covenant not to compete was not void for lack of adequate consideration. *See id.*

■ ***News America Marketing v. Emmel***, No. 09-11858, 429 Fed. App'x 851 (11th Cir. 2011).

An unpublished decision issued by the 11th Circuit in June illustrates the need for carefully-worded nondisclosure language to protect confidential company information, especially in the context of separation or post-separation agreements.

In *News America*, the 11th Circuit addressed whether an ex-News America employee had breached his post-employment nondisclosure agreement by providing confidential company documents to a Senate staffer.

While employed at News America, Robert Emmel had allegedly become convinced that the company ''was engaged in widespread illegal activity against its customers, competitors, and shareholders.'' *Id.* at 853. Emmel reached out to several Senate staffers and other government officials to discuss his concerns about the company, during which time he disclosed a variety of News America's confidential documents and information.

News America eventually terminated Emmel in November 2006, though it was unaware of Emmel's disclosures of confidential company information at the time. The following month, Emmel asked News America to confirm to a new, potential employer that he was not subject to any noncompetition agreement.

News America agreed to do so in return for Emmel's signing a nondisclosure agreement. Hence, on Dec. 21, 2006, Emmel signed the agreement, in which he promised that he ''*will* not disparage, denigrate, or defame the Company . . . and that he *will* maintain in complete confidence . . . any 'Confidential Information' of the Company.'' *Id.* at 854 (emphasis added). The day *before* signing this agreement, however, Emmel mailed a final 55 pages of confidential News America documents to a staffer for the U.S. Senate Finance Committee.

Holding that the Dec. 20 mailing was not prohibited by the Dec. 21 nondisclosure agreement, the court explained that Emmel's ''act of disclosure or disparagement occurred when he mailed the package of materials.'' *Id.* at 856. Because Emmel mailed the package of materials prior to signing the nondisclosure agreement, the mailing did not constitute a breach of the agreement—at least in the absence of language indicating that the agreement was intended to apply retroactively.

The court, however—citing the agreement's use of the present tense rather than the present perfect tense—found no such indication. *See id.* at 855. The court went on to reject the contention that Emmel's failure to attempt to retrieve the package after it had been mailed somehow constituted a breach of the nondisclosure agreement, explaining that ''the language of the agreement does not cover acts of omission or inaction, only acts of commission.'' *Id.* at 856.

''If it had wanted the agreement to cover past acts or future inaction,'' the court explained, ''News America should have written the agreement to say that.'' *Id.*

Remedies

No survey of 2011 trade secret litigation developments would be complete without mention of the year's blockbuster verdicts. Indeed, two of the three largest jury verdicts of the year—a $920 million verdict in *E.I. Du Pont de Nemours and Co. v. Kolon Industries Inc.* and a $2.3 billion verdict in *Pacesetter Inc. v. Nervicon Co.*—arose in trade secret cases, according to data compiled by VerdictSearch. *See* VerdictSearch, *Largest Jury Verdicts of the Year*, *available at* http://www.verdictsearch.com/index.jsp?do=us.

■ ***E.I. DuPont de Nemours and Co. v. Kolon Industries Inc.***, No. 09-CV-00058 (E.D. Va.); 637 F3d 435, 98 USPQ2d 1020 (4th Cir.) (81 PTCJ 682, 3/25/11).

A federal jury in September awarded E.I. DuPont de Nemours and Co. $920 million in damages in its suit against Kolon Industries Inc., over trade secrets regarding the manufacture of Kevlar—a para-aramid fiber used to make protective body gear.

DuPont brought suit against the South Korea-based Kolon in February 2009, alleging that Kolon had misappropriated its Kevlar-related trade secrets and other confidential, proprietary information through Michael Mitchell, an ex-DuPont employee whom Kolon had hired as a consultant. According to DuPont, Kolon actively sought to employ former DuPont employees like Mitchell with experience in the sale and marketing of Kevlar when it began to experience difficulties in developing and marketing its own para-aramid fiber product to compete with Kevlar.

In March 2010, Mitchell was sentenced to 18 months in prison after he pled guilty to trade secret theft and obstruction of justice. Kolon, however, continued to maintain that it did not steal any confidential information or trade secrets from DuPont, and the case against it proceeded to trial.

Although it lost at trial on DuPont's trade secret misappropriation claim, Kolon has announced its intention to continue to pursue its antitrust counterclaim against DuPont. Kolon responded to DuPont's allegations of trade secret misappropriation by arguing that DuPont violated Section 2 of the Sherman Act through its monopolization and attempted monopolization of the market for para-aramid fiber. Specifically, Kolon maintains that DuPont committed antitrust violations by entering into multi-year supply agreements with its high-volume customers, which required the customers to purchase 100 percent of their para-aramid materials from DuPont.

The district court initially granted DuPont's motion to dismiss Kolon's counterclaim in December 2009, but the Fourth Circuit reversed in March 2011, finding that Kolon had sufficiently pled a distinct, relevant geographic market, DuPont's possession of monopoly power, and the willful maintenance of that power through anticompetitive conduct.

■ ***Bryant v. Mattel Inc.***, No. 04-CV-09049 (C.D. Cal.).

2011 saw several significant developments in the seven-year feud between MGA Entertainment Inc. and Mattel Inc. over MGA's line of Bratz toy dolls.

The litigation between MGA and Mattel began in 2004, when Mattel sued its former toy designer Carter Bryant, alleging that Bryant violated his duties to Mattel by failing to disclose his concept for the Bratz dolls before leaving Mattel to join MGA. MGA intervened in the suit and filed its own complaint against Mattel for unfair competition, trade dress infringement, dilution, and unjust enrichment.

Mattel responded with claims against MGA for intentional interference with contract, copyright infringement, unfair competition, and aiding and abetting breach of fiduciary duty. In 2008, a jury found for Mattel on all counts, awarding Mattel $100 million in damages, in light of its conclusion that MGA's Bratz dolls were based on the concept sketches that Bryant had made while he was still employed by Mattel.

The district court placed the Bratz trademarks in a constructive trust and enjoined MGA from continuing to sell the dolls. The Ninth Circuit, however, vacated the verdict for Mattel, based on errors in the jury instructions.

A new trial began in January 2011, in which MGA asserted additional claims against Mattel for trade secret misappropriation, based on Mattel's use of a ''market intelligence group,'' which it allegedly dispatched to various toy fairs and showrooms, in an attempt to learn about its competitors' upcoming products and designs. In April 2011, the jury reached its verdict in the second trial, this time finding that *Mattel* had stolen MGA's trade secrets through its market research tactics, and awarding MGA $3.4 million for each of the violations, for a total award of approximately $88.5 million.

The judge subsequently reduced the damages award to $85 million because of a duplication error by the jury, but then added an additional $85 million in exemplary

   ISSN 0148-7965

damages, and granted MGA's request for attorneys' fees and costs, bringing the total award to almost $310 million.

While the trial was still underway, MGA filed another complaint against Mattel, alleging that Mattel had violated Section 2 of the Sherman Act by monopolizing or attempting to monopolize the sale and distribution of ''fashion dolls'' in the United States, primarily through its use of an allegedly illegal litigation strategy against its competitors. However, in October 2011, the district court granted Mattel's motion to dismiss the antitrust complaint, on the ground that MGA's claims arose out of the same nucleus of operative facts as the earlier lawsuit, and hence, were barred by the doctrine of res judicata.

■ ***Trust Company of the West v. Gundlach***, No. BC429385 (Cal. Sup. Ct. 2011).

One of the most dramatic trade secret cases of the year recently came to a close, as TCW Group Inc., a unit of Societe Generale SA, reached a settlement in December 2011 with its former chief investment officer and star bond manager, Jeffrey Gundlach.

Shortly after he was fired from TCW in December 2009, Gundlach founded his own asset management firm, DoubleLine Capital LP. In January 2010, TCW brought suit against Gundlach, DoubleLine, and several other ex-TCW employees who had left to join DoubleLine, alleging breach of fiduciary duty, trade secret misappropriation, and intentional interference with contract. According to TCW, Gundlach had begun stealing the company's proprietary information in the final months of his employment with the express purpose of establishing his own, competing asset management firm.

Gundlach counterclaimed, arguing that TCW had breached his oral employment contract by firing him in order to avoid having to pay him the substantial performance fees to which he was entitled for his successful management of TCW funds. After a seven-week trial in which Gundlach and TCW presented diametrically-opposed views of the circumstances surrounding Gundlach's termination, a jury found that Gundlach had breached his fiduciary duty to TCW, but that he owed TCW no damages for the breach.

The jury additionally found that Gundlach was owed $66.7 million in damages for unpaid wages, and that Gundlach had misappropriated TCW's trade secrets.

The judge had not yet decided the ''reasonable royalties'' to which TCW was entitled as a result of the trade secret misappropriation when the parties reached their settlement. TCW, however, had offered expert testimony suggesting that it was entitled to more than $80 million in damages.

The terms of the parties' settlement agreement are confidential.

■ ***Pacesetter Inc. v. Nervicon Co.***, No. BC424443 (Cal. Sup. Ct. 2011).

A California jury in April awarded Pacesetter Inc. (commonly known as ''St. Jude Medical'') a $2.3 billion verdict in a case against its former employee, Yongning Zou, and his new company, Nervicon Co.

St. Jude, a California-based manufacturer of pacemakers and defibrillators, argued that Zou stole the company's trade secrets and other confidential, technical information in order to start Nervicon—a competing medical device business in China. Zou formed Nervicon only weeks before resigning from St. Jude, and owned 47.5 percent of the company.

Zou refused to appear or present a defense at trial, but his past appearances in the case enabled St. Jude to proceed against him. At trial, the jury found against the absent defendant, concluding that Zou had, in fact, misappropriated St. Jude's trade secrets and breached his confidentiality agreement with the company, and that St. Jude was entitled to $947 million in damages from Zou and Nervicon for past harm.

The jury also recommended an award of $868 million against Nervicon for future economic losses and an award of $500 million against Nervicon in punitive damages, bringing the total award to approximately $2.3 billion. The judge, however, declined to adopt the jury's recommended award against Nervicon, since Nervicon did not enter an appearance in the matter, and St. Jude did not claim a specific amount of damages against Nervicon in its first amended complaint.

Nevertheless, the judge entered a default judgment against Nervicon on the trade secret misappropriation and unfair competition claims against it, and issued a permanent injunction restraining the company from future uses of St. Jude's trade secrets and proprietary information.

The jury's damages award against Zou remains intact.

CRIMINAL DEVELOPMENTS

In its October 2011 report to Congress, the U.S. Office of the National Counterintelligence Executive predicted that ''foreign attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to U.S. economic security.'' U.S. Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* (Oct. 2011), *available at* www.dni.gov/reports/20111103_report_fecie.pdf.

This trend was reflected in part in the rising number of prosecutions under the Economic Espionage Act of 1996, which makes the theft of trade secrets a federal crime. *See* 18 U.S.C. §§ 1831; 1832.

Over the past year, there have been several high-profile prosecutions and convictions under the Act—including two cases involving the theft of high-frequency trading programs from major financial institutions, *see United States v. Agrawal*, No. 1:10-CR-417 (S.D.N.Y.); *United States v. Aleynikov*, No. 1:10-CR-00096 (S.D.N.Y.); No. 11-1126 (2nd Cir.), and multiple cases in which Chinese nationals were found to have stolen trade secrets for the benefit of Chinese corporations and government entities, *see, e.g.*, *United States v. Yu*, No. 2:09-CR-20304 (E.D. Mich.); *United States v. Huang*, No. 10-CR-00102; No. 11-CR-00163 (S.D. Ind.).

In response to these and other cases involving foreign economic espionage, the U.S. Senate Judiciary Committee recently approved legislation that would amend the Economic Espionage Act to increase the maximum term of imprisonment for those found guilty of economic espionage from 15 to 20 years. *See* 112th Cong., 1st Sess., S. 678 (''Economic Espionage Penalty Enhancement Act of 2011'') (83 PTCJ 214, 12/16/11). According to Sen. Herbert H. Kohl (D-Wis.), the sponsor of the legislation, this increase in criminal penalties available under the act would help protect American

''businesses and make sure their ideas and processes worth billions of dollars remain intact.'' *See* Press Release, Sen. Herb Kohl, *Kohl's Bipartisan Economic Espionage Bill to Protect U.S. Businesses Passes Committee* (Dec. 8, 2011), *available at* http://kohl.senate.gov/mobile/pressrelease.cfm?customel_dataPageID_1464=4859.

Although Kohl's proposed legislation has yet to be enacted, the U.S. government has continued to seek severe criminal penalties for foreign economic espionage and trade secret theft in accordance with existing law, as demonstrated by the following notable prosecutions from 2011.

■ ***United States v. Liu***, No. 3:05-CR-00085 (M.D. La.).

On Feb. 7, a former Dow Chemical Co. research scientist was convicted of conspiracy to commit trade secrets theft and perjury (81 PTCJ 497, 2/18/11).

The defendant, Wen Chyu Liu, also known as David W. Liou, worked at Dow's Plaquemine, La., facility, where he had access to trade secrets and confidential information regarding Dow's process for manufacturing Tyrin chlorinated polyethylene (CPE)—a kind of rubber used in the production of automotive and industrial hoses, as well as wire and cable jacketing.

Liu allegedly bribed other Dow employees for information regarding CPE in an effort to sell CPE design packages to various Chinese companies. In addition to finding Liu guilty of conspiracy to commit trade secret theft, the jury found Liu guilty of perjury based on false statements that Liu made during a deposition in a related civil suit filed against him by Dow.

Liu currently faces a maximum of ten years in prison on the trade secret theft charge and five years in prison on the perjury charge, as well as a maximum $250,000 fine for each count.

■ ***United States v. Lin***, No. 6:07-CR-06083 (W.D.N.Y.). On Feb. 11, Yeong C. Lin was sentenced to a term of 30 months imprisonment and ordered to pay a $1,000 fine after pleading guilty to one count of conspiracy to commit trade secrets theft.

From 1999 to 2002, Lin worked as a consultant for Picvue Optoelectronics, a Taiwanese company that sought to compete with Corning Inc. in the manufacture of Thin Film Transistor (TFT) Liquid Crystal Display (LCD).

During his employment with Picvue, Lin conspired to steal Corning's trade secrets and confidential information related to the production of TFT LCD. Specifically, in 2000, Lin purchased technical drawings regarding Corning's TFT LCD manufacturing process from Jonathan Sanders, a Corning employee whom Lin had met when Sanders interviewed for a position at Picvue.

When Corning learned of Lin's conduct, it brought a civil suit against Picvue, alleging trade secret misappropriation and copyright infringement. The parties resolved the civil suit through a settlement agreement in 2005.

Sanders was sentenced in 2006 to four years in prison and fined $200,000 as a result of his involvement in the scheme.

■ ***United States v. Jhaveri***, No. 5:10-MJ-00065 (N.D.N.Y.).

On Feb. 17, Shalin Jhaveri was sentenced to time served and three years of supervised release and ordered to pay a $5,000 fine for stealing trade secrets from his former employer, Bristol-Myers Squibb Co.

In November 2010, Jhaveri admitted that he had downloaded confidential files from Bristol-Myers' server during his employment as a technical operations associate in the company's management training program. Jhaveri apparently intended to use the information to establish a competing pharmaceutical company in his native India, but was arrested by the FBI during a meeting with a potential investor in his new company.

■ ***United States v. Agrawal***, No. 1:10-CR-417 (S.D.N.Y.).

On Feb. 28, a former trader at Société Générale SA, was sentenced to three years in prison for stealing Société Générale's computer code for a high-frequency trading program. According to the prosecution, the defendant, Samarth Agrawal, stole the code in an attempt to procure a new, lucrative position at Société Générale's competitor, Tower Capital Management.

Agrawal was in the midst of employment negotiations with Tower at the time of the alleged conduct, and told Tower employees that he could develop a high-frequency trading program for the company if he were to be hired. The code stolen by Agrawal reportedly cost Société Générale almost $10 million to develop and generated tens of millions of dollars in annual profits.

In November 2010, a jury convicted Agrawal of trade secret theft and transportation of stolen property in interstate and foreign commerce. Agrawal was28 years old at the time of his conviction, and only 26 years old when the alleged illegal activities occurred. On March 10, Agrawal filed a notice of appeal of his conviction and sentence, which remains pending before the Second Circuit.

■ ***United States v. Aleynikov***, No. 1:10-CR-00096 (S.D.N.Y.); No. 11-1126 (2nd Cir.).

On March 18, Sergey Aleynikov, a former computer programmer for Goldman Sachs Group Inc., was sentenced to eight years in prison and fined $12,500 for stealing Goldman's high-frequency trading code, which he allegedly intended to use to develop a competing code for his new employer, Teza Technologies.

According to the prosecution, Aleynikov uploaded the code to a server in Germany on his last day of work at Goldman, erased records of the upload, encrypted the code, and then downloaded the code onto his home computer later that night (79 PTCJ 455, 2/19/10).

For purposes of sentencing, the government estimated that Goldman's loss from the theft was between $7-$20 million, based on the many years that it had taken Goldman programmers to develop the code, and the $300 million in annual income that Goldman generated from its high-frequency trading groups. On March 23, Aleynikov filed a notice of appeal of his conviction and sentence.

The Second Circuit has yet to rule on the merits of the appeal, but denied Aleynikov's motion for bail on May 3.

■ ***United States v. Yu***, No. 2:09-CR-20304 (E.D. Mich.).

On April 12, former Ford Motor Co. engineer Xiang Dong Yu was sentenced to 70 months in prison and ordered to pay a $12,500 fine after he pled guilty to two counts of trade secret theft for stealing an estimated $50-$100 million worth of trade secrets from Ford.

Yu, a Chinese national, copied 4,000 pages of confidential and proprietary Ford documents onto an external hard drive in December 2006, shortly before leaving the company. Yu took the external hard drive with him to China, where he eventually began working for Ford

  PTCJ ISSN 0148-7965

competitor Beijing Automotive Co. (BAC). When Yu returned to the United States in 2009, the FBI discovered that Yu's BAC laptop contained thousands of proprietary documents that Yu had taken from Ford.

■ ***United States v. Doxer***, No. 11-CR-10268 (D. Mass.).

On Aug. 30, Elliot Doxer pled guilty to one count of foreign economic espionage for providing trade secrets to an undercover FBI agent posing as an Israeli intelligence officer.

Doxer, an employee in the finance department of Akamai Technologies Inc., had contacted the Israeli consulate in Boston, offering to provide any information in his company's possession that could assist Israel in its ''war against our enemies.'' An FBI agent pretending to be a representative of the Israeli government subsequently contacted Doxer and arranged for the creation of a secret ''dead drop'' to facilitate the transfer of information.

Doxer visited the ''dead drop'' on 62 occasions over an 18-month period, during which time he disclosed a wide array of his employer's trade secrets and confidential information, including information regarding Akamai's customer lists, security systems, and pricing. In December 2011, Doxer was sentenced to six months in prison and six months of home confinement, and ordered to pay a $25,000 fine.

■ ***United States v. Yang***, No. 11-CR-458 (N.D. Ill.). On Sept. 28, Chunlai Yang, a former software engineer at CME Group Inc., was indicted for two counts of trade secret theft.

According to the indictment, Yang downloaded CME trade secrets and confidential source code relating to CME's ''Globex'' trading platform to several USB flash drives, and then transferred the data to his personal computer. Yang allegedly intended to use the data to develop a trading platform for the Zhangjiagang China chemical electronic trading exchange.

■ ***United States v. Jin***, No. 08-CR-00192 (N.D. Ill).

On Nov. 15, closing arguments were held in the bench trial of Hanjuan Jin, an ex-Motorola Inc. software engineer accused of economic espionage and trade secret theft.

According to the indictment, Jin—a Chinese-born U.S. citizen—was detained at Chicago's O'Hare International Airport in February 2007, carrying a one-way ticket to China, more than $30,000 in cash, and 1,000 of Motorola's documents containing confidential and proprietary information regarding the company's telephone communications technologies.

The government maintains that Jin downloaded Motorola's documents only days after accepting an offer of employment from Kai Sun News (Beijing) Technology Co. (also known as SunKaisens), and that she intended to share Motorola's trade secrets and confidential information with Kai Sun, and/or Kai Sun's customer, the Chinese military.

Jin is also one of several ex-Motorola employees named as a defendant in a related civil suit by Motorola against Lemko Corp., alleging trade secret misappropriation and violations of the CFAA.

In its civil complaint, Motorola maintains that Jin secretly accepted a position with Lemko in June 2004, despite the fact that she continued to work for Motorola through February 2007. During this period of ''dual employment,'' Jin allegedly accessed Motorola's computers without authorization or in excess of her authorization in order to download and transfer Motorola trade secrets and proprietary information to Lemko.

■ ***United States v. Huang***, No. 10-CR-00102; No. 11-CR-00163 (S.D. Ind.).

On Dec. 21, Kexue Huang, a former research scientist for Dow Agrosciences LLC and Cargill Inc., was sentenced to seven years and three months in prison and three years of supervised release after pleading guilty to economic espionage and trade secret theft earlier this year.

Huang, a Chinese national, worked for Dow from January 2003 through February 2008, where he led a team of research scientists in developing unique strains of organic insecticides. Despite having signed a confidentiality agreement with Dow, Huang shared his employer's trade secrets with individuals in China and Germany.

Huang then used the trade secrets to direct and conduct research at Hunan Normal University—a foreign instrumentality of the People's Republic of China. Huang apparently planned to use this research to develop his own line of organic insecticides in China, which would directly compete with Dow's products.

Shortly after leaving Dow, Huang joined Cargill Inc. as a biotechnologist, where he was privy to a secret company project to develop a new food product. Huang again signed a confidentiality agreement with his employer, which he again violated by sharing Cargill trade secrets regarding the company's new food product with a student at Hunan Normal University.

According to Huang's plea agreement, the estimated aggregate losses caused by his criminal conduct are between $7 million and $20 million.

CONCLUSION

2011 was another significant year for civil and criminal trade secret litigation.

In light of the growing threat posed by trade secret theft, corporate executives and law departments would be well advised to follow the recommendation of the U.S. Office of the National Counterintelligence Executive, by ensuring that ''the protection of trade secrets and computer networks is an integral part of all corporate decisions and processes and that all managers—not just security and information systems officials—have a stake in the outcome.'' U.S. Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* (Oct. 2011), *available at* www.dni.gov/reports/20111103_report_fecie.pdf.

Companies should consider taking proactive steps to reduce the risk of trade secret theft and to strengthen their position in litigation should it occur, by enhancing security measures, audits and exit procedures. Given the high stakes in trade secret litigation, companies should also consider appropriate steps in the interview and new hire process to reduce the risk of unjustified claims from competitors of trade secret misappropriation associated with the hiring of key employees.