Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

TRADE SECRETS

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

2014 Trade Secrets Litigation Round-Up





By Jason C. Schwartz,
Alexander H. Southwell,
Martin A. Hewett,
Andrea R. Lucas and
Christopher Smith

Last year's *Trade Secrets Litigation Round-Up* reported on notable federal measures to strengthen protections against trade secrets theft, including important amendments to the Economic Espionage Act (EEA) in January 2013 and the Obama administration's release of a detailed white paper laying out its strategy for combating trade secret theft.[1] Despite this increased focus at the federal level, cyber-attacks against U.S. trade secrets continued to rise in 2014.[2] Indeed, during a May 2014 Senate Judiciary Committee hearing on trade secret theft, Sen. Sheldon Whitehouse (D-R.I.) highlighted an estimate that 1 to 3 percent of national GDP is lost annually through trade secret theft.[3]

2014 saw a variety of activity at both the federal and state levels in the trade secret arena. On the legislative front, both the House of Representatives and the Senate introduced bipartisan amendments to the EEA that would create a federal civil cause of action for the mis-

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 is Co-Chair of Gibson Dunn's Information Technology and Data Privacy Practice Group, and a partner in the firm's New York office.

Martin A. Hewett, Andrea R. Lucas and Christopher Smith are litigation associates in the firm's Washington, D.C. office.

[1] *See* Jason C. Schwartz, Alexander H. Southwell, Molly T. Senger and David A. Schnitzer, "2013 Trade Secrets Litigation Round-Up," 87 Bloomberg BNA's Patent, Trademark & Copyright Journal 717, (87 PTCJ 717, 1/31/14) (2013 TS Round-Up). The authors thank Angelique Kaounis, a litigation of counsel in Gibson Dunn's Century City office with a focus on intellectual property and technology-related issues, for her valuable contributions to this year's *Round-Up*.

[2] *Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 113th Cong. 1 (2014) (statement of Sen. Sheldon Whitehouse, Chairman, Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary).

[3] *Id.*

 ISSN 0148-7965

appropriation of trade secrets related to products used in interstate commerce, while Massachusetts debated legislation that would make it the 48th state to adopt the Uniform Trade Secrets Act (UTSA).

In the criminal arena, the Department of Justice secured the first-ever indictment against foreign government actors for trade secret theft and economic espionage, charging five officers of the Chinese military with engaging in a sophisticated cyber-hacking scheme to steal U.S. company trade secrets for the benefit of Chinese competitors. The Department of Justice also achieved the first federal jury conviction for economic espionage charges against individuals who misappropriated a U.S. company's trade secrets and sold them to an entity controlled by the Chinese government.

On the civil front, state and federal courts addressed a variety of substantive and procedural issues with respect to trade secret and related claims, including the preemptive effect of the UTSA, the types of information that merit protection as trade secrets, the standards applicable to alleging and proving misappropriation of trade secrets, the types of ''reasonable measures'' that companies should take to protect their trade secrets and the nature and scope of the remedies available for trade secret theft. There were also significant developments in several ongoing and high-profile trade secret litigation matters, including the Fourth Circuit's vacatur of a nearly $1 billion jury verdict in favor of DuPont based on an evidentiary error by the district court.

We address these and other 2014 developments in trade secrets law below. We first address developments in the statutory landscape, followed by criminal developments and then civil developments.

STATUTORY DEVELOPMENTS

Trade secret law is based primarily on state law, though the EEA provides a basis for federal criminal prosecutions for trade secret theft and the federal Computer Fraud and Abuse Act (CFAA), discussed further below, provides for civil and criminal causes of action that may apply to the theft of trade secrets through unauthorized access of a computer. In 2014, there were several notable legislative proposals concerning both the EEA and state laws related to the protection of trade secrets.

Federal Economic Espionage Act Developments

Bipartisan amendments to the EEA that would create a federal civil cause of action for trade secret theft were introduced in both the House of Representatives and the Senate this year. According to their sponsors, both amendments are designed to provide greater uniformity to the ''patchwork [of] state and federal statutes''[4] regarding the protection of trade secrets by ''creat[ing] a uniform standard for trade secret misappropriation.''[5]

The Senate bill—introduced in April by Sens. Orrin Hatch (R-Utah) and Chris Coons (D-Del.) and known as the Defend Trade Secrets Act (DTSA)[6]—would create a civil cause of action for violations of the EEA's trade secret theft and/or economic espionage provisions, as well as the misappropriation of a trade secret ''related to a product or service used in, or intended for use in, interstate or foreign commerce.''[7] The companion bill in the House—introduced in July by Rep. George Holding (R-N.C.) and a bipartisan group of cosponsors and known as the Trade Secrets Protection Act (TSPA)[8]—is narrower than the DTSA, as its civil cause of action would not extend to violations of the EEA that do not otherwise qualify as misappropriation of a trade secret that is related to a product used in interstate or foreign commerce. While the DTSA and TSPA both adopt a definition of misappropriation modeled after the UTSA, neither amendment would preempt state law or grant federal courts exclusive jurisdiction.[9]

In addition to creating a federal civil cause of action, both amendments would strengthen the remedies available to prevent, remedy and deter trade secret theft. Most notably, both the Senate and House legislation would authorize courts to issue *ex parte* seizure orders to preserve evidence or prevent the use or disclosure of the trade secret at issue.[10] In addition, both amendments would authorize an award of treble damages for willful and malicious misappropriation, as compared to the double damages authorized by most state versions of the UTSA.[11] Finally, both the DTSA and the TSPA provide for a five-year statute of limitations, as compared to the three-year statute of limitations under the UTSA.[12]

The TSPA was approved by the House Judiciary Committee in September and is currently awaiting a vote by the full House of Representatives,[13] while the DTSA was reviewed by the Senate Judiciary Committee.[14] Though neither bill was voted on by the full House or Senate prior to the close of the last session of the 113th Congress, Senator Hatch recently emphasized that it is ''past time'' for Congress to create a federal cause of action for trade secrets misappropriation[15] and Senator Coons has stated that he is optimistic that legislation will pass quickly after it is reintroduced in the new Congress.[16] Although similar pieces of legisla-

[4] Press Release, Office of Rep. George Holding, *Congressman Holding Introduces Bipartisan Trade Secrets Protection Act of 2014*, (Jul. 29, 2014), available at http://holding.house.gov/media-center/press-releases/congressman-holding-introduces-bipartisan-trade-secrets-protection-act.

[5] Press Release, Office of Sen. Christopher Coons, *Senators Coons, Hatch introduce bill to combat theft of trade secrets and protect jobs*, (Apr. 29, 2014), available at http://www.coons.senate.gov/newsroom/releases/release/senators-coons-hatch-introduce-bill-to-combat-theft-of-trade-secrets-and-protect-jobs.

[6] Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014).

[7] *Id.* at § 2(a).

[8] Trade Secrets Protection Act of 2014, H.R. 5233, 113th Cong. (2014).

[9] *See id.*

[10] *See id.*

[11] *See id.*

[12] *See id.*

[13] Tamlin Bason, *Many Hope Trade Secrets Legislation Moves in Lame-Duck Session; Critics, Skeptical of Bills' Effectiveness, Ask: ''Why Here, Why Now?''* 89 Bloomberg BNA's Patent, Trademark & Copyright Journal 115, (89 PTCJ 115, 11/13/14).

[14] Edward H. Pappas, Daniel D. Quick and Max A. Aidenbaum, ''The Defend Trade Secrets Act-Trade Secret Protection Act—Finally, Federal Protection for Trade Secrets?,'' *Bloomberg Law* (Nov. 3, 2014), *available at* http://www.bna.com/defend-trade-secrets-n17179910868/.

[15] *Id.*

[16] Tal Kopan, ''Today: USPS in the crosshairs - Meet the new House Intel chairman - Fatal blow for surveillance reform, info sharing?'' *Politico* (Nov. 19, 2014), available at http://

   ISSN 0148-7965

tion have been introduced in prior years,[17] the DTSA and the TSPA warrant close monitoring in 2015 given the bipartisan support that both have thus far enjoyed.

State Law Developments

In April of this year, Gov. Deval Patrick introduced legislation that would make Massachusetts the 48th state to adopt the Uniform Trade Secrets Act. After that legislation—which included significant new restrictions on non-competition agreements—failed to pass, Governor Patrick reintroduced the package in August.[18] However, no vote on the bill occurred prior to the close of the most recent legislative session. If the legislation is enacted, New York and North Carolina would become the only remaining states that have not yet adopted some form of the UTSA.

CRIMINAL DEVELOPMENTS

Last year's *Trade Secrets Litigation Round-Up* reported on the Obama administration's announcement of several additional steps it planned to take to bolster its protection of U.S. intellectual property.[19] The administration continued to implement those steps in 2014, including the creation of a new Deputy Assistant Attorney General position in the National Security Division of the Department of Justice ''to oversee [the National Security Division's] efforts to protect national assets'' and ''combat economic espionage, proliferation, and cyber-based national security threats.''[20] In the Department's announcement, Assistant Attorney General John P. Carlin cited the new position as an important component of the Department of Justice's efforts to ''sharpen [its] focus and increase [its] attention on the emerging threats of economic espionage and proliferation.''[21]

The Obama administration also continued to pursue criminal prosecutions to address and deter trade secret theft and economic espionage during 2014. During the first nine months of fiscal year 2014, the Department of Justice reported 20 new prosecutions under the EEA (a 33 percent increase from fiscal year 2013) and seven convictions (a 17 percent increase from fiscal year 2013).[22] Similarly, in May 2014, the FBI reported a 60 percent increase in trade secret investigations from fiscal year 2009 through fiscal year 2013.[23]

Trade Secret Theft and Cyber-Espionage Prosecutions Involving Chinese Actors

In last year's *Round Up*, we reported on the Department of Justice's high-profile indictments of several Chinese nationals alleged to have stolen U.S. trade secrets for the benefit of Chinese competitors. The Department continued to pursue prosecutions of such individuals in 2014—including a landmark indictment of five Chinese military officers for allegedly hacking into major U.S. companies' computer systems to steal trade secrets—and secured the first federal convictions through a jury trial for violations of the EEA against two individuals charged with stealing U.S. trade secrets to sell them to entities controlled by the Chinese government.

United States v. Dong (W.D. Pa.)[24]

In May 2014, a Pennsylvania federal district court unsealed a 48-page indictment charging five officers of the Chinese military with conspiracy and substantive violations of the Computer Fraud and Abuse Act, trade secret theft, economic espionage and aggravated identity theft. The indictment alleges that the officers hacked into the computer systems of several U.S. companies in the nuclear power, metals and solar product industries and stole trade secrets and other sensitive information—including technical and design specifications, manufacturing metrics and information regarding strategies for pending trade disputes—for the purpose of providing that information to Chinese competitors, including state-owned enterprises. In the Department of Justice's press release announcing the indictment, Attorney General Holder noted that these were the ''first ever charges against a state actor for this type of hacking,'' and warned that the Obama administration ''will not tolerate actions by any nation that seeks to illegally sabotage American companies.''[25]

United States v. Liew (N.D. Cal.) [26]

In March 2014, the Department of Justice secured the first federal convictions through a jury trial for violations of the Economic Espionage Act against two individuals and a corporation charged with the theft of trade secrets related to DuPont's titanium dioxide products, which are used to produce specialized coatings and plastics.[27] Following a two-month jury trial in a California federal district court, the defendants were

---

www.politico.com/morningcybersecurity/1114/morningcybersecurity16162.html.

[17] *See* Bason, *supra* note 13 (discussing previous measures introduced by Sen. Herbert H. Kohl (D-Wis.), Rep. Zoe Lofgren (D-Calif.), and Sen. Jeffry L. Flake (R-Ariz.)).

[18] H. 4401, 188th Leg. (Mass. 2014).

[19] *See* 2013 TS Round-Up, *supra* note 1.

[20] Press Release, U.S. Dep't of Justice, *National Security Division Announces New Senior Leadership Hires and Restructuring of Counterespionage Efforts* (Oct. 21, 2014), *available at* http://www.justice.gov/opa/pr/national-security-division-announces-new-senior-leadership-hires-and-restructuring.

[21] *Id.*

[22] *See Prosecutions for 2014: Lead Charge: 18 U.S.C. 1831—Economic Espionage*, Transactional Records Clearinghouse (Oct. 2014), *Prosecutions for 2014: Lead Charge: 18 U.S.C. 1832—Theft of trade secrets*, Transactional Records Clearinghouse (Oct. 2014), *Convictions for 2014: Lead Charge: 18 U.S.C. 1831—Economic Espionage*, Transactional Records Clearinghouse (Oct. 2014), *Convictions for 2014: Lead Charge: 18 U.S.C. 1832—Theft of trade secrets*, Transactional Records Clearinghouse (Oct. 2014).

[23] *Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 113th Cong. 2 (2014) (statement of Randall C. Coleman, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation).

[24] No. 14 Cr. 00118 (W.D. Pa. May 1, 2014).

[25] Press Release, U.S. Dep't of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (May 19, 2014), *available at* http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[26] No. 11 Cr. 00573 (N.D. Cal. Mar. 5, 2014).

[27] Press Release, U.S. Atty's Office for the N. Dist. of Cal., *Walter Liew Sentenced to 15 Years in Prison for Economic Espionage* (Jul. 11, 2014), *available at* http://www.fbi.gov/sanfrancisco/press-releases/2014/walter-liew-sentenced-to-15-years-in-prison-for-economic-espionage.

convicted of attempted economic espionage, attempted theft of trade secrets, bankruptcy fraud, tax evasion and obstruction of justice charges arising out of their participation in a scheme to steal DuPont's trade secrets and sell them to an entity controlled by the Chinese government. All three defendants were sentenced in the summer of this year. The most significant sentence was imposed on Defendant Walter Liean-Heen Liew—the alleged mastermind of the scheme—who was ordered to serve 15 years' imprisonment, forfeit $27.8 million in unlawful profits, and pay more than $367,000 in restitution to DuPont. Charges against two additional individuals and four other companies—including the Chinese-government controlled entities to which DuPont's trade secrets were sold—remain pending.

United States v. Bin (C.D. Cal.) [28]

In August 2014, a federal grand jury in California indicted Chinese businessman Su Bin for violations of the Computer Fraud and Abuse Act, conspiracy to steal trade secrets, and conspiracy to illegally export defense articles arising out of a scheme to infiltrate computer systems of Boeing and other U.S. companies to steal trade secret information about several military programs, including cargo aircrafts and fighter jets. As of the date of the indictment, Chen was being held in Canada following his arrest by Canadian authorities. A Canadian court has scheduled an extradition hearing for Bin for July 2015.[29]

Criminal Restitution Awards

United States v. Nosal (N.D. Cal.) [30]

As reported in last year's *Round-Up*, David Nosal was sentenced in 2013 to one year and one day of imprisonment and ordered to pay $60,000 in fines for violating the Computer Fraud and Abuse Act by misappropriating confidential information from a database maintained by his former employer, the executive search firm Korn/Ferry International.[31] This May, the court imposed an additional penalty on Nosal, finding that Korn/Ferry was entitled to restitution under the Mandatory Victims Restitution Act. The court ordered restitution of $827,983.25, representing (1) the costs that Korn/Ferry incurred in investigating the nature and scope of Nosal's theft, (2) the value of time Korn/Ferry's employees spent assisting the government's investigation and prosecution of Nosal, and (3) approximately $600,000 in attorneys' fees that Korn/Ferry incurred in connection with the investigation and prosecution.[32]

The court's restitution order in this case—as well as the significant restitution that Walter Liean-Heen Liew was ordered to pay to DuPont (discussed above)—are reminders that under certain circumstances criminal referral can be an attractive alternative option to civil litigation for corporate victims of trade secret theft.

Notable Acquittal in Long-Pending Trade Secret Theft Prosecution

United States v. Yeh (N.D. Tex.) [33]

In March 2014, a federal district court jury in Texas acquitted Ellen Chen Yeh, a former employee of Texas Instruments, of committing trade secret theft by downloading proprietary information concerning TI's semiconductor chips before moving to China to begin employment with a Shanghai-based competitor. Yeh's principal defense at trial was that she lacked the requisite intent under the EEA because she (1) was not aware that TI considered the downloaded files to be trade secrets and (2) only downloaded the files so that she would have them in the event that an employment opportunity with TI in China became available in the future.[34]

While the jury's verdict seems to underscore the difficulties of proving that a defendant intended to ''convert a trade secret'' with knowledge that the theft would ''injure [its] owner''[35] beyond a reasonable doubt, the *Yeh* prosecution is also notable for the extensive delays in prosecuting the case. Though the FBI detained and searched Yeh at the airport in 2005 before she flew to China, it failed to seize CDs in Yeh's possession that contained the TI data that Yeh had downloaded and allowed her to depart the country. After the indictment was filed in April 2008, Yeh remained abroad until April 2013 when she was detained at the South Korean border pursuant to an Interpol Red Notice. Yeh coordinated her return to the United States to face charges through counsel following her detention, ultimately returning in August 2013. Yeh's trial took place nearly six years after the indictment was filed and almost nine years after the alleged trade secret theft occurred.[36]

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.''[37] Employers who are the victims of trade secret misappropriation by their employees often bring claims for violation of the CFAA because such theft is often committed by accessing the employer's computer. However, to establish a violation of the CFAA in such circumstances, the employee must have (1) lacked authorization to access the computer or (2) ''exceed[ed]'' his or her ''authorized access.''

Continued Circuit Split Over ''Authorized Access'' Under the CFAA

A substantial circuit split remains over what types of conduct are cognizable under the ''exceeds authorized access'' prong. The Second, Fourth and Ninth Circuits have taken the ''narrow'' view that an employee's violation of a usage restriction—e.g., using a company com-

[28] No. 14 Cr. 00131 (C.D. Cal. Aug. 14, 2014).

[29] The Canadian Press, ''Su Bin, accused by FBI of hacking, has extradition pre-hearing next month'', *CBC News* (Oct. 8, 2014), *available at* http://www.cbc.ca/news/canada/british-columbia/su-bin-accused-by-fbi-of-hacking-has-extradition-pre-hearing-next-month-1.2793174.

[30] No. 08 Cr. 00237, 2014 BL 145070 (N.D. Cal. May 20, 2014).

[31] *See* 2013 TS Round-Up, *supra* note 1.

[32] No. 08 Cr. 00237 at *13 (N.D. Cal. May 20, 2014).

[33] No. 08 Cr. 00096 (N.D. Tex. Mar. 14, 2014).

[34] No. 08 Cr. 00096 (N.D. Tex. Mar. 3, 2014).

[35] 18 U.S.C. § 1832(a).

[36] No. 08 Cr. 00096 (N.D. Tex. Dec. 13, 2013).

[37] *See* 18 U.S.C. § § 1030(a)(2)(C), (a)(5)(C), (g) (2012).

  PTCJ ISSN 0148-7965

puter for non-business purposes—on a computer that the individual otherwise had a right to access does not violate the CFAA. In contrast, under the ''broad'' view adopted by the Fifth, Seventh and Eleventh Circuits, such usage violations are sufficient to state a claim under the CFAA.

In 2014, none of the outstanding circuits—the First, Third, Sixth, Eighth, Tenth and D.C. Circuits—definitively weighed in on the scope of the ''exceeds authorized access'' requirement. However, dicta from the Third Circuit's April 2014 decision in *United States v. Auernheimer*[38]—which reversed criminal convictions for violations of the CFAA due to improper venue—suggests that the Third Circuit may be leaning towards the narrow position on this issue. The defendants in *Auernheimer* had engaged in a practice known as ''slurping,'' in which they accessed public portions of AT&T's account login screens and obtained individuals' email addresses on those screens by exploiting a design flaw in the web page.[39] In a footnote, the court stated that in order for the government to show that the defendants were ''guilty of accessing [a computer] 'without authorization, or in excess of authorization,' '' it would need to prove that they had breached some code-or-password-based barrier to authorized access, regardless of whether they used the information they accessed in an unauthorized manner.[40] This dicta is arguably consistent with the position taken by the Second, Fourth and Ninth Circuits that usage violations are not cognizable under the CFAA.

Continued Debate Over What Constitutes ''Loss'' Under the CFAA

The CFAA requires that a civil plaintiff show, among other things, that it suffered a ''loss'' of at least $5,000 in any one-year period as a result of an intentional violation that recklessly caused damage.[41] The CFAA defines ''loss'' as ''any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.''[42] Courts are divided over whether a plaintiff can satisfy this requirement where the individual or entity did not experience any interruption of service but did incur costs in responding to the violation, conducting a damage assessment, or restoring data or programs to their prior condition before the violation occurred.[43] That is, some courts interpret the statute as providing ''interruption of service'' as just one of several methods of demonstrating loss, while others read the provision to require the loss to *result* from an interruption of service.[44]

In December 2014, the Sixth Circuit directly addressed this issue.[45] Yoder & Frey, a company that hosts auctions for used construction equipment, contracted with EquipmentFacts LLC (Efacts), an online bidding services company, to provide those services for Yoder & Frey's annual large auction in Florida. After the companies had a falling out, Yoder & Frey terminated the contract and hired another online bidding services company, RealtimeBid.com (RTB). Yoder & Frey alleged that Efacts then used a username and password of which it was aware from its prior relationship with Yoder & Frey to access RTB's bidding platform in a subsequent year's auction without authorization and enter numerous fraudulent bids. After an extensive investigation, Yoder & Frey traced the bids to Efacts. Yoder & Frey and RTB subsequently filed suit against Efacts for violations of the CFAA, among other claims. A jury returned a verdict for both plaintiffs but only awarded damages to RTB. Efacts then brought a motion for judgment as a matter of law, arguing that RTB had failed to show a ''loss'' cognizable under CFAA because it had failed to produce evidence establishing it suffered damages resulting from an ''interruption in service.'' The district court rejected this argument and denied Efacts' motion.[46]

On appeal, the Sixth Circuit affirmed the district court's denial of the motion for judgment as a matter of law, holding that ''it was not necessary that Plaintiffs establish that an 'interruption in service' occurred'' to show the requisite loss.[47] The court reasoned that the ''loss'' was ''defined in the disjunctive'' in the provision at issue.[48] As a result, the court held that if ''a plaintiff is able to establish a loss of at least $5,000 in value, whether that be composed solely of costs identified in the first clause, or solely costs identified in the second clause, or a combination of both, then he may recover under the statute.''[49] Applying that reading, the court concluded that Efacts' actions had sufficiently caused ''loss'' by requiring RTB to investigate the incident and conduct a damage assessment, regardless of whether any of RTB's damages stemmed from an interruption of service.[50]

CIVIL DEVELOPMENTS

In 2014, both federal and state courts considered a variety of substantive and procedural issues with respect to trade secret claims, including the extent to which the UTSA preempts common law claims protecting confidential information that does not qualify as a ''trade secret'' and whether certain types of information—including ''mere ideas'' and undisclosed data underlying published materials—are eligible for trade secret protection. We discuss these and other developments in civil trade secret litigation below.

[38] 748 F.3d 525, 2014 BL 101472 (3rd Cir. 2014).
[39] *Id.* at 534, n. 5.
[40] *Id.*
[41] 18 U.S.C. § 1030(c)(4)(A)(i)(I).
[42] 18 U.S.C. § 1030(e)(11).
[43] *See Continental Group, Inc. v. KW Property Mgmt, LLC*, 622 F. Supp. 2d 1357, 1371, 2009 BL 185585 (2009) (collecting cases); *Southern Parts & Eng'r'g Co. v. Air Compressor Services, LLC,* No. 13 Cv. 02231 at *11, *12 n. 5. (N.D. Ga., Feb. 19, 2014) (same).
[44] *See Continental v. KW*, 622 F. Supp. 2d at 1371 (collecting cases); *Southern Parts v. Air Compressor*, No. 13 Cv. 02231, at *11, *12 n. 5 (same).
[45] *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, No. 14 Cv. 03002, 2014 BL 360420 (6th Cir. Dec. 22, 2014).
[46] *Id.* at *8.
[47] *Id.* at *9-10.
[48] *Id.* at *9.
[49] *Id.*
[50] *Id.*

Preemptive Effect of the UTSA

More than three decades after the UTSA was first introduced, courts continue to grapple with whether and to what extent the UTSA preempts common law and statutory claims providing remedies for the misappropriation of confidential information that does not qualify as a ''trade secret.''

Many courts that have addressed this issue have concluded that the UTSA preempts such claims, reasoning that a broad construction of the UTSA's preemption provision—which displaces ''conflicting tort[s]'' and other laws ''providing civil remedies for misappropriation of a trade secret''[51]—best effectuates the UTSA's goal of replacing the patchwork of state-by-state common law torts used to enforce the protection of trade secrets with a uniform statutory remedy.[52] The Arizona Supreme Court squarely bucked that trend in its November 2014 decision in *Orca Communications Unlimited LLC v. Noder*,[53] holding that Arizona's version of the UTSA did not preempt an unfair competition claim based on the theft of confidential, but non-trade secret, information. The court concluded that the Arizona UTSA's preemption provision unambiguously ''displaces only conflicting tort claims for 'misappropriation' of a '*trade secret*,' '' and that had the legislature intended a ''broader displacement,'' it ''was required to express that intent clearly.''[54] Notwithstanding this ongoing debate, common law claims for the protection of confidential information are often pled in the alternative to trade secret claims, and the misappropriation of confidential, non-trade secret information in violation of a confidentiality agreement can also give rise to a separate cause of action for breach of contract.[55]

In addition to the substantive preemption issue, courts have taken conflicting views as to whether the preemptive effect of the UTSA is a question that is appropriate for adjudication on a motion to dismiss or a fact-issue more appropriately considered at summary judgment or trial. In *U.S. Legal Support Inc. v. Hofioni*,[56] a district court in California recently declined to dismiss state law claims for breach of the duties of loyalty and confidence, conversion and unfair competition on preemption grounds. Somewhat ironically, the court invoked the defendants' own complaints that the plaintiff's claims were based on confidential, proprietary ''and/or'' trade secret information—and that the plaintiff had ''fail[ed] to identify with any reasonable particularity where its trade secrets stop and its non-trade secret[s] . . . begin[]''—in concluding that the issue of preemption was more ''properly addressed'' at summary judgment and after full discovery.[57]

[51] National Conference of Commissioners on Uniform State Laws, Uniform Trade Secrets Act with 1985 Amendments § 7(a) (1985).

[52] *See, e.g.*, *Firetrace USA, LLC v. Jesclard*, 800 F. Supp. 2d 1042, 1047-48 (D. Ariz. 2010) (collecting cases); *CDC Restoration v. Tradesmen Contractors*, 274 P.3d 317, 329-30 (Utah App. 2012) (collecting cases).

[53] 337 P.3d 545 (Ariz. 2014).

[54] *Id.* at 550.

[55] *See* National Conference of Commissioners on Uniform State Laws, Uniform Trade Secrets Act with 1985 Amendments § 7(a) (1985).

[56] No. 13 Cv. 01770, 2013 BL 353322 (E.D. Cal. Dec. 19, 2013).

[57] *Id.* at *25.

Information Eligible for Trade Secret Protection

Federal and state courts continued to be confronted this year with the recurring issue of what types of information merit protection as a ''trade secret.'' Notable decisions in this area involved the trade secret eligibility of data underlying publicly-disclosed information and the circumstances in which an idea may be protected as a trade secret.

Hallmark Cards Inc. v. Monitor Clipper Partners LLC (8th Cir.)[58]

In July 2014, the Eighth Circuit considered whether the public disclosure of conclusions based on a set of underlying, undisclosed data necessarily renders that data ineligible for protection as a trade secret. Monitor Company Group L.P. was hired by Hallmark to compile confidential research on consumer behavior in the greeting card market. Monitor provided its market research to Hallmark and, unbeknownst to Hallmark, to a private equity group called Monitor Clipper Partners LLC, which allegedly used the information in connection with its acquisition of one of Hallmark's competitors. Monitor settled with Hallmark for $16.6 million before trial, but a jury found Clipper liable for breach of contract and misappropriation of trade secrets and awarded Hallmark compensatory and punitive damages totaling more than $30 million.

On appeal, Clipper argued that because Hallmark had published general conclusions about the greeting card market based on the data provided by Monitor, the allegedly misappropriated information could no longer qualify as a trade secret. The Eighth Circuit rejected that argument and concluded that there was sufficient evidence to support the jury's verdict.[59] The court emphasized that Hallmark had neither published the underlying data nor any information about how it reached the conclusions about the greeting card market that were publicly disclosed. The court also reasoned that others could reach different conclusions based on the same data, which gave the data value that was independent of the conclusions published by Hallmark.[60]

Altavion, Inc. v. Konica Minolta Sys. Lab. Inc. (Cal. Ct. App.) [61]

A California appellate court recently considered whether design concepts that a defendant allegedly misappropriated constituted ''generalized ideas'' ineligible for protection as trade secrets. The origin of the case was a non-disclosure agreement between Altavion, a company that develops digital stamping technology to create self-authenticating documents, and Konica Minolta Systems, a printer company, in connection with the negotiation of an agreement for Altavion to provide digital stamping design concepts to assist Konica with the development of a new product. Before the negotiations were terminated, Konica filed several patent applications which allegedly incorporated Altavion's design concepts. Upon discovering Konica's applications, Altavion sued Konica for misappropriation of trade secrets, breach of the non-disclosure agreement and other torts. Following a bench trial, the court found in favor of Altavion.[62]

[58] 758 F.3d 1051, 111 U.S.P.Q.2d 1538 (8th Cir. 2014) (88 PTCJ 756, 7/18/14).

[59] *Id.* at 1056-57.

[60] *Id.*

[61] 226 Cal. App. 4th 26, 2014 BL 129306 (2014).

[62] *Id.* at 34.

   ISSN 0148-7965

On appeal, Konica argued that the design concepts incorporated in its patent applications were merely ''generalized ideas''—as opposed to ''a set of products or specific formulae''—that may be eligible to be patented but are not eligible for trade secret protection.[63] In assessing that argument, the court examined the interplay between patent and trade secret law, reasoning that the former protects the actual use of an idea while the latter ''protects only the right to control the dissemination of information.''[64] The court nonetheless strongly rejected Konica's argument that a patentable idea can never qualify as a trade secret, reasoning that so long as it is kept confidential, the ''idea itself'' can qualify as the type of information whose dissemination is protected by trade secret law.[65] The court went on to hold that trade secret protection extended to the design concepts at issue because Altavion did not disclose them to other parties and the disclosure to Konica was subject to a non-disclosure agreement.[66]

Bianco v. Globus Med., Inc. (E.D. Tex.)[67]

A federal district court in Texas recently considered a similar issue in a case involving a non-disclosure agreement between a physician and Globus Medical, a medical device manufacture, concerning a potential agreement to manufacture the physician's idea for a new design for implants used in spinal fusion surgeries. After the negotiations proved unsuccessful, Globus began marketing an implant that was allegedly based on the physician's design. The physician sued Globus for misappropriation of trade secrets and was awarded (1) approximately $4.3 million in damages for past trade secret misappropriation and (2) an ongoing royalty of 5 percent of the net sales of the implant for a maximum period of 15 years.[68] Globus then moved for judgment as a matter of law, arguing that the implant design was a ''mere idea'' that was ineligible for trade secret protection as a matter of Texas law.[69] The court disagreed and denied Globus' motion, holding that ''[i]deas, whether 'mere' or otherwise, are protected from misappropriation as long as they provide an opportunity to obtain a business advantage over competitors and are maintained in secret.''[70]

Alleging and Proving Misappropriation

Two recent federal district court decisions underscore the importance of identifying trade secrets with particularity and the challenges that companies face in establishing misappropriation through indirect or circumstantial evidence.

Purchasing Power, LLC v. Bluestem Brands, Inc. (N.D. Ga.) [71]

Bluestem was a national retailer who sold products primarily to low income and ''credit-constrained'' consumers through installment payment plans.[72] Purchasing Power was a retailer who sold ''big[ger] ticket'' consumer products through a ''voluntary payroll deduction program.''[73] The two companies entered into a non-disclosure agreement in August 2010 to explore a possible merger. Shortly before entering into the NDA, Bluestem created an internal project team to develop its own payroll-deduction model, which was screened off from the team responsible for conducting due diligence for the potential merger or acquisition. After the negotiations proved to be unsuccessful, Bluestem launched its payroll deduction service. Purchasing Power then sued Bluestem for misappropriation of trade secrets, among other torts.

In May, the district court granted Bluestem's motion for summary judgment, concluding that Purchasing Power had identified only ''general categories of information''—e.g., a ''unique underwriting process'' and ''areas . . . of its business utilizing unique approaches and processes''—that were insufficient to satisfy Purchasing Power's burden of alleging and proving the existence of a protectable trade secret.[74] The court also held that summary judgment was appropriate as to the separate element of misappropriation, concluding that the purported ''circumstantial evidence'' of misappropriation that Purchasing Power pointed to was insufficient to overcome the substantial direct evidence that Bluestem had not developed its payroll deduction model using Purchasing Power's information—including testimony from Bluestem employees and evidence detailing how the payroll deduction model was developed.[75] The court similarly reasoned that certain ''similarities'' between the two models were insufficient to avoid summary judgment in light of that direct evidence.

Integral Dev. Corp. v. Tolat (N.D. Cal.) [76]

A California federal district court recently addressed these same issues and, as in *Bluestem*, concluded that the plaintiff had failed to identify its trade secrets with sufficient particularity or adequately establish an inference of misappropriation on the basis of circumstantial evidence. Integral Development—a company that designed software for ''online trading and liquidity aggregation on the foreign exchange market''[77]—sued a former employee for misappropriating its source code in connection with his employment with a competitor. In February 2014, the district court granted the former employee's motion for summary judgment, concluding that Integral's failure to identify the ''specific source code files'' and the trade secrets they contained was ''fatal'' to its misappropriation claim.[78] The court also concluded that neither of the key pieces of circumstantial evidence on which Integral relied—*i.e.*, that the former employee downloaded Integral's source code at the same time that he was discussing employment opportunities with the competitor, and that the competitor was able to quickly develop a competing software product after hiring the employee—demonstrated that the former employee ''must have used the information he downloaded improperly.''[79]

[63] *Id.* at 53.
[64] *Id.* at 54.
[65] *Id.* at 55.
[66] *Id.* at 61.
[67] No. 12 Cv. 00147, 2014 BL 301993 (E.D. Tex. Oct. 27, 2014) (89 PTCJ 25, 11/7/14).
[68] *Id.* at *3.
[69] *Id.* at *15.
[70] *Id.* at *17.
[71] 22 F. Supp. 3d 1305, 2014 BL 130561 (N.D. Ga. 2014).
[72] *Id.* at 1308.
[73] *Id.*
[74] *Id.* at 1313.
[75] *Id.* at 1317-18.
[76] No. 12 Cv. 06575, 2014 BL 51364 (N.D. Cal. Feb. 24, 2014).
[77] *Id.* at *2.
[78] *Id.* at *5.
[79] *Id.* at *6.

Reasonableness of Measures to Protect Trade Secrets

nClosures Inc. v. Block and Co. (7th Cir.) [80]

The Seventh Circuit recently applied a demanding threshold for what constitutes ''reasonable measures'' to protect a company's proprietary information in the context of a claim for breach of a confidentiality agreement. NClosures, an industrial design firm, entered into a confidentiality agreement with Block and Co. to discuss and evaluate a potential business relationship to develop and manufacture metal cases for electronic tablets, such as iPads. Although the two companies did business together for a period of time, Block eventually developed its own metal cases and ended its relationship with nClosures. NClosures then sued Block for fraud, trade secret misappropriation, breach of fiduciary duty and breach of contract. The district court granted summary judgment for Block on all four claims, but nClosures appealed the court's ruling only with respect to the breach of contract and fiduciary duty claims.

In October 2014, the Seventh Circuit affirmed. With respect to nClosures' claim for breach of the confidentiality agreement, the Seventh Circuit agreed with the district court that nClosures had not taken reasonable steps to maintain the confidentiality of its proprietary information. Although acknowledging that the parties had signed a confidentiality agreement at the outset of their partnership, the court found it significant that nClosures had taken virtually no other step to protect the confidentiality of its designs. In particular, the court found it significant that (1) no additional confidentiality agreements were required of other individuals who accessed the designs during the course of the parties' collaboration; (2) none of the designs had been marked ''confidential'' or ''contains proprietary information''; (3) the designs were ''not kept under lock and key'' or ''stored on a computer with limited access''; and (4) contrary to nClosure's stated policy, it had not required a designer and manufacturers who had produced previous versions of the product to sign confidentiality agreements.[81]

E.I. DuPont De Nemours & Co. v. Kolon Indus., Inc. (4th Cir.) [82]

A recent decision by the Fourth Circuit serves as a cautionary tale of the potential consequences that disclosing trade secret information in litigation can have in future actions concerning similar or related types of trade secrets.

As discussed in last year's *Round Up*, in 2013 DuPont secured a favorable jury verdict and a damages award of nearly $1 billion in its long-running suit against Kolon Industries—a South Korean synthetic fiber producer—over Kolon's alleged misappropriation of DuPont's process for producing Kevlar, a high strength fiber that is used in ballistics, bullet-resistant armor and industrial and automotive products.[83] Before trial, the district court granted DuPont's motion in limine to exclude evidence that was introduced during DuPont's intellectual property litigation against another company, AkzoNobel, in the 1980s (the Akzo Litigation). Kolon had argued that certain trial exhibits introduced in that litigation contained details of the Kevlar production process that were similar to aspects of several of the trade secrets underlying DuPont's misappropriation claim.

In a per curiam opinion issued in May, the Fourth Circuit concluded that the district court's ''blanket exclusion'' order was an abuse of discretion and vacated the jury's verdict and damages award. The court rejected the district court's conclusion that evidence from the Akzo Litigation was irrelevant because it did not ''amount[] to an actual trade secret at issue in this case.''[84] Instead, the Court found it sufficient that evidence from the Akzo Litigation contained details about DuPont's production process that were ''strikingly similar'' to several aspects of the trade secrets at issue in the present litigation, and it reasoned that such evidence was probative of whether DuPont had taken reasonable efforts to maintain their confidentiality. Though the court acknowledged that, as a general matter, the ''mere presence'' of confidential information in public court files does not make the information '' 'generally known' for purposes of the UTSA,'' it held that whether DuPont's production processes remained protectable as trade secrets despite the disclosures in the Akzo Litigation was a ''fact-intensive question to be resolved upon trial.''[85]

Remedies

PharMerica Corp. v. McElyea (N.D. Ohio)[86]

A federal district court in Ohio recently considered the appropriateness of a preliminary injunction restraining the disclosure of trade secrets where it was undisputed that (1) no disclosure of trade secrets at issue had yet occurred, and (2) the defendant no longer possessed documents containing those trade secrets. McElyea, a former account executive of PharMerica—a company that sells products and services to skilled nursing facilities—downloaded client lists, pricing and strategy information, and contracts to a thumb drive before she left PharMerica to work for a competitor. PharMerica sued McElyea for misappropriation and moved for a preliminary injunction; while that motion was pending, McElyea returned the documents at issue to PharMerica.

Though there was no evidence that McElyea had contacted any of PharMerica's clients or disclosed any of the information she had downloaded, the court nonetheless issued a preliminary injunction restraining McElyea from contacting any PharMerica clients or clients that she had solicited on PharMerica's behalf during the six months prior to her departure. The court rejected McElyea's argument that it was not authorized to enter an injunction in the absence of evidence of a prior disclosure, holding that such injunctions are permissible where ''the former employee possess[es] timely, sensitive, strategic, and/or technical information that . . . pose[s] a serious threat to his former employer's business.''[87] The court also concluded that the fact that

[80] 770 F.3d 598, 112 U.S.P.Q.2d 1774 (7th Cir. 2014) (88 PTCJ 1699, 10/31/14).

[81] *Id.* at 602.

[82] 564 Fed. Appx. 710, 2014 BL 93219 (4th Cir. 2014).

[83] *See DuPont*, 564 Fed. Appx at 711; 2013 TS Round-Up, *supra* note 1.

[84] *DuPont*, 564 Fed. Appx. at 714.

[85] *Id.* at 715.

[86] No. 14 Cv. 00774, 2014 BL 130503 (N.D. Ohio May 9, 2014).

[87] *Id.* at *8.

   ISSN 0148-7965

McElyea had returned the documents she downloaded ''does not mean she no longer has confidential information to use on behalf of'' her new employer, including her knowledge of PharMerica's pricing information and strategies.[88]

StorageCraft Tech. Corp. v. Kirby (10th Cir.) [89]

In March 2014, the Tenth Circuit held that Utah's version of the UTSA authorizes a ''reasonable royalty'' as damages for misappropriation regardless of whether the defendant personally makes ''commercial use'' of the trade secret. Kirby, a cofounder and former director of StorageCraft—a software development company—disclosed the company's computer source code to a rival competitor after a ''falling out'' with his former colleagues. Following a trial on StorageCraft's misappropriation claim, the jury awarded StorageCraft a reasonable royalty of $2.92 million. On appeal, Kirby sought to draw upon common law misappropriation precedent and the federal patent infringement statute in support of his argument that the award was invalid because he did not put the source code to ''commercial use'' for his personal profit. The Tenth Circuit rejected that argument, holding that the express language of the Utah UTSA—which authorizes a reasonable royalty as damages for the ''*disclosure or use* of a trade secret''—does not require the defendant to have personally used the trade secret for commercial gain.[90]

TNS Media Research, LLC v. TiVo Research & Analytics, Inc. (S.D.N.Y.) [91]

In November 2014, Judge Shira A. Scheindlin of the U.S. District Court for the Southern District of New York awarded TNS Media Research attorneys' fees and expenses it incurred in successfully defending against counterclaims for patent infringement and misappropriation of trade secrets brought against it by TiVo Research & Analytics. TNS sued TiVo in 2011 for a declaratory judgment of noninfringement of a patent for technology that determines which television programs are the best match for advertisers seeking to market specific products. In response, TiVo brought several counterclaims against TNS, including claims for patent infringement and 24 counts of misappropriation of trade secrets. TiVo dropped 19 of its trade secret claims shortly after TNS moved for summary judgment, and the court granted summary judgment on the remainder of those claims in November 2013.

In its November 2014 decision, the district court relied on its inherent authority—which requires a finding that the sanctioned party's claims were both ''entirely without color'' and ''brought in bad faith''—to award attorneys' fees with respect to TiVo's misappropriation claims.[92] The court concluded that each of TiVo's trade secret claims were sanctionable under that standard because TiVo had either (1) alleged misappropriation claims that failed as a matter of law, (2) previously disclosed most of the properties of the information it alleged was misappropriated, and/or (3) failed to show any misappropriation of that information.

Though the district court relied on its inherent authority to impose sanctions with respect to the misappropriation claims, a recent decision by the U.S. Supreme Court may have the result of relaxing the standard for awarding attorneys' fees in trade secret cases governed by the UTSA. In its April 2014 decision in *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*,[93] the Supreme Court adopted a significantly more flexible standard for awarding attorneys' fees under 35 U.S.C. § 285, which authorizes an award of attorneys' fees in patent cases where the case is ''exceptional.'' The *Octane* Court held that claims need not be objectively baseless or brought in bad faith to qualify as ''exceptional''—instead, the case need only ''stand[] out from others with respect to the substantive strength of a party's litigating position . . . or the unreasonable manner in which the case was litigated.''[94] This holding may prove to have significance in trade secret cases given the comment to Section 4 of the UTSA, which cites 35 U.S.C. § 285 and states that ''patent law is followed in allowing the judge to determine whether attorney's fees should be awarded even if there is a jury.''[95] The district court in *TNS Media* unsurprisingly did not address that issue given that New York has not adopted the UTSA.

Retiree, Inc. v. Anspach (D. Kan.) [96]

In July 2014, the District of Kansas enforced a liquidated damages clause in a confidentiality agreement after concluding that the defendant breached that agreement by misappropriating the plaintiff's proprietary information. Retiree Inc. and Dana Anspach entered into confidentiality and non-compete agreements in connection with the negotiation of a potential merger of their respective financial planning businesses. The confidentiality agreement included a liquidated damages provision entitling Retiree to recover $250,000 for each violation of the agreement by Anspach. After the attempted merger failed, Anspach allegedly began using the financial planning processes and strategies that she had been exposed to during the merger negotiations for her own business and disclosed them to Retiree's competitors.

Retiree sued Anspach in 2012 for breach of the confidentiality agreement, and, following a bench trial, the court found in favor of Retiree and enforced the liquidated damages clause. The court concluded that the liquidated damages clause was ''particularly appropriate'' given that the damages suffered by Retiree—which included ''diminishing the novelty'' of its trade secrets and competition from Anspach—would be ''difficult, if not impossible, to calculate.''[97] The Court also held that the amount of liquidated damages was reasonable in light of evidence that Retiree lost a licensing opportunity potentially worth a similar amount as a result of Anspach's disclosure of Retiree's trade secrets.

---

[88] *Id.*

[89] 744 F.3d 1183, 109 U.S.P.Q.2d 2110 (10th Cir. 2014) (87 PTCJ 1093, 3/14/14).

[90] *Id.* at 1186.

[91] No. 11 Cv. 04039, 2014 BL 311568 (S.D.N.Y. Nov. 4, 2014).

[92] *Id.* at *40.

[93] 134 S. Ct. 1749, 2014 BL 118431, 110 U.S.P.Q.2d 1337 (2014) (88 PTCJ 28, 5/2/14).

[94] *Id.* at 1756.

[95] National Conference of Commissioners on Uniform State Laws, Uniform Trade Secrets Act with 1985 Amendments § 4 (1985).

[96] No. 12 Cv. 02079, 2014 BL 184358 (D. Kan. July, 2, 2014).

[97] *Id.* at *15.

Collateral Attacks on Trade Secret Protection Efforts

Two recent decisions from the Eastern District of Michigan and the Western District of Pennsylvania addressed creative attempts by plaintiffs to ''collaterally attack'' their former employers' efforts to protect their trade secrets.

Bonds v. Philips Elec. N. Am. (E.D. Mich.) [98]

In January 2014, a federal district court in Michigan strongly rejected an employee's attempt to hold his former employer liable for tortious interference with a business relationship for advising his new employer of the employee's continuing obligations under confidentiality agreements, which allegedly resulted in the employee losing his job. The plaintiff, a former employee of Philips Electronic, was responsible for maintaining and repairing medical imaging equipment. He was fired when Philips discovered that he had taken a second job working for Barrington, a competitor. Following his termination, Philips sent a letter to the plaintiff and Barrington asking both to confirm in writing that the plaintiff had not disclosed any of Philips' confidential information to Barrington. When Barrington fired the plaintiff approximately one week later, he sued Philips for tortious interference, alleging that Barrington fired him after receiving Philips's letter out of fear of becoming involved in litigation. The court granted summary judgment on the tortious interference claim on several independent grounds. Most importantly, the court concluded that Philips' letter to Barrington was not actionable as a matter of law because it was motivated by ''concern about potential disclosure [of confidential information]''—''exactly the kind of legitimate business reason that insulates [an employer] from liability.''[99]

Peek v. Whittaker (W.D. Pa.) [100]

A federal district court in Pennsylvania recently held that the Pennsylvania UTSA does not create a ''standalone'' claim for attorneys' fees as a remedy for defending against a misappropriation claim in a separate lawsuit that was allegedly brought in bad faith. A carpet cleaning company named Whittaker was sued for numerous torts—including fraud, unfair competition and abuse of process—by a former employee, his business partner and their company for Whittaker's conduct during a state court lawsuit against them for misappropriation of trade secrets. The crux of the plaintiffs' claims was their allegation that Whittaker had sued them to interfere with their establishment of a competing venture. In May 2014, the court denied Whittaker's motion to dismiss with respect to the majority of the claims, but granted the motion with respect to the plaintiffs' claim for attorneys' fees, which they sought to recover under Pennsylvania's Uniform Trade Secrets Act as a ''result of having to defend'' against Whittaker's allegedly bad-faith misappropriation claims. As the court explained, it could find no support for the plaintiff's argument that Section 5305 of the Pennsylvania UTSA—which authorizes an award of attorneys' fees to the ''prevailing party'' where, among other circumstances, a ''claim of misappropriation is made in bad faith''—''creates a standalone cause of action for attorneys' fees . . . to be recovered in a separate lawsuit'' than the case in which the allegedly bad-faith claims were asserted.[101]

Developments in High-Stakes Trade Secret Cases in 2014

Seagate Tech. LLC v. W. Digital Corp. (Minn.) [102]

The Supreme Court of Minnesota recently declined to vacate an arbitrator's award of more than $600 million against a former employee of Seagate Technology and his new employer, Western Digital Corp., for misappropriation of Seagate's trade secrets. According to the court, the arbitrator concluded that the former employee had altered documents in an attempt to establish that some of the trade secrets at issue had been publicly disclosed before he left Seagate.[103] As a result, the arbitrator ordered that the defendants would be precluded from presenting any evidence or defense disputing the validity, misappropriation, or use of the trade secrets.[104] The arbitrator ultimately awarded Seagate $525 million in compensatory damages, prejudgment interest of approximately $96 million, and post-judgment interest on certain of Seagate's trade secrets claims.[105] In October 2014, the Minnesota Supreme Court declined to vacate the arbitrator's award, concluding that the arbitrator was authorized to issue the sanctions at issue under a broad clause in the arbitration provision that authorized the granting of ''injunctions or other relief.''[106] While acknowledging the risk that ''entrusting an arbitrator with broad powers over forms of relief'' can ''lead to unfair results in arbitration,'' the court emphasized that the decision to arbitrate ''necessarily limited the availability of the protections and advantages of the judicial system.''[107]

MGA Entm't Inc. v. Mattel Inc. (L.A. Sup. Ct.) [108]

The underlying dispute between Mattel and MGA Entertainment—the respective makers of the Barbie and Bratz dolls—originally began when Mattel sued MGA for trade secret misappropriation over a decade ago, alleging that a former Mattel employee had designed the Bratz dolls while working for Mattel. After the Ninth Circuit vacated a jury verdict in favor of Mattel—but before a second trial—the district court granted MGA's motion to add counterclaims for trade secret misappropriation and Racketeer Influenced and Corrupt Organizations Act (RICO) violations based on alleged corporate espionage by Mattel. MGA framed its claims as compulsory counterclaims-in-reply which, under Federal Rule of Civil Procedure 13(a)(1)(A), allowed them to be brought outside of the relevant limitations period. Although the court granted summary judgment on MGA's RICO counterclaim, in the second trial the jury found for MGA on its misappropriation counterclaim and awarded it $172 million in damages. On appeal, as discussed in detail in the 2013 *Round-Up*,[109] the Ninth Circuit concluded that MGA's surviving counterclaim for misappropriation was not compulsory and

[98] No. 12 Cv. 10371, 2014 BL 20595 (E.D. Mich. Jan. 21, 2014).
[99] *Id.* at *17.
[100] No. 13 Cv. 01188, 2014 BL 143002 (W.D. Pa. May 22, 2014).
[101] *Id.* at *14-15.
[102] 854 N.W. 2d 750, 2014 BL 282893 (Minn. 2014).
[103] *Id.* at 755-56.
[104] *Id.*
[105] *Id.*
[106] *Id.* at 754.
[107] *Id.* at 765.
[108] BC532708 (L.A. Sup. Ct. Dec. 3, 2014).
[109] *See* 2013 TS Round-Up, *supra* note 1.

  PTCJ ISSN 0148-7965

should not have reached the jury because it was time-barred. The court therefore vacated the jury award and ordered the district court to dismiss the claim without prejudice on remand.[110]

As also reported in last year's *Round-Up*, on Jan. 13, 2014, MGA filed a new action against Mattel in Los Angeles Superior Court.[111] MGA's latest complaint 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.''[112] MGA seeks $1 billion in compensatory damages, exemplary damages, a permanent injunction and attorneys' fees.[113] Most recently, on Dec. 3, 2014, the California court denied Mattel's demurrer in which Mattel had argued that the state court suit was barred by *res judicata*.[114]

MSC Software Corp. v. Altair Eng'g, Inc. (E.D. Mich.)[115]

In November 2014, a federal district judge vacated a $26 million jury award and ordered a new trial on damages in litigation between MSC Software Corp. and Altair Engineering that dates back to 2007. The vacatur was the result of MSC's failure to introduce competent evidence of what would constitute a reasonable royalty for the misappropriated information.[116] The court also criticized MSC for failing to apportion damages to each trade secret that was allegedly misappropriated.[117]

Asian Am. Entm't Corp. v. Las Vegas Sands Corp. (D. Nev.) [118]

In July 2014, Asian American Entertainment Corp. (AAE) brought a suit for misappropriation of trade secrets, among other claims, against Las Vegas Sands, seeking $5 billion in damages stemming from AAE's unsuccessful bid for a Macau gambling license in 2002 that Las Vegas Sands allegedly secured using confidential information obtained during negotiations with AAE.[119] The litigation followed two related suits by AAE against Las Vegas Sands, including a suit before the same Nevada federal court which was dismissed with prejudice in 2007 and another in Macau. In its new complaint, AAE asserted that it only obtained a copy of Las Vegas Sands' bid proposal—which allegedly demonstrates Las Vegas Sands' improper use of AAE's proprietary information—in 2011.[120] In December, Las Vegas Sands filed a motion for sanctions, arguing that the court had previously dismissed with prejudice claims arising out of the same facts at issue in the present litigation. Las Vegas Sands also argued that AAE's allegations about the timing of its knowledge of defendants' casino proposal were untrue and designed to avoid the *res judicata* effect of AAE's prior lawsuit's dismissal and evade the statute of limitations.[121] Days after the sanctions motion was filed, AAE voluntarily dismissed the case.[122]

Nike, Inc. v. Dekovic (Cir. Ct. Multnomah Co.) [123]

In December 2014, Nike sued three of its former footwear designers in an Oregon state court seeking injunctive relief and $10 million in damages. Nike alleges that, while still employed by Nike, the three designers developed a strategy for a creative design studio to compete against Nike, began consulting for Nike's rival Adidas, misappropriated Nike trade secrets for use in their new business venture with Adidas, and attempted to conceal evidence of their unlawful acts by destroying or deleting evidence.[124] According to the complaint, the stolen Nike trade secrets include ''a treasure trove of Nike product designs, research information, and business plans.''[125] These allegations form the basis for Nike's misappropriation of trade secrets claim and seven related tort and contract claims, including (i) conversion and (ii) breach of the designers' non-compete and invention and secrecy contracts. The court granted Nike's motion for a temporary restraining order against all three defendants, which requires, among other things, that the defendants turn over their devices for a forensic examination. The parties subsequently stipulated to the entry of a preliminary injunction, and trial is scheduled for summer 2015. Gibson Dunn represents Nike in the lawsuit.

Bus. Logic Holding Corp. v. Ibbotson Assocs., Inc. (Cir. Ct. Cook Co.)[126]

In July 2014, Ibbotson Associates and its parent company Morningstar Inc. agreed to settle trade secret misappropriation and breach of contract claims against them by Business Logic Holding Corporation. In 2003, Business Logic and Ibbotson, both software companies serving financial institutions and investors, entered into a contract in which Business Logic gave Ibbotson the right to combine Business Logic's software with its own to develop a retirement plan management project. Morningstar, a provider of independent investment research, acquired Ibbotson in 2006. After Ibbotson's contract with Business Logic ended, Business Logic filed suit in 2009, alleging that Morningstar launched a new software product that was developed with Business Logic's trade secrets. As part of the settlement, Morningstar paid Business Logic $61 million representing past damages and consideration for future rights to use the intellectual property at issue.[127]

State Government Civil Activity

The trend of state governments bringing or threatening to bring their own civil lawsuits to protect trade secret interests under state unfair competition statutes continued in 2014. In 2014, Louisiana successfully used the threat of an unfair competition suit to reach a settlement with a Chinese barbeque grill manufacturer. Near the end of 2013, Louisiana State Attorney General James Caldwell sent a letter to Guangdong Canbo Elec-

[110] *Mattel, Inc. v. MGA Entm't, Inc.*, 705 F.3d 1108, 1110-11, 105 U.S.P.Q.2d 1574 (9th Cir. 2013) (85 PTCJ 453, 2/1/13).
[111] BC532708 (L.A. Sup. Ct. Jan. 13, 2014).
[112] *Id.* at ¶ 3.
[113] *Id.* at *41.
[114] BC532708 (L.A. Sup. Ct. Dec. 3, 2014).
[115] No. 07 Cv. 12807, 2014 BL 323999 (E.D. Mich. Nov. 13, 2014).
[116] *Id.* at *26-27.
[117] *Id.* at *2.
[118] No. 14 Cv. 01124 (D. Nev. July 9, 2014).
[119] *Id.* at ¶¶ 64-67.
[120] *Id.*
[121] No. 14 Cv. 01124 *1, *4-5 (D. Nev. Dec. 2, 2014).
[122] No. 14 Cv. 01124 (D. Nev. Dec. 27, 2014).
[123] No. 14 Cv. 18876 (Cir. Ct. Multnomah Co. Dec. 8, 2014).
[124] *Id.* at ¶ 1.
[125] *Id.* at ¶ 5.
[126] No. 09 Ch. 46687 (Cir. Ct. Cook Co. 2009).
[127] *See* Morningstar Inc., Current Report (Form 8-K), Exhibit 10.1 (July 17, 2014), available at http://www.sec.gov/Archives/edgar/data/1289419/000110465914052003/a14-17342_1ex10d1.htm.

trical Appliance Co. alleging that the manufacturer was using pirated American business software to compete against American manufacturers. Louisiana threatened to bring suit under Louisiana's 2010 Unfair Trade Practices Act, which specifically identifies software piracy as an unfair trade practice. In March 2014, Louisiana announced that Guangdong agreed to pay over $250,000 to software providers, as well as to submit to a compliance audit next year.[128]

A few days after Louisiana's announcement, Oklahoma State Attorney General Scott Pruitt filed a lawsuit against Neway Valve Co., China's largest valve manufacturer, alleging that it was unlawfully using pirated software in its valve manufacturing process to gain an unfair competitive advantage in Oklahoma's oil and gas industry. The lawsuit seeks to recover civil penalties, bar imports into Oklahoma by Neway until it complies with licensing requirements, and require Neway to provide a biannual software inventory to the state for five years and to submit to court-appointed trustees who would verify compliance.[129]

[128] Press Release, La. Office of the Att'y General, *Louisiana Attorney General leads crackdown on software piracy* (Mar. 6, 2014), *available at* https://www.ag.state.la.us/Article.aspx?articleID=823&catID=2.

[129] *Oklahoma v. Neway Valve Co.*, No. 14 Cj. 01482 (Ok. D. Ct. Mar. 13, 2014).

CONCLUSION

2014 made clear that U.S. companies continue to face threats to their trade secrets and intellectual property from sophisticated theft and misappropriation schemes, including several high-profile attacks on U.S. trade secrets in 2014 involving foreign interests and foreign governmental actors. Although foreign cyber-attacks may attract more press attention than other types of trade secret theft, developments in 2014 also underscored that companies continue to face potential threats to their intellectual property interests from unscrupulous competitors, former employees and joint venture partners. In light of these developments and trends, it will be all the more important in 2015 for companies to continue to regularly assess all aspects of their intellectual property safeguards.

Judicial and legislative developments in 2014 also serve as a reminder that key substantive issues regarding the protection of trade secrets continue to evolve and, in many instances, be hotly debated, including the types of causes of action available to enforce trade secret rights, the types of information eligible for protection, the security measures that companies are expected to take to protect their trade secrets, and the remedies available for theft and misappropriation. In light of the constantly developing nature of trade secrets law and litigation, U.S. companies should keep apprised of and scrutinize significant legislative and judicial developments in this area.

  PTCJ ISSN 0148-7965