Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

TRADE SECRETS

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

2012 Trade Secrets Litigation Round-Up




BY JASON C. SCHWARTZ,
ALEXANDER H. SOUTHWELL,
MOLLY T. SENGER, AND
SUE J. BAI

INTRODUCTION

The year 2012 saw continued expansion of trade secret law into the realm of cyberspace, with two federal courts of appeal tackling the scope of the federal Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, and numerous trial courts grappling with the application of trade secrets to social media. Both the Fourth and Ninth Circuit Courts of Appeals issued key rulings on the meaning of "authorized access" under the CFAA, while several federal district courts addressed social media questions including whether a list of MySpace "friends" or Twitter "followers" can constitute a protectable trade secret.

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

The Department of Justice also brought a number of successful criminal trade secret prosecutions this year, one of which resulted in the conviction and imprisonment of an ex-Motorola employee found to have stolen trade secrets for the benefit of a Chinese company. In another controversial criminal case under the Economic Espionage Act of 1996, 18 U.S.C. § 1832 et seq., the U.S. Court of Appeals for the Second Circuit overturned the conviction of a former Goldman Sachs employee who had been found guilty of misappropriating trade secrets related to Goldman's high-frequency trading program.

On the legislative front, 2012 saw the continued "federalization" of trade secret law. Congress passed the Theft of Trade Secrets Clarification Act (S. 3462) (85 PTCJ 303, 1/4/13) in an attempt to strengthen the government's ability to prosecute criminal trade secret theft under the EEA.

In addition, on July 17, Sen. Herbert H. Kohl (D-Wis.) introduced the Protecting American Trade Secret and

Innovation Act of 2012 (S. 3389) (84 PTCJ 459, 7/20/12), which, if passed, would provide a federal civil cause of action for trade secret misappropriation where the misappropriation is from the United States to another country, or where there is a ''substantial need for nationwide service of process.'' The bill has the potential to revolutionize civil trade secret litigation, which—until now—has been almost entirely a creature of state law.

We discuss these and other significant 2012 developments in trade secrets litigation below, first addressing civil developments and then criminal developments.

CIVIL DEVELOPMENTS

Intersection with the Computer Fraud and Abuse Act

Both the Fourth and Ninth Circuit Courts of Appeal issued significant decisions this year regarding the meaning of ''authorized access'' under the Computer Fraud and, deepening a circuit split on this issue.

The CFAA creates federal civil and criminal causes of action against, in part, 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), (g)). Because employees or others seeking to steal trade secrets often do so by accessing confidential information on the employer's or owner's computers, it is common for federal trade secret cases to include claims brought under the CFAA as well.

In order for an employee's conduct to violate the CFAA, however, the employee must not have been authorized to access his employer's computer, or he must have ''exceed[ed] authorized access.'' Two cases examined in last year's Trade Secrets Litigation Round-Up[1]—*WEC Carolina Energy* and *Nosal*—reached different conclusions as to the meaning of ''authorized access'' under the CFAA. But the Ninth Circuit has since reexamined the issue, and in an en banc decision in April, the court endorsed the interpretation of ''authorized access'' previously adopted by the federal district court in *WEC Carolina Energy*. The Ninth Circuit's en banc decision—and the Fourth Circuit's affirmance of *WEC Carolina Energy*—are both described below.

United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc). *Nosal* involved a criminal prosecution under CFAA, in which the Ninth Circuit examined whether an employee who violates his employer's policy ''prohibiting the use of work computers for nonbusiness purposes . . . . commit[s] a federal crime.'' *Id.* at 856.

David Nosal, a former employee of an executive search firm, was alleged to have violated the CFAA by enlisting several employees at the firm to assist him in obtaining confidential information from the firm's ''Searcher'' database. Nosal allegedly planned to use the information to establish his own, competing executive search firm. After he was indicted for violating the CFAA, Nosal filed a motion to dismiss, arguing that the 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 their employer's computer and information from the ''Searcher'' database.

The district court agreed with Nosal, and dismissed the charges against him under the CFAA. The Ninth Circuit, however, reversed, holding that an employee ''exceeds authorized access'' under the CFAA not only when he accesses a computer without permission, but also when he violates his employer's computer *usage* restrictions. Because all employees were subject to a formal computer usage policy, which placed restrictions on access to the Searcher database—and because the employees' use of the database to defraud the company was in violation of the company's computer usage policies—the Ninth Circuit found that the employees did, in fact, ''exceed'' their authorized access within the meaning of the CFAA when they obtained information from the database for former employee Nosal.

Nosal filed a motion for rehearing en banc, which was granted. The Ninth Circuit affirmed the district court's dismissal of the indictment, holding that ''the phrase 'exceeds authorized access' in the CFAA does not extend to violations of [employer computer] use restrictions.'' *Id.* at 863. A contrary interpretation of the CFAA, the court explained, ''would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer.'' *Id.* at 859. For example, ''minor dalliances'' such as ''g-chatting with friends, playing games, shopping or watching sports highlights'' on an employer's computer would—if prohibited by the employer's computer usage policies—constitute federal crimes. *See id.* at 860. Refusing to countenance such a result, the Ninth Circuit declared that ''[i]f Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly.'' *Id.* at 863.

The Justice Department decided not to seek certiorari in *Nosal*, so the en banc decision now deepens the split of authority concerning the interpretation of the CFAA's acting ''without authorization'' language in the disloyal employee context. That split is between the ''narrow'' approach—that the CFAA applies only when an employee improperly accesses, not just improperly uses, information (which has been followed by the Fourth Circuit and district courts within the Second Circuit in addition to the Ninth Circuit after the *Nosal* en banc decision), and the ''broad'' approach—that an employee acts without authorization when the employee acquires an interest adverse to his or her employer or breaches a duty of loyalty to the employer (which has been adopted by the Fifth, Seventh, and Eleventh circuits).

WEC Carolina Energy Solutions L.L.C. v. Miller, 687 F.3d 199 (4th Cir. 2012). The Fourth Circuit in *WEC Carolina Energy* reached the same conclusion as the Ninth Circuit in its *en banc* decision in *Nosal* that ''authorized access'' under the CFAA should be narrowly interpreted.

The case involved a suit by WEC Carolina Energy Solutions L.L.C. against its former employee, Willie Miller, and his assistant, Emily Kelley. According to WEC, Miller and Kelley downloaded WEC's confidential and proprietary documents and emailed them to Miller's personal email account shortly before Miller resigned from WEC to work for WEC's competitor, Arc Energy Services Inc. Miller allegedly then used the stolen infor-

[1] *See* Jason C. Schwartz, Alexander H. Southwell, and Molly T. Senger, ''2011 Trade Secret Litigation Round-Up'' (83 PTCJ 339, 1/13/12).

   ISSN 0148-7965

mation in a presentation to a potential customer, who chose to do business with Arc over WEC. Among other claims, WEC alleged that Miller and Kelley had violated the CFAA when they accessed WEC's computers to send Miller the confidential WEC documents. The district court, however, dismissed the CFAA claim, on the ground that Miller and Kelley did not act ''without authorization'' or ''exceed authorized access'' within the meaning of the CFAA.

The Fourth Circuit affirmed. The court explained that there are currently ''two schools of thought'' regarding the meaning of authorized access under the CFAA. *Id.* at 203. The first—which has been adopted by the Seventh Circuit, and which had been endorsed by the Ninth Circuit's now superseded panel decision in *Nosal*—''holds that when an employee accesses a computer or information on a computer to further interests that are adverse to his employer . . . [, he] los[es] any authority he has to access the computer or any information on it.'' *Id.* (citing *International Airport Centers L.L.C. v. Citrin*, 400 F.3d 418, 420-21 (7th Cir. 2006)). The second—set forth in the *Nosal*en banc decision—''interprets 'without authorization' and 'exceeds authorized access' literally and narrowly, limiting the terms' application to situations where an individual accesses a computer or information on a computer without permission.'' *Id.*

Adopting the latter interpretation, the Fourth Circuit held that the terms ''without authorization'' and ''exceeds authorized access'' ''apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access.'' *Id.* at 206. Because Miller and Kelley only violated WEC's computer *use* restrictions—but were authorized to *access* the computers at issue—the court found that they did not access a computer without authorization or exceed their authorized access. *Id.* at 206-07.[2]

Social Media and Trade Secrets

The rising use of social media for both business and personal purposes has had a significant impact on employment law and trade secret issues arising in the employment context over the past year. In 2012, six states—Maryland, Delaware, Illinois, Michigan, New Jersey, and California—passed legislation prohibiting employers from requesting or requiring that employees or prospective employees provide them with access to their personal social media accounts. (*See* National Conference of State Legislatures, *Employer Access to Social Media Usernames and Passwords* (Dec. 28, 2012), *available at* http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx (last visited Dec. 31, 2012)). Many employers, however, continue to maintain that such access is necessary to protect their trade secrets. *See id.*

And even when employers lack access to their employees' personal social media accounts, disputes often arise as to the ownership of those accounts—and their associated ''followers'' or ''subscribers''—when the accounts are used for business purposes.

PhoneDog L.L.C. v. Kravitz, No. 3:11-CV-03474, 2012 BL 27330 (N.D. Cal. Jan. 30, 2012). A federal district court in California was recently presented with the question of whether information contained in an employee's Twitter account, such as a list of subscribers, constitutes a trade secret belonging to his former employer.

PhoneDog is a company that provides reviews for mobile products and services and allows users to research and compare such products. As part of his employment with PhoneDog, Noah Kravitz created a Twitter account with the handle @PhoneDog_Noah. Kravitz accessed the account using his password, and promoted PhoneDog's services through his account. The company alleged that during Kravitz's employment, the account generated approximately 17,000 followers. When Kravitz ended his employment with PhoneDog, the company requested that he relinquish his Twitter account. Kravitz, however, simply changed his handle to @noahkravitz and continued to use the account. *PhoneDog*, 2011 BL 290583 at *1 (N.D. Cal. Nov. 8, 2011).

PhoneDog brought suit against Kravitz for trade secret misappropriation, among other claims. Before the court could reach the merits of the misappropriation claim, the parties settled out of court. Although the precise terms of the settlement remain undisclosed, Kravitz has been permitted to maintain sole custody of the Twitter account.[3]

Christou v. Beatport, 849 F. Supp. 2d 1055 (D. Colo. 2012). A recent decision from the U.S. District Court for the District of Colorado provides additional guidance on whether social media contacts can constitute protectable trade secrets.

Regas Christou, the founder of several nightclubs in the Denver area, sued Beatport and its founder, Bradley Roulier, who was formerly Christou's employee, alleging that after Roulier founded his own competing nightclub in Denver, Roulier misappropriated from Christou ''login information for profiles on MySpace, lists of MySpace 'friends,' confidential lists of personal cell phone numbers and email addresses for DJs, agents, and promoters, and customer lists.'' *Id.* at 1074.

In denying Beatport's motion to dismiss, the court rejected Roulier's claim that Christou's MySpace profile and ''friends'' list did not constitute trade secrets. *Id.* at 1076. Addressing this issue of first impression, the court relied on an eight-factor test outlined by the Tenth Circuit. *Id.* at 1075. According to the court, Christou had taken reasonable steps to maintain the secrecy of the information on his MySpace profile and to restrict access to the same. Critically, the court found that Christou's list of ''friends'' was not publicly-available because the alleged ''trade secret is not merely the list of names but [the friends'] email and contact information as well as the ability to notify them and promote directly to them via their MySpace accounts.'' *Id.* at 1076. The court noted that while Roulier could ''likely duplicate or nearly duplicate the list of MySpace friends'' that Christou had developed, ''this would involve individually contacting thousands of individuals with friend requests, and it is by no means clear that all of those individuals would grant Beatport permission to contact them.'' *Id.* For all these reasons, the court found that Christou had alleged sufficient facts to withstand Beatport's motion to dismiss his claim that his MySpace friends list was a trade secret.

[2] On Oct. 24, WEC filed a petition for writ of certiorari with the Supreme Court. As of the date of publication of this article, that petition had not yet been ruled on.

[3] *See* Chris Taylor, ''Writer Sued for his Twitter Followers Settles Case,'' *Mashable* (Dec. 3, 2012), *available at* http://mashable.com/2012/12/03/noah-kravitz-lawsuit-twitter/ (last visited Jan. 7, 2013).

Eagle v. Morgan, No. 2:11-CV-04303, 2012 BL 260238 (E.D. Pa. Oct. 4, 2012). Just as the rising use of Twitter and MySpace for business purposes has sparked litigation between employees and employers over the ownership of ''followers'' and ''friend lists,'' so too, has employees' use of LinkedIn resulted in litigation over the ownership of professional contacts.

Linda Eagle was the founder and president of Edcomm, a banking education company. While she was president, she established an account on LinkedIn—a social networking website for professionals. Eagle used her account ''to promote Edcomm's banking education services, foster her reputation as a businesswoman, reconnect with family, friends, and colleagues; and build social and professional relationships.'' *Id.* at *1. Edcomm recommended that all employees participate in LinkedIn and list Edcomm as their current employer. Edcomm's practice when employees left the company was to ''mine'' their former employees' LinkedIn pages for information and to monitor the pages' traffic. *Id.*

After Eagle was terminated from her position in June 2011, Edcomm accessed her LinkedIn account and changed the password so Eagle could no longer access it. Then, the company replaced Eagle's name and photo with that of the company's interim chief executive officer. Eagle brought suit against Edcomm and several of its employees, alleging violations of the CFAA, the Lanham Act, and a number of state law claims, including claims for invasion of privacy by misappropriation of identity, and misappropriation of publicity. *Id.* at *5.

The court granted Edcomm's motion for summary judgment on the CFAA claim, on the ground that Eagle had failed to demonstrate any legally cognizable damages resulting from her inability to access her LinkedIn account. The court additionally found that Edcomm's use of Eagle's LinkedIn account did not cause ''a likelihood of confusion,'' as required to establish a viable claim under the Lanham Act. *Id.* at *7. A bench trial was held on the remaining state law claims, but no opinion had been issued as of the date of publication of this article. The outcome, however, may be an important development as to whether social media accounts and relationships can be owned, misappropriated, and converted.

Importance of Proactive Measures to Protect Trade Secrets

Courts this year have repeatedly emphasized that companies must take proactive security measures to keep their information confidential in order for that information to qualify as a protectable trade secret.

Fail-Safe L.L.C. v. A.O. Smith Corp., 674 F.3d 889 (7th Cir. 2012). A recent case from the Seventh Circuit highlights how a company's failure to protect its confidential information in the course of external business negotiations can defeat subsequent attempts to claim that information is a trade secret.

Fail-Safe involved an anti-entrapment swimming pool pump created by Fail-Safe L.L.C.. Fail-Safe began to negotiate with A.O. Smith regarding its right to market and sell the pump. During the negotiations, Fail-Safe signed A.O. Smith's standard one-way confidentiality agreement, but did not request that A.O. Smith sign a similar agreement—even though Fail-Safe's general practice was to require execution of confidentiality agreements. Fail-Safe subsequently shared details about its anti-entrapment pump with A.O. Smith without a confidentiality agreement in place. *Id.* at 891. When negotiations between the two companies broke down, A.O. Smith began to market two of its own pump motors. Fail-Safe responded by suing A.O. Smith for trade secret misappropriation and unjust enrichment under Wisconsin law. *Id.* at 892.

The district court granted summary judgment in favor of A.O. Smith on both counts. The court not only found that Fail-Safe's trade secret misappropriation claim was barred by the applicable three-year statute of limitations, but also held that the claim failed on the merits, since the company had not taken ''reasonable steps to protect the secrecy of its claimed trade secret.'' *Id.* Fail-Safe's unjust enrichment claim similarly failed as a result of the company's ''voluntary disclosure'' of the information. *Id.*

The Seventh Circuit affirmed. Without addressing the statute of limitations issue, the court emphasized that Fail-Safe's failure to take ''*any* steps to protect its information'' was ''not reasonable under these circumstances.'' *Id.* at 893 (emphasis in original). Although it acknowledged that smaller companies may be ''held to a looser standard'' in terms of the steps that must be taken to protect their trade secrets, the Seventh Circuit deemed this an ''extreme case,'' in which Fail-Safe's complete lack of precautionary measures was fatal to its trade secret misappropriation claim. *Id.* at 894. As the court explained, ''[i]f the information . . . provided was confidential, then [Fail-Safe] should have requested reciprocal confidentiality in its communications and exchanges with [A.O. Smith].'' *Id.* Fail-Safe's unjust enrichment claim similarly failed, the court explained, since A.O. Smith could not profit unjustly from information that Fail-Safe had willingly volunteered. *Id.*

FormFactor Inc. v. Micro-Probe Inc., No. C-10-3095-PJH, 2012 BL 159474 (N.D. Cal. June 7, 2012) (84 PTCJ 268, 6/15/12). A recent California case illustrates the need for companies to institute internal security measures to protect their trade secrets.

FormFactor involved two companies competing in the production of ''advanced wafer probe card assemblies,'' which are used to test semiconductor wafers. FormFactor brought suit against its competitor, Micro-Probe, alleging trade secret misappropriation, among other claims. *Id.* at *4. According to FormFactor, Micro-Probe had hired ''current and former FormFactor employees . . . for the express purpose of having them disclose FormFactor's confidential technical and marketing information.'' *Id.* at *1.

The court, however, granted Micro-Probe's motion for summary judgment on the trade secret misappropriation claim. As the court explained, there had been ''no evidence that FormFactor made reasonable efforts to protect the secrecy of any particular trade secret.'' *Id.* at 7. Rather, the evidence demonstrated that FormFactor ''did not enter into a written agreement with its former employee to protect its trade secret,'' and that ''it did not request that [the employee] return any FormFactor data when he tendered his resignation and left the company.'' *Id.* In addition, the company had ''allowed/authorized [employees] to work from home,'' to use personal email for business purposes, and to back-up business data on external hard drives. *Id.*

Given the company's failure to implement protective measures to safeguard its alleged trade secrets, FormFactor could not claim that its supposedly confidential information rose to the level of a protectable trade se-

   ISSN 0148-7965

cret. *See id.* The court further noted that FormFactor had failed to sufficiently identify with particularity the nature of its trade secrets that were allegedly misappropriated, as required under California law. *See id.* at *6.

Early Identification of Trade Secrets with Particularity

California is not alone is requiring plaintiffs to identify allegedly misappropriated trade secrets with particularity at an early stage in litigation. And this requirement often poses complex challenges for companies contemplating trade secret misappropriation claims, as they must balance the benefit of filing suit against the cost of disclosing the subject matter of their alleged trade secrets to a competitor (albeit usually under a court protective order).

MSCI Inc. v. Jacob, 945 N.Y.S.2d 863 (N.Y. Sup. Ct. 2012). *MSCI* arose from a trade secret misappropriation claim filed by MSCI, a computer software company, against its former employee and his new employer, Axioma. *Id.* at 864. Following a discovery conference, the New York trial court held that MSCI was required to ''identify [its] trade secrets with reasonable particularity early in the case.'' *Id.* at 865. MSCI responded by identifying the aspects of its computer source code that were covered by third-party licenses or in the public domain—that is, ''by identifying those aspects *not* claimed to be trade secrets.'' *Id.* at 864 (emphasis in original).

Rejecting this approach, the court explained that MSCI's ''disclosure does not enlighten either defendants or the court as to what sequencing of publicly known components or licensed components, are trade secrets.'' *Id.* at 866. Moreover, allowing MSCI to proceed with discovery of the defendants' source code without identifying its own trade secrets would be unfair, said the court, because MSCI then ''could tailor their theory of misappropriation to Axioma's work,'' and in so doing, could misappropriate Axioma's trade secrets. *See id.*

Switch Communications Group v. Ballard, No. 2:11-cv-00285 (D. Nev. June 19, 2012). The U.S. District Court for the District of Nevada recently had occasion to examine the justification for the requirement that plaintiffs describe their alleged trade secrets with reasonable particularity.

The case involved Switch Communications—a company that owns and operates computer data centers located in the Las Vegas area. Switch sued its former chief financial officer, alleging that he was ''planning to build a competing data center'' near Switch's three data centers. According to Switch, its former CFO had become aware of the company's trade secrets during his employment, ''including the location of Plaintiffs' carrier fiber and the structure of the related carrier fiber agreements, the location of Switch's key clients' installations, the terms of Switch's agreements with those key clients . . . , and the design and operation of Switch's data center facilities.'' *Id.* at *1. The former CFO purportedly persuaded key contractors for a new, competing data center to participate in his project by using ''technical drawings and schematics that were either identical or materially similar to those owned by Switch and utilized to construct the Switch data centers.'' *Id.*

Citing case law from eight states, the court applied the ''reasonable particularity'' requirement to assess Switch's trade secret misappropriation claim. Although Switch had generally identified ''various concepts, elements or components'' that made up its data center facilities, the court held that the company needed to ''specifically describe what particular combination of components renders each of its designs novel or unique, how the components are combined, and how they operate in unique combination.'' *Id.* at *5.

The court went on to list several policies that ''underlie this requirement,'' noting that the requirement is necessary to prevent ''fishing expeditions'' by trade secret plaintiffs; to ensure that information requested by plaintiffs in discovery is truly relevant; to provide adequate notice to defendants of the allegations against them; and to prevent plaintiffs from molding their causes of action to the discovery received. *See id.* at *4.

''Use'' of Trade Secrets

Although it is often difficult for a plaintiff to establish the *existence* of a trade secret—and specify that trade secret with the requisite level of particularity—a recent decision by the Fifth Circuit suggests that the showing required to establish a defendant's *use* of a claimed trade secret may be quite low.

Bohnsack v. Varco L.P., 668 F.3d 262 (5th Cir. 2012) (83 PTCJ 434, 2/3/12). In *Bohnsack*, the Fifth Circuit held that filing a patent application for another person's invention may constitute ''use'' of a trade secret, giving rise to liability for trade secret misappropriation—even when no patent for the invention is ever issued.

Bohnsack involved a machine known as ''the Pit Bull,'' which was used to clean drilling fluids. The inventor of the Pit Bull, Clyde Bohnsack, negotiated with Varco, a company that cleans drilling fluids, regarding the right to manufacture the machine. *Id.* at 262. After Bohnsack expressed interest in filing a patent application for the Pit Bull, Varco initiated the application process through its outside counsel, Guy McClung. *Id.* at 268.

McClung drafted the patent application and stated on the application that he was a co-inventor of the Pit Bull, because he ''had added ideas to the drawing.'' *Id.* At Varco's request, Bohnsack signed a declaration to the patent application stating that both he and McClung were inventors of the Pit Bull. *Id.* However, shortly after signing the declaration, Bohnsack emailed McClung to tell him that he did not understand why McClung had been listed as a co-inventor. McClung responded that Bohnsack should seek legal counsel and that he would not file the declaration to the patent application until ''we have sorted this all out.'' *Id.* at 268-69. Despite his representation to the contrary, McClung then proceeded to file the patent application and accompanying declaration without resolving his dispute with Bohnsack. *Id.* at 269. Bohnsack's negotiations with Varco subsequently broke down, and no patent for the Pit Bull was ever issued. *Id.* at 271. Varco ultimately assigned its rights in the Pit Bill to Bohnsack, and brought a declaratory judgment action, seeking a determination that it was not liable for any wrongdoing. Bohnsack counterclaimed for fraud and trade secrets misappropriation.

The jury found for Bohnsack on the trade secrets misappropriation claim, awarding him $600,000 in compensatory damages. *Id.* at 272. On appeal, the Fifth Circuit affirmed. The court explained that in order to prevail on a trade secret misappropriation claim under Texas law, the plaintiff must prove ''(1) existence of a trade secret; (2) breach of a confidential relationship or

improper discovery of a trade secret; (3) use of the trade secret; and (4) damages.'' *Id.* at 279. According to Varco, Bohnsack had failed to prove either (3) or (4)—*i.e.*, Varco's use of the trade secret or damages.

Rejecting this argument, the court explained that ''[a]ny exploitation of [a] trade secret that is likely to result in injury to the trade secret owner or enrichment to the defendant'' constitutes a ''use'' of that trade secret. *Id.* (quoting *General Universal Systems Inc. v. HAL Inc.*, 500 F.3d 444, 450 n.4, 84 U.S.P.Q.2d 1436 (5th Cir. 2007) (74 PTCJ 698, 10/12/07)). The court went on to find that ''[u]nder this broad definition of 'use,' a reasonable jury had sufficient evidence to conclude that Varco exploited Bohnsack's idea for the Pit Bull'' by filing a patent application for the invention. *Id.* The patent, if granted, would have caused Varco's competitors to ''become significantly less interested in compensating Bohnsack for the use of the Pit Bull,'' since Varco would stand to receive a share of the profits from all uses of the Pit Bull once a patent was issued. *Id.* at 280. In this manner, Varco's filing of the patent application was likely to reduce the market value of Bohnsack's invention—i.e., it was an ''exploitation . . . likely to result in injury to the trade secret owner.'' *See id.*

The court likewise rejected Varco's argument that Bohnsack had failed to present ''evidence of damages caused by Varco's use of the Pit Bull.'' *Id.* As the court explained, damages may be measured not only by profits lost as a result of trade secret misappropriation, but also by the ''value a reasonably prudent investor would pay for the trade secret.'' *Id.* Because Varco, during its negotiations with Bohnsack, had been willing to pay at least $600,000 for the right to use the Pit Bill, the court affirmed the award of $600,000 in compensatory damages to Bohnsack.

Remedies

Not only did this year bear witness to several significant trade secret damages awards—such as the $22 million verdict against Best Buy in *TechForward v. Best Buy Co.* described below—but it was also notable for the injunctions that were entered against companies found liable for trade secret misappropriation, including the sweeping, worldwide injunction against Kolon Industries Inc.

E.I. DuPont de Nemours Co. v. Kolon Industries Inc., No. 09-cv-00058, 2012 BL 221919 (E.D. Va. Aug. 30, 2012); No. 12-1260 (4th Cir. Sept. 21, 2012). Last year, a federal jury found that Kolon had misappropriated trade secrets relating to the manufacture of Kevlar—a para-aramid fiber used to make protective body gear—and awarded E.I. DuPont de Nemours and Co. $920 million in damages.

This year, the court entered a 20-year, worldwide injunction barring the South Korean company from manufacturing Heracron, the synthetic fiber that Kolon allegedly made with the trade secrets that it misappropriated from DuPont. In granting the sweeping injunction, the court found that the Supreme Court's decision in *eBay Inc v. MercExchange L.L.C.*, 547 U.S. 388, 78 U.S.P.Q.2d 1577 (2006) (72 PTCJ 50, 5/19/06), which required a finding of irreparable injury for a permanent injunction in a post-trial proceeding involving a patent, was inapplicable to permanent injunctions requested under state law. *Id.* at 3, 5, 10. Accordingly, the court held that DuPont need not prove irreparable harm or that there were inadequate remedies at law in order to be entitled to the injunction; rather, a permanent injunction could be entered under Virginia's Uniform Trade Secrets Act, the court found, because the harm suffered in the absence of an injunction outweighed the harm suffered by Kolon as a result of the injunction. *Id.* at 12, 14.

Notably, this decision was based on an interpretation of the Uniform Trade Secrets Act, which has been adopted by 47 states. The decision thus has the potential to open the door to permanent injunctions in other cases, even when substantial damages are awarded. *See id.* at 12. The Fourth Circuit has, however, granted Kolon's motion to stay enforcement of the injunction.

In October, the Department of Justice announced the unsealing of an indictment against Kolon and five of its executives, seeking the forfeiture of at least $225 million from Kolon's alleged theft of DuPont's Kevlar-related trade secrets. The $225 million allegedly represents the approximate gross proceeds that Kolon derived from its sale of Heracron from January 2006 through June 2012, plus the amount that Kolon allegedly paid former DuPont employees for access to DuPont's trade secrets. Kolon has been charged with one count of conspiracy to convert trade secrets, four counts of trade secret theft, and one count of obstruction of justice.[4]

Skycam L.L.C. v. Bennett, No. 09-cv-00294, 2012 BL 252198 (N.D. Okla. Sept. 30, 2012) (84 PTCJ 1002, 10/12/12). While some courts have found broad permanent injunctions to be the necessary and appropriate remedy for trade secrets misappropriation, other courts trying to balance the interest in protecting trade secrets with the need to maintain industry competition have turned to royalty injunctions as an alternative remedy.

The suit between Skycam and Actioncam—two competitors in the aerial camera industry—arose when Patrick Bennett, Skycam's chief engineer, left the company to join Actioncam. According to Skycam, Bennett had full access to Skycam's engineering and design documents for its aerial camera system, which is used in the broadcast of sporting events where cameras are suspended by cables over the playing field. Skycam alleged that Actioncam developed a competitive aerial camera system with the help of Bennett, using Skycam's trade secrets. Skycam sued Bennett, alleging breach of his non-disclosure agreement, trade secrets misappropriation, and unfair competition. After the jury found in favor of Skycam on all three claims and awarded $594,000 in damages, including $75,000 in punitive damages, Skycam sought to enjoin Actioncam from using Skycam's trade secrets. *Id.* at *1.

Although the court concluded that injunctive relief was appropriate for the trade secrets misappropriation claim, it found that a prohibitory injunction would put Actioncam out of business, thus eliminating competition and technological innovation in the aerial camera market, which already had relatively few competitors. The court therefore decided to award a royalty injunction to Skycam instead, in the amount of $5,000 per event during the covered period. *Id.* at *3.

TechForward v. Best Buy Co., No. 2:11-cv-01313 (C.D. Cal.). A California jury this year returned a $22 million

[4] DOJ Press Release, *Top Executives at Kolon Industries Indicted for Stealing DuPont's Kevlar Trade Secrets* (Oct. 18, 2012), *available at* http://www.justice.gov/opa/pr/2012/October/12-crm-1257.html (last visited January 7, 2013).

   ISSN 0148-7965

verdict against the electronics retail chain Best Buy, based on Best Buy's misappropriation of trade secrets relating to TechForward's Guaranteed Buyback Plan. Because the jury determined that Best Buy's conduct was willful and malicious, the court also ordered Best Buy to pay an additional $5 million in punitive damages.

Under the Guaranteed Buyback Plan, retail customers pay for the right to redeem newly-purchased electronic devices at a future date in exchange for a store credit that is a percentage of the purchase price. TechForward alleged that, while negotiating with Best Buy regarding a potential pilot program for the Guaranteed Buyback Plan in Best Buy stores in the Los Angeles area, it shared highly confidential information regarding the Plan. When the pilot program fell through, the jury found that Best Buy then used the confidential information that it had obtained from TechForward to introduce its own buyback program in February 2011.

Hallmark Cards Inc. v. Monitor Clipper Partners L.L.C., No. 4:08-cv-00840 (W.D. Mo.). Hallmark Cards this year won a $31.3 million verdict against a Massachusetts-based private equity firm for the misappropriation of the card company's trade secrets. The jury award included $21.3 million in actual damages and $10 million in punitive damages.

Monitor Company Group, a consulting company related to the defendant private equity firm, helped Hallmark redesign its business model, and allegedly divulged the card company's confidential proprietary information to Monitor Clipper, which shares a headquarters, support systems, and administrative functions with Monitor Company Group. According to Hallmark, Monitor Clipper then went on to use its trade secrets and confidential information to facilitate its purchase of Hallmark's competitor, Recycled Paper Greetings, in 2005.

Management and Engineering Technologies International v. Information Systems Support Inc., No. 10-17784, 2012 BL 184079 (9th Cir. July 23, 2012). The Ninth Circuit recently reversed a damages award in a case involving trade secret theft by Information Systems Support Inc. The plaintiff, Management and Engineering Technologies International, alleged that its former employee, Ross Romeo, had downloaded METI's confidential documents before leaving the company, and then used the information in a presentation to ISS, which, in turn, used the information for strategic planning. *Id.* at 1.

Although the court held that sufficient evidence supported the jury's decision to award METI royalty damages, it concluded that the evidence did not support the amount of damages awarded. *Id.* at 2. The jury's damage award had been based on METI's successful trade secret misappropriation claim, but METI had raised a number of other trade secret claims that failed as a matter of law. For example, METI's employee roster and METI's ranking by Carnegie Mellon's Capable Maturity Model Integration program were found not to have been trade secrets because they were publicly-known. *Id.* Yet the expert at trial had only testified to the hypothetical negotiated price that ISS would have paid for *all* of the information alleged to be trade secret—and did not break down the hypothetical price for each of the alleged trade secrets at issue. Accordingly, the Ninth Circuit vacated the jury's damage award and remanded the case to the district court. *Id.* at 3.

CRIMINAL DEVELOPMENTS

Companies facing trade secret misappropriation often consider criminal referrals as an important option, and there have been a number of significant criminal developments in the trade secret arena this year. Significantly, a 2012 report on the Economic Espionage Act (EEA) found that in more than 90 percent of prosecutions under the act, ''the defendant was an 'insider,' and had access to the trade secret because he was an employee of the victim, or worked for a vendor or contractor of the victim.'' *See* Peter Toren, ''A Report on Prosecutions Under the Economic Espionage Act,'' *Trade Secret Law Summit, AIPLA Annual Meeting* (Oct. 23, 2012).

That was certainly the case in *United States v. Aleynikov*—arguably the most significant EEA decision of the year. There, the Second Circuit reversed the conviction of a former Goldman Sachs computer programmer, who had been found guilty of stealing source code for Goldman Sachs's high-frequency trading program. The defendant had been charged with violating 18 U.S.C. § 1832 of the EEA, which criminalizes the theft of trade secrets ''produced for'' or ''placed in'' interstate or foreign commerce.

After the Second Circuit held that the source code for Goldman's high-frequency trading program did not fall within this definition—because it was not ''produced for'' or ''placed in'' interstate commerce, as Goldman had no intention of selling the program—Congress responded by enacting the Theft of Trade Secrets Clarification Act, which amends the EEA to make clear that the theft of all products ''used in'' interstate or foreign commerce fall within the purview of the act (85 PTCJ 303, 1/4/13).

Aleynikov and other significant 2012 criminal prosecutions and convictions are discussed below.

United States v. Li, No. 3:12-CR-00034 (D.N.J.). On Jan. 17, Yuan Li pled guilty to one count of trade secrets theft for stealing information regarding chemical compounds developed by her former employer, Sanofi Aventis—a French pharmaceutical company.

From 2006 to 2011, Li worked as a research scientist in the U.S. headquarters of Sanofi, located in Bridgewater, New Jersey. Li admitted that from January 2010 to June 2011, she downloaded confidential data on Sanofi's chemical compounds, which had not yet been disclosed to the public, and transferred the information to her home computer using her personal email or a USB flash drive.

Li later attempted to sell Sanofi's proprietary chemical compounds on the website of a company known as Abby Pharmatech Inc., which was the U.S. unit of a Chinese company, Xiamon KAK Science & Technology Co. Li was a 50 percent owner of Abby Pharmatech. On May 7, Li was sentenced to eighteen months' imprisonment and two years of supervised release, and ordered to pay $131,000 in restitution.

United States v. Jin, 833 F. Supp. 2d 977 (N.D. Ill. 2012) (83 PTCJ 531, 2/17/12). On Feb. 8, the U.S. District Court for the Northern District of Illinois found Hanjuan Jin, an ex-Motorola Inc. software engineer, guilty of three counts of trade secret theft under 18 U.S.C. § 1832.

As the court explained in its 77-page memorandum opinion and order, Jin had been detained at Chicago's O'Hare International Airport in February 2007 while attempting to board a flight to China, after a security offi-

cer conducting a random screening found that she was carrying more than $30,000 in cash, and a number of Motorola documents marked as ''confidential and proprietary.'' *Id.* at 985-86. According to the court, ''when Jin was stopped with the documents . . . she had planned to move to China for an indefinite duration and work for Sun Kaisens,'' and she believed that ''the documents she took from Motorola—including the trade secrets—would help her prepare for her future employment at Sun Kaisens.'' *Id.* at 1016-17.

Although the court found Jin guilty of trade secret theft, it found that the government had failed to prove beyond a reasonable doubt that Jin violated 28 U.S.C. § 1831(a)(3)—the foreign economic espionage provision of the EEA. In order to be guilty of foreign economic espionage, Jin must have intended or known that her conduct would benefit a foreign government or instrumentality. *See id.* at 1019.

The government maintained that Jin ''knew her conduct would benefit the [People's Republic of China] because Sun Kaisens develops telecommunications technology for the Chinese military,'' and the trade secrets that Jin stole ''pertained to telecommunications technology.'' *Id.* Rejecting this argument, the court explained that there had been ''minimal evidence of a connection'' between the stolen trade secrets and the Chinese military. *See id.* at 1020.

On August 29, Jin was sentenced to four years in prison and fined $20,000.

Jin was also named as a defendant in a related civil suit by Motorola against Lemko Corp. and 14 individuals, alleging trade secret misappropriation and other claims. *See Motorola Inc. v. Lemko Corp.*, No. 08 C 5427, 2012 BL 5305 (N.D. Ill. Jan. 10, 2012) (83 PTCJ 379, 1/20/12). Lemko and nine of the individual defendants (though not Jin) moved for summary judgment on the trade secret misappropriation claim, arguing that Motorola failed to set forth its trade secrets with the required specificity, and that Motorola failed to take reasonable efforts to maintain the secrecy of the information that it alleged to be trade secret.

Rejecting these arguments, the court found that Motorola had, in fact, identified its trade secrets with the requisite level of particularity by referencing ''particular documents, files, inventions, and aspects of its technology,'' as opposed to ''general methods or areas of its business.'' *Id.* at *17. The court also concluded that ''[a] reasonable jury could find . . . the information . . . was the subject of reasonable efforts by Motorola to keep it a secret.'' *Id.* at *19. Accordingly, the defendants' motion for summary judgment on the trade secret misappropriation claim was denied. *See id.* at *20.

Nevertheless, shortly after the court issued its decision, Motorola and Lemko reached a settlement,[5] and Motorola voluntarily stipulated to the dismissal of all of its claims with prejudice—including its claims against Jin.

United States v. Aleynikov, No. 1:10-CR-00096 (S.D.N.Y.); 676 F.3d 71 (2d Cir. 2012) (83 PTCJ 910, 4/20/12). On Apr. 11, the Second Circuit reversed the conviction of Sergey Aleynikov, a former computer programmer for Goldman Sachs Group Inc., who had been found guilty of stealing computer source code for Goldman's high-frequency trading program in violation of the National Stolen Property Act of 1961 and the EEA.

The NSPA makes it a crime to ''transport[], transmit[], or transfer[] in interstate or foreign commerce any goods, wares, merchandise, securities or money . . . knowing the same to have been stolen, converted or taken by fraud,'' while the EEA prohibits the theft of trade secrets that are ''related to or included in a product that is produced for or placed in interstate or foreign commerce.'' *Id.* at 74. On appeal, Aleynikov argued that Goldman's computer source code was not a ''good'' within the meaning of the NSPA, and that it was not ''related to or included in a product that is produced for or placed in interstate or foreign commerce,'' as required by the EEA. *Id.* at 73. The Second Circuit agreed on both counts. *Id.*

With respect to the NSPA, the court explained that ''the theft and subsequent interstate transmission of purely intangible property is beyond the scope of the NSPA.'' *Id.* at 77. Because Aleynikov had uploaded Goldman's source code to a server in Germany—and did not ''physically seize[] anything tangible from Goldman, such as a compact disc or thumb drive''—the court found that Aleynikov had not violated the NSPA. While acknowledging that in almost every case involving source code, ''the value of the intangible code will vastly exceed the value of any physical item on which it might be stored,'' the court declined to ''stretch or update statutory words of plain and ordinary meaning [contained in the NSPA] to better accommodate the digital age.'' *Id.* at 79.

The court went on to find that Aleynikov's indictment under the EEA was also insufficient as a matter of law. *Id.* at 79. Aleynikov had been charged with violating 18 U.S.C. § 1832, which criminalizes the theft of trade secrets ''produced for'' or ''placed in'' interstate or foreign commerce. According to the Second Circuit, Goldman's HFT program was not ''produced for'' or ''placed in'' interstate commerce, as Goldman ''had no intention of selling its HFT system or licensing it to anyone.'' *Id.* at 82. Because the HFT program was ''not designed to enter or pass in commerce, or to make something that does,'' the court found that Aleynikov's theft of the computer source code for the HFT program ''was not an offense under the EEA.'' *Id.*

In a concurring opinion, Judge Calabresi wrote that Congress probably intended to criminalize this type of conduct and expressed the ''hope that Congress will return to the issue and state, in appropriate language, what I believe they meant to make criminal in the EEA.'' *Id.* at 83.

Congress took note of this judicial expression of hope in passing the Theft of Trade Secrets Clarification Act of 2012 (85 PTCJ 271, 12/21/12), which took effect in December, and limited the effect of the *Aleynikov* decision by striking the requirement in 18 U.S.C. § 1832(a) that the trade secret at issue be ''produced for'' or ''placed in'' interstate commerce. Under the Act, the trade secret need only be ''a product or service used in or intended for use in'' interstate commerce.

As to Aleynikov himself, after the reversal of his conviction by the Second Circuit, he was arrested and arraigned on state felony charges in the New York County Criminal Court (84 PTCJ 675, 8/17/12). Aleynikov entered a plea of not guilty in September to charges of un-

[5] *See* Press Release, ''Motorola Solutions, Lemko Corp. Jointly Announce Settlement of All Pending Litigation,'' *Reuters* (Jan. 31, 2012), *available at* http://www.reuters.com/article/2012/01/31/idUS249191+31-Jan-2012+BW20120131 (last visited Jan. 9, 2013).

   ISSN 0148-7965

lawful use of secret scientific material and unlawful duplication of computer related material.

Aleynikov also initiated a federal action against Goldman in the U.S. District Court for the District of New Jersey, seeking indemnification for the attorneys' fees and expenses that he incurred in the federal criminal action, and an advancement of the attorneys' fees and expenses that he is incurring in the state criminal proceedings. *See Aleynikov v. The Goldman Sachs Group Inc.*, No. 2:12-cv-05994-KM-MAH (D.N.J. filed Sept. 25, 2012). Both the state prosecution of Aleynikov and the federal action against Goldman remain pending.

United States v. Zhang, No. 5:05-CR-00812 (N.D. Cal.). On May 7, after a two-week bench trial, the U.S. District Court for the Northern District of California found Suibin Zhang guilty of three counts of computer fraud under the CFAA, three counts of trade secret theft, one count of unauthorized transmission of trade secrets, and one count of unauthorized possession of stolen trade secrets.

Evidence at trial showed that while Zhang was a project engineer at Netgear Inc., he had access to the secure database of Marvell Semiconductor Inc.—a supplier of semiconductor chips to Netgear. After accepting a position at Marvell's chief competitor, Broadcom Corp., Zhang used his Netgear account to download Marvell's trade secrets onto a laptop that had been provided to him by his new employer, Broadcom. Zhang faces a maximum statutory penalty of ten years' imprisonment and $250,000 in fines, as well as restitution. Zhang's sentencing is currently scheduled for February 2013.

United States v. Mohapatra, No. 1:11-CR-00132 (D. Utah). On May 11, Prabhu Mohapatra entered a plea of guilty to one count of unlawful access to a protected computer in exchange for prosecutors dismissing twenty-five other charges against him. Mohapatra admitted that while he worked as a senior scientist at Frontier Scientific Inc. from October 2009 until November 2011, he accessed the company's chemical resource notebook, copied the formula for meso-Tetraphenylporphine, and emailed the information to his brother-in-law, who was setting up a competing pharmaceutical company in India. Mohapatra faces up to five years' imprisonment, a fine of up to $250,000, and a term of supervised release post-imprisonment of up to three years. Mohapatra's sentencing is currently scheduled for January 2013.

United States v. Zhang, No. 1:12-CR-00390 (S.D.N.Y.). On May 29, Bo Zhang pled guilty to one count of theft of government property and one count of visa fraud after downloading proprietary software code owned by the U.S. Department of Treasury while working as a contract employee for the Federal Reserve Bank of New York. On Dec. 5, Zhang was sentenced to time served and three years of supervised release, with six months of home confinement.

United States v. Yang, No. 11-CR-458 (N.D. Ill.) (84 PTCJ 920, 9/28/12). On Sept. 19, Chunlai Yang, an ex-software engineer at CME Group Inc., pled guilty to two counts of trade secret theft based on his illicit downloading of CME trade secrets and source code relating to CME's ''Globex'' trading platform, which he intended to use to develop a trading platform for the Zhangjiagang China chemical electronic trading exchange. Yang now faces a maximum of 10 years in prison and a $250,000 fine for each count. Yang's sentencing has been scheduled for February 2013.

United States v. Qin, No. 2:10-cr-20454 (E.D. Mich.). On Nov. 30, a former General Motors engineer and her husband were convicted of one count of conspiracy to possess trade secrets without authorization, and two counts of unauthorized possession of trade secrets. According to the indictment, Shanshan Du worked as an engineer within GM's Advanced Technology Vehicles Group from 2000 until 2005, during which time she had access to GM's trade secrets regarding its hybrid vehicle technology. Around the time that she joined GM, Du and her husband, Yu Qin, formed Millennium Technology International Inc., which was engaged in the business of developing technology for hybrid vehicles. Du provided Qin with GM's trade secrets regarding hybrid vehicles, which Qin then used to market himself to potential employers. Qin additionally formed joint venture companies associated with MTI to market and sell hybrid vehicle technology in China, and reached out to Chery Automobile—a Chinese competitor of GM—regarding a hybrid vehicle joint venture.

The jury found both Qin and Du guilty of conspiracy to possess trade secrets and unauthorized possession of trade secrets, and also found Qin guilty of three counts of wire fraud and one count of obstruction of justice. Sentencing has been scheduled for February 2013.

United States v. Liew, No. 3:11-CR-00573 (N.D. Cal). On Feb. 8, the U.S. Department of Justice unveiled a case charging four individuals and five corporations under 18 U.S.C. § 1832 for their roles in a long-running scheme to steal proprietary information from DuPont with the intent to benefit the Chinese government.[6] Significantly, the indictment included Panang Group Co., a company owned and controlled by the Chinese government, as well as one of its Chinese executives. The trade secrets related to the manufacture of titanium dioxide, which, according to the indictment, China had identified as a priority for the country's development.

The case unfolded after federal prosecutors indicted Walter Liew and his wife, accusing them of obstructing justice in connection with the investigation of possible theft of DuPont's titanium dioxide. In a search of the Liews' home, the FBI found a ''trove'' of correspondence establishing that Liew was in the process of obtaining DuPont's titanium dioxide processes and data to sell to Chinese companies. According to the superseding indictment, Liew was tasked by representatives of the Chinese government to obtain technology for the purpose of developing large scale titanium dioxide production capability in China. In addition to being the first foreign economic espionage prosecution against a corporation, this case is unprecedented in that it directly asserts that the Chinese government had a role in the trade secret allegations at issue.

CONCLUSION

Prosecutions like *Liew* are all the more troubling in light of recent studies showing the significance of trade secrets and other forms of intellectual property to the U.S. economy. According to a March report from the Economics and Statistics Administration and the Patent

[6] *See* DOJ Press Release, *U.S. and Chinese Defendants Charged with Economic Espionage and Theft of Trade Secrets in Connection with Conspiracy to Sell Trade Secrets to Chinese Companies* (Feb. 8, 2012), *available at* http://www.justice.gov/opa/pr/2012/February/12-nsd-180.html (last visited Jan. 7, 2013).

and Trademark Office, IP-intensive industries accounted for approximately 27.1 million American jobs in 2010, and 34.8 percent of the U.S. gross domestic product.[7] And yet, the United States Intellectual Property Enforcement Coordinator (IPEC) recently reported that ''[t]he pace of foreign economic collection of information and industrial espionage activities against major US corporations is accelerating.''[8]

In the face of this growing threat, U.S. companies should consider implementing increased security measures to protect their trade secrets and other valuable intellectual property, and should continue to stay apprised of significant legislative and judicial developments in this area.

At the same time, with the rising use of social media by employees, the internal threat faced by U.S. companies is perhaps just as great as that posed by foreign economic espionage. Employers seeking to minimize this threat should work to ensure that their employees are well-versed with respect to company computer usage policies (and that those policies include clear language regarding the use of social media).

Employers may also consider conducting background checks of key employees prior to providing them with access to valuable trade secret information. In addition, employers would be well-advised to monitor the internet for references to the company by its employees. To the extent that trade secret or other confidential information has been disclosed online, early detection may prove critical in mitigating the harm.

---

[7] *See* Economics and Statistics Administration and United States Patent and Trademark Office, *Intellectual Property and the U.S. Economy: Industries in Focus* (Mar. 2012), *available at* http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf (last visited Jan. 7, 2013).

[8] *See* IPEC, 2011 Annual Report on Intellectual Property Enforcement (Mar. 2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_mar2012.pdf (last visited Jan. 7, 2013).

  PTCJ ISSN 0148-7965