SEYFARTH SHAW

Management Alert

Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2013

By Robert B. Milligan and Daniel Joshua Salinas

As part of our annual tradition, we are pleased to present our discussion of the top 10 developments/headlines in trade secret, computer fraud, and non-compete law for 2013. Please join us for *our complimentary webinar* on March 6, 2014, at 10:00 a.m. P.S.T., where we will discuss them in greater detail. As with *all of our other webinars* (including the 12 installments in our 2013 Trade Secrets webinar series), this webinar will be recorded and later uploaded to our Trading Secrets blog to view at your convenience.

Last year we predicted that social media would continue to generate disputes in trade secret, computer fraud, and non-compete law, as well as in privacy law. 2013 did not disappoint with significant social media decisions involving the ownership of social media accounts and "followers" and "connections," as well as cases addressing liability or consequences for actions taken on social media, such as *updating one's status*, *communicating with "restricted" connections*, *creating fake social media accounts*, or *deleting one's account* during pending litigation.

We also saw more states (e.g., *Arkansas, Utah, New Mexico*, *California*, *Colorado, Nevada*, *Michigan*, *New Jersey*, *Oregon*, and *Washington*) enact *legislation* to protect employees' "personal" social media accounts and we expect more states to follow.

The circuit split regarding the interpretation of what is unlawful access under the Computer Fraud and Abuse Act ("CFAA") remains *unresolved* and another case will need to make its way up to the Supreme Court or legislation passed to clarify its scope as federal courts continue to reach differing results concerning whether employees can be held liable under for violating computer use or access policies.

There have also been several legislative efforts to modify trade secret, computer fraud, or non-compete law in various jurisdictions. Texas adopted a version of the *Uniform Trade Secrets Act*, leaving Massachusetts and New York as the lone holdouts. *Oklahoma* passed legislation expressly permitting employee non-solicit agreements. *Massachusetts*, *Michigan*, *Illinois*, *New Jersey*, *Maryland*, *Minnesota*, and *Connecticut* considered bills that would provide certain limitations on non-compete agreements but they were not adopted.

We expect more legislative activity in 2014, particularly regarding privacy, the scope of the CFAA, and trade secret legislation to curb foreign trade secret theft and cyber-attacks.

Finally, while the Snowden kerfuffle and NSA snooping captured the headlines in 2013, government agencies remained active, including some high profile *prosecutions* under the Economic Espionage Act, the release of the Obama

Administration's *Strategy on Mitigating the Theft of U.S. Trade Secrets*, and the *National Labor Relations Board's continued* scrutiny of employers' social media policies. We expect more government activity in this space in 2014.

Here is our listing of top developments/headlines in trade secret, computer fraud, and non-compete law for 2013 in no particular order:

1. Dust Off Those Agreements . . . Significant New Non-Compete Cases Keep Employers On Their Toes.

Employers were kept on their toes with some significant non-compete decisions which forced some employers to update their agreements and onboarding/exiting practices. First, in *Fifield v. Premier Dealer Services*, an Illinois appellate court found that less than two years employment is inadequate consideration to enforce a non-compete against an at-will employee where no other consideration was given for the non-compete. Second, in *Dawson v. Ameritox*, an Alabama federal court found that a non-compete executed prior to employment was unenforceable. Next, in *Corporate Tech. v. Hartnett*, a Massachusetts federal court held that initiating contact was not necessary for finding solicitation in breach of a customer non-solicitation agreement. Lastly, in *Assurance Data v. Malyevac*, the Virginia Supreme Court found that a demurrer (i.e., a pleading challenge) should not be used to determine the enforceability of non-compete provisions but rather evidence should be introduced before making such a determination.

2. Continued Split of Authority On the Computer Fraud and Abuse Act and Efforts to Reform CFAA and Enhance Federal Trade Secret and Cybersecurity Law.

Courts in *Massachusetts*, *Minnesota*, and *New York* joined the Ninth Circuit's narrow reading of the CFAA and limited its applicability to pure hacking scenarios rather than violations of employer computer usage or access policies. Additionally, in 2013, Representative Zoe Lofgren *introduced* Aaron's Law, named after the political hackvist Aaron Swartz, to reform of the Computer Fraud and Abuse Act. Her proposed legislation would limit the CFAA to pure hacking scenarios and exclude violations of computer usage policies and internet terms of service from its scope. Lofgren also introduced legislation which would create a federal civil cause of action in federal court for trade secret misappropriation. Other legislation to prevent intellectual property theft was also introduced including the *Deter Cyber Theft Act*, which aims to block products that contain intellectual property stolen from U.S. companies by foreign countries from being sold in the United States. The *Cyber Economic Espionage Accountability Act* was also introduced and allows U.S. authorities to "punish criminals backed by China, Russia or other foreign governments for cyberspying and theft." We expect Congress to consider similar legislation in 2014.

3. Texas Adopts Uniform Trade Secrets Act

Texas joined forty-seven other states in *adopting* some version of the Uniform Trade Secrets Act. Until recently, Texas common law governed misappropriation of trade secrets lawsuits in Texas. The new changes under the Texas UTSA (which we discuss in more detail *here*) provide protection for customer lists, the ability to recover attorneys' fees, a presumption in favor of granting protective orders to preserve the secrecy of trade secrets during pending litigation, and that information obtained by reverse engineering does not meet the definition of a trade secret. Legislation has been *introduced* in Massachusetts to adopt the Act but has yet to pass. For additional information on recent trade secret and non-compete legislative updates, check out our webinar "*Trade Secrets and Non-Compete Legislative Update*."

4. High Profile Prosecutions and Trials under Computer Fraud and Abuse Act and Economic Espionage Act

2013 saw several high profile prosecutions and trials under the CFAA and Economic Espionage Act. *Bradley Manning*, who allegedly leaked confidential government documents, to WikiLeaks, and *Andrew 'Weev' Auernheimer*, who allegedly hacked AT&T's servers, were both convicted under the CFAA. Executive recruiter David Nosal was *convicted* by a San Francisco jury of violating federal trade secret laws and the CFAA and *sentenced* to one year and a day in federal prison. In *U.S v. Jin*, the Seventh Circuit *upheld the conviction* of a Chicago woman sentenced to four years in prison for stealing trade secrets of her employer before boarding a plane for China. For additional information on criminal liability for trade secret misappropriation, check out our webinar "*The Stakes Just Got Higher: Criminal Prosecution of Trade Secret Misappropriation.*"

5. More Social Media Privacy Legislation

Arkansas, Utah, New Mexico, *Colorado, Nevada*, *Michigan*, *New Jersey*, *Oregon*, and *Washington* all passed legislation social media privacy legislation in 2013 that prohibited employers from asking or insisting that their employees provide access to their personal social networking accounts. *California* extended its current social media privacy law to specify that it encompassed public employers. We expect more states to enact social media privacy legislation in 2014.

6. Continued Uncertainty on the Scope of Trade Secret Preemption

Courts have continued to struggle with the scope and timing of applying preemption in trade secret cases, but there is a growing movement to displace common law tort claims for the theft of information. Such claims are typically tortious interference with contract, conversion, unfair competition, and breach of fiduciary duty. In essence, plaintiffs may only be left with a breach of contract and a trade secret claim for the theft of information if a jurisdiction adopted a broad preemption perspective. Courts in western states such as *Arizona*, *Hawaii*, *Nevada*, *Utah*, and *Washington* have preempted "confidential information" theft claims under their respective trade secret preemption statutes.

In *K.F. Jacobsen v. Gaylor*, an Oregon federal court, however, found that a conversion claim for theft of confidential information was not preempted. In *Triage Consulting Group v. IMA*, a Pennsylvania federal court permitted the pleading of preempted claims in the alternative. Additionally, in *Angelica Textile Svcs. v. Park*, a California Court of Appeal found that there was no preemption of claims for breach of contract, unfair competition, conversion, or tortious interference because the claims were based on facts distinct from the trade secret claim and the conversion claim asserted the theft of tangible documents. In contrast, in *Anheuser-Busch v. Clark*, a California federal court found that a return of personal property claim based on the taking of "confidential, proprietary, and/or trade secret information" was preempted because there was no other basis beside trade secrets law for a property right in the taken information. For additional information on the practical impact of preemption on protecting trade secrets and litigating trade secret cases, check out our webinar "*How and Why California is Different When it Comes to Trade Secrets and Non-Competes.*"

7. Growing Challenge of Protecting of Information in the Cloud with Increasing Prevalence of BYOD and Online Storage

While the benefits of cloud computing are well documented, the growth of third party online data storage has facilitated the ability for *rogue employees to take valuable trade secrets* and other proprietary company electronic files, in the matter of minutes, if not seconds. The increasing use of mobile devices and cloud technologies by companies both large and small is likely to result in more mobile devices and online storage being relevant in litigation. A recent article in The Recorder entitled "*Trade Secrets Spat Center on Cloud*," observed that the existence of cloud computing services within the workplace makes it "harder for companies to distinguish true data breaches from false alarms."

An insightful Symantec/Ponemon *study* on employees' beliefs about IP and data theft was released in 2013. It surveyed 3,317 employees in 6 countries (U.S., U.K., France, Brazil, China, South Korea). According to the survey, 1 in 3 employees move work files to file sharing apps (e.g. Drop Box). Half of employees who left/lost their jobs kept confidential information 40% plan to use confidential information at a new job. The top reasons employees believe data theft acceptable: (1) does not harm the company does not strictly enforce its policies; (2) information is not secured and generally available; or (3) employee would not receive any economic gain. The results of this study serve as a reminder that employers *must be vigilant* to ensure that they have robust agreements and policies with their employees as well as other sound trade secret protections, including employee training and IT security, to protect their valuable trade secrets and company data before they are compromised and stolen. Employers should implement policies and agreements to restrict or clarify the use of cloud computing services for storing and sharing company data by employees. Some employers may prefer to simply block all access to such cloud computing services and document the same in their policies and agreements. For a further discussion about steps and responses companies can take when their confidential information and/or trade secrets appear, or are threatened to appear, on the Internet, check out our webinar "*My Company's Confidential Information is Posted on the Internet! What Can I Do?*"

8. Continued Significance of Choice of Law and Forum Selection Provisions In Non-Compete and Trade Secret Disputes

The U.S. Supreme Court's recent decision in *Atlantic Marine v. U.S.D.C. for the W.D. of Texas* appears to strengthen the enforceability of forum selection clauses as it held that courts should ordinarily transfer cases pursuant to applicable and enforceable forum selection clauses in all but the most extraordinary circumstances. While *Atlantic Marine* did not concern restrictive covenant agreements or the employer-employee context, it may nonetheless make it more difficult for current and/or former employees to circumvent the forum selection clauses contained in their non-compete or trade secret protection agreements. Many federal courts continue to enforce out-of-state forum selection clauses in non-compete disputes (see *AJZN v. Yu* and *Meras Eng'r'g v. CH2O*), while some courts have *disregarded* forum selection clauses in such disputes "in the interests of justice." The Federal Circuit in *Convolve and MIT v. Compaq and Seagate* held that information at issue lost its trade secret protection when the trade secret holder disclosed the information because it failed to comply with the confidential marking requirement set forth in a non-disclosure agreement. Accordingly, trade secret holders should be careful what their non-disclosure agreements say about trade secret protection otherwise they may lose such protection if they fail to follow such agreements.

9. Social Media Continues to Change Traditional Legal Definitions and Analyses

Social media continues to change the way we define various activities in employment, litigation, and our everyday lives. A Pennsylvania federal district court in the closely watched *Eagle v. Morgan* case found that a former employee was able to successfully prove her causes of action against her former employer for the theft of her LinkedIn account, but she was unable to prove damages with reasonable certainty. Recent cases in *Massachusetts* and *Oklahoma* held that social media posts, updates and communications with former customers did not violate their non-solicitation restrictive covenants with their former employer. In the litigation context, a New Jersey federal court issued sanctions against a litigant for *deleting his Facebook profile*, while a New York federal court allowed the FTC to *effectuate service of process on foreign defendants* through Facebook. The Fourth Circuit held that "liking" something on Facebook is "a form of free speech protected by the First Amendment." Federal district courts in *Nevada* and *New Jersey* illustrated the growing trend of courts finding that individuals may lack a reasonable expectation of privacy in social media posts. For further discussion on the relationship between social media and trade secrets, check out our webinar "*Employee Privacy and Social Networking: Can Your Trade Secret Survive?*"

10. ITC Remains Attractive Forum to Address Trade Secret Theft

The Federal Circuit caught the attention of the ITC and trade secret litigators alike when it ruled in *TianRui Group Co. v. ITC* that the ITC can exercise its jurisdiction over acts of misappropriation occurring entirely in China. Since then, victims of trade secret theft by foreign entities are increasingly seeking relief from the ITC (e.g. *In the Matter of Certain Rubber Resins and Processes for Manufacturing Same (Inv. No. 337-TA-849)*). For valuable insight on protecting trade secrets and confidential information in China and other Asian countries, including the effective use of non-compete and non-disclosure agreements, please check out our recent webinar titled, "*Trade Secret and Non-Compete Considerations in Asia.*"

We thank everyone who followed us this year and we really appreciate all of your support. We also thank everyone who helped us make the *ABA's Top 100 Law Blogs list*. We will continue to provide up-to-the-minute information on the latest legal trends and cases across the country, as well as important thought leadership and resource links and materials.

Don't forget to *register* to receive a copy of our Annual Blog Year in Review.

Robert B. Milligan is a co-chair of the Trade Secrets, Computer Fraud & Non-Competes practice group. *Daniel Joshua Salinas* is an attorney in the Los Angeles office. If you would like further information, please contact your Seyfarth attorney, Robert B. Milligan at *rmilligan@seyfarth.com* / (310) 201-1579, or Daniel Joshua Salinas at *jsalinas@seyfarth.com* / (310) 201-1514. You may also visit and register for our blog, Trading Secrets, at *www.tradesecretslaw.com*. You can also follow us on Twitter at @tradesecretslaw.