SEYFARTH SHAW

Management Alert

Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2014

By Robert B. Milligan and Daniel P. Hart

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 2014. Please join us for our complimentary webinar on January 27, 2015, at 1:00 p.m. e.s.t., where we will discuss them in greater detail. As with all of our other webinars (including the 10 installments in our 2014 Trade Secrets webinar series), this webinar will be recorded and later uploaded to our Trading Secrets blog to view at your convenience.

Here is our listing of top developments/headlines in trade secret, computer fraud, and non-compete law for 2014, as well as our predictions for 2015, in no particular order:

1. Increased Threat to Trade Secrets by Hackers. As demonstrated by recent cyber-attacks, hackers represent a significant and growing threat to the intellectual property of U.S. and multinational companies. ICANN recently reported its own data breach and indicated that the email credentials of some ICANN staff members were compromised. Security company Mandiant published a report finding that the government of the People's Republic of China ("PRC") is sponsoring cyber-espionage to attack top U.S. companies. Moreover, CREATe.org released a whitepaper that highlighted how far-reaching and deeply challenging trade secret theft is for companies operating on a global scale and identified "hacktivists," some foreign governments, and organized crime (as well as competitors and rogue employees) as major threats to trade secrets. While much of the attention on foreign threats to trade secrets has focused on the PRC, recent decisions from courts in Shanghai suggest that some courts in the PRC may be adopting an enforcement approach in trade secrets and non-compete cases that is closer to the approach of U.S. courts. Notwithstanding this potentially significant development in the PRC, hackers, especially those tied to foreign governments, will likely continue to pose a major threat to U.S. and multinational companies in the near future. Please see our recent webinar on addressing data security breaches.

2. More High-Profile Prosecutions under the Computer Fraud and Abuse Act and Economic Espionage Act. In response to the growing threat to the trade secrets of U.S. companies, the Obama Administration released a 150-page report that unveiled a government-wide strategy designed to reduce trade secret theft by hackers, employees, and companies. Consistent with this strategy, in 2014 the U.S. Department of Justice continued to pursue high-profile prosecutions under the CFAA and Economic Espionage Act, particularly against defendants tied to the Chinese government. As we previously reported, earlier this year the DOJ obtained the first-ever federal jury conviction under the Economic Espionage Act in the *U.S. v. Liew case*. Following the jury's conviction of two individuals and one company in that case, a federal court sentenced defendant Walter Liew to 15 years in prison for theft of trade secrets from chemical giant DuPont and selling them to an overseas company controlled by the government of the PRC. In another high-profile criminal case, a federal grand jury

indicted five high-ranking officials of the PRC's People's Liberation Army for computer hacking, economic espionage and other offenses directed at American companies in the nuclear power, metals and solar products industries. More high-profile prosecutions will likely continue in the next year as the federal government further cracks down on trade secret theft.

3. Continued Attempt to Create Civil Cause of Action for Trade Secrets Theft in Federal Court. As we previously reported, the past several years have seen increased attempts to create a civil cause of action for trade secrets misappropriation at the federal level. 2014 was no exception. Earlier this year, Sens. Christopher Coons (D-Del.) and Orrin Hatch (R-Utah) introduced the Defend Trade Secrets Act of 2014 in the U.S. Senate. The bill amends the Economic Espionage Act to provide a civil cause of action to private litigants for violations of 18 U.S.C. § 1831(a) and 1832(a) of the EEA and for "misappropriation of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce." The bill also would allow a plaintiff to obtain a seizure order, though some have questioned whether this remedy may be subject to abuse and have concerns about implementation. A few months later, a bi-partisan group led by Reps. George Holding (R-N.C.) and Jerrold Nadler (D-N.Y.) introduced a similar bill in the House of Representatives, the Trade Secrets Protection Act of 2014. The House bill largely tracks the Senate bill but refines the seizure provisions and contains other notable refinements that we discussed here. The House Judiciary Committee has reported favorably on the bill and recommended its passage. Although the House did not pass the bill before adjourning, expect to see the same or similar legislation introduced early this year. With the recent high profile hacking incidents, we believe that there is momentum for the passage of a bill this year.

4. Attempt to Harmonize Trade Secrets protection in EU. Across the pond, European lawmakers are considering a similar proposal to harmonize trade secrets protection throughout the EU's 28 members states. As we discussed here, currently there is no uniform protection of trade secrets across the EU. Instead, a patchwork of uneven levels of protection and remedies exist among EU Member States. After a study prepared for the European Commission identified substantial perceived weaknesses in the trade secrets protections afforded by the laws of many Member States, the European Commission announced a proposal for a Directive on trade secrets that, if enacted, will substantially alter the legal landscape in Europe regarding trade secret protection and will enhance cross-border certainty within the EU. The draft directive is currently being reviewed by the EU Parliament's Legal Affairs, Internal Market, and Industry Committees and their decisions have not been released yet. While the European Parliament has not yet voted on the proposal, it is expected that the matter will be scheduled for a first reading in the Parliament during the first half of 2015.

5. Massachusetts Fails to Enact Proposed Non-Compete / Trade Secrets Legislation. In what has become an annual tradition over the past several years, lawmakers in Massachusetts once again debated, but failed to pass, legislation that would overhaul the Bay State's existing law on non-competes and trade secrets, which are currently governed by state common law. Along with New York, Massachusetts is one of only two states that has not yet adopted a version of the Uniform Trade Secrets Act ("UTSA"). This past legislative session, the Massachusetts legislature considered a proposed bill that would have adopted the UTSA and that (more controversially) would have virtually eliminated employee non-compete agreements in Massachusetts. Although the state Senate overwhelmingly approved a compromise bill that, if enacted, would have imposed certain notice requirements and established presumptions of reasonableness for employee non-competes (among other provisions), ultimately the legislature did not pass either the compromise bill or any of the various alternative non-compete or trade secrets bills proposed this year. But if recent history is any guide, expect to see attempts to overhaul Massachusetts non-compete law once again introduced in 2015. In fact, after this year's legislative session ended, outgoing Governor Duval Patrick introduced another compromise bill that legislators may debate when the new legislative session begins in January.

6. Courts Continue to Grapple with UTSA's Preemptive Impact. Among the 48 states that have adopted some version of the UTSA, courts continue to grapple with the impact of the UTSA on common law remedies for misappropriation of confidential information (such as claims for unfair competition, conversion, tortious interference, or unjust enrichment). The UTSA contains a provision stating that the Act "displaces conflicting tort, restitutionary, and other laws of this State providing civil remedies for misappropriation of a trade secret" but "does not affect (1) contractual remedies, whether or not based on misappropriation of a trade secret; (2) other civil remedies that are not based on misappropriation of a trade secret; or (3) criminal remedies, whether or not based on misappropriation of a trade secret." As we discussed here, courts in several states have held that the UTSA should be read broadly to preempt all claims related to the misappropriation of

information, regardless of whether or not the information falls within the definition of a trade secret. In contrast, courts in other states have concluded that the UTSA preempts only claims for misappropriation of "trade secrets," as defined by the UTSA, and leaves available all other remedies for the protection of confidential information that is not a trade secret. With its recent decision in *Orca Communications Unlimited, LLC v. Noder*, 337 P.3d 545 (Az. 2014), the Arizona Supreme Court joined this latter group and held as a matter of first impression that the AUTSA does not displace common law remedies for misappropriation of confidential information that does not qualify as a trade secret. Expect to see states continue to line up on either side of this divide.

7. Continued Significance of Choice of Law and Forum Selection Provisions In Non-Compete Disputes. Following the U.S. Supreme Court's decision in *Atlantic Marine v. U.S.D.C. for the W.D. of Texas*, choice of law and forum selection clauses are increasingly significant in non-compete litigation. In *Atlantic Marine*, the Supreme Court 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, the decision appears to strengthen the enforceability of forum selection clauses generally. For example, in *AAMCO Transmissions, Inc. v. Romano*, — F. Supp. 2d –, 2014 WL 4105986 (E.D. Pa. Aug. 21, 2014), a federal district court in Pennsylvania enforced a forum-selection clause in a non-compete agreement against both a franchisee who signed the agreement and the franchisee's wife who, though not a signatory the agreement, was also deemed to be bound by the forum selection clause because of her close connection to the signatory. In addition, as we reported here, federal district courts in California are increasingly enforcing forum selection clauses in non-compete agreements of California employees and finding that enforcement of such clauses does not violate California's strong public policy of employee mobility. In light of *Atlantic Marine*, expect companies to make greater use of choice of law and forum selection clauses (and the resulting "race to the courthouse") in suits to enforce their restrictive covenants.

8. Social Media Continues to Generate Disputes. Continuing a trend that we discussed last year, social media continues to generate disputes in trade secret, computer fraud, and non-compete law, as well as in privacy law. Wisconsin, Louisiana, Oklahoma, New Hampshire, and Rhode Island joined several other states in enacting legislation to protect "personal" use of social media by employees. Expect other states to get on the social media bandwagon in the next year. The ownership of content stored in LinkedIn and other social medial accounts is also a continuing source of disputes. Like courts in the UK and elsewhere, US courts continue to grapple with whether there can be trade secret protection for such information. For example, a few months ago, a federal district court in California issued a well-publicized decision in *Cellular Accessories For Less, Inc. v. Trinitas LLC*, No. CV 12–06736 D, 2014 WL 4627090 (C.D. Cal. Sept. 16, 2014), in which it denied a motion for summary judgment on a trade secrets misappropriation claim against a former employee who retained the contacts in a LinkedIn account that he created while employed by the plaintiff. That case illustrates that LinkedIn and other social media contacts can be protectable as trade secrets if the methods used to compile the contact information are "sophisticated," "difficult," or "particularly time consuming," though the purported trade secret holder will also have to establish that the contacts were not made public in order to be entitled to trade secret protection. Although the Cellular Accessories court did not rely on decisions from other jurisdictions, the court's decision is consistent with a handful of recent decisions in which English courts have suggested that an employee's competitive use of LinkedIn contacts that the employee developed during his or her employment might, in some circumstances, constitute a breach of the duty of good faith. (*See, e.g., Whitmar Publications Limited v. Gamage* [2013] EWHC 1881 (Ch.) and *Hays Specialist Recruitment (Holdings) v. Ions* [2008] EWHC 745 (Ch.).) As use of social media continues to proliferate, more courts are likely to weigh-in on this issue.

9. NLRB Challenges Employer Policies on Employee Use of Social Media and IT Resources. Speaking of social media, the National Labor Relations Board ("NLRB") issued significant decisions this year that have left many employers scrambling to revise their policies on employee use of social media and IT resources. As we reported here, in *Triple Play Sports Bar & Grille*, 361 NLRB No. 31 (2014), the NLRB ruled that a Facebook discussion regarding an employer's tax withholding calculations and an employee's "like" of the discussion constituted concerted activities protected by Section 7 of the National Labor Relations Act ("NLRA"), which protects employees' rights to engage in concerted activities regarding the terms and conditions of their employment. The Board also held that the employer's internet and blogging policy (which provided that "engaging in inappropriate discussions about the company, management, and/or co-workers, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment") was overly broad and, therefore, violated the NLRA. Additionally, as we reported here, the NLRB recently ruled that employees who have access to an employer's

email system as part of their job generally may, during non-working time, use the email system to communicate about wages, hours, working conditions and union issues. The NLRB's ruling (*Purple Communications*, 361 NLRB No. 126 (2014)) poses a major headache for employers who seek to control use of their IT assets. As the new Republican-led Congress seeks to reign-in the NLRB, expect these rulings to be hotly debated in the coming year.

10. Courts, Lawmakers, and Regulators Continue to Scrutinize Non-Competes and Consideration Remains a Hot Button Issue. Finally, as in past years, many employers are once again reviewing and tweaking their non-competes and onboarding procedures in light of continued scrutiny of non-competes by courts, legislatures, and regulators. On the enforcement side, the Texas Supreme Court found that the enforcement of a forfeiture provision for competitive activity in an employee incentive compensation plan was not contrary to Texas public policy. Courts have, however, continued to issue significant decisions invalidating some non-competes. For example, in *Dawson v. Ameritox, Ltd.*, 571 Fed. App'x. 875 (11th Cir. 2014), the Eleventh Circuit affirmed an Alabama federal court's ruling that a non-compete executed prior to employment was unenforceable. In *Nott Co. v. Eberhardt*, Nos. A13–1061, A13–1390, 2014 WL 2441118 (Minn. Ct. App. June 2, 2014), the Minnesota Court of Appeals held that a non-compete was unenforceable against an employee who signed the non-compete and received benefits purportedly as consideration for the agreement because another employee did not sign a non-compete but nevertheless received the same benefits. In *Charles T. Creech, Inc. v. Brown*, 433 S.W.3d 345 (Ky. 2014), the Kentucky Supreme Court held that a non-compete with an existing employee was not supported by consideration where the employee was offered no payment, no change in employment terms, and was not threatened with termination if he failed to execute the agreement. Following an Illinois Court of Appeals' decision in *Fifield v. Premier Dealer Servs., Inc.*, 993 N.E.2d 938 (Ill. App. Ct. 2013), courts in Illinois are continuing to consider whether less than two years employment is adequate consideration to enforce a non-compete against an at-will employee where no other consideration is given for the non-compete. Courts in Pennsylvania and Wisconsin are also grappling with what constitutes sufficient consideration for the enforcement of non-competes. We also expect that government agencies and employees will continue to mount challenges to the use and enforcement of non-compete and other restrictive covenants (including no poaching provisions) with certain employees and industries this year. In light of these decisions and other continuing developments in non-compete law, employers should periodically review their existing agreements and on-boarding procedures to maximize the likelihood that their agreements will be upheld.

We thank everyone who followed us this year and we really appreciate all of your support. We will continue to provide up-to-the-minute information on the latest legal trends and cases in the U.S. and across the world, as well as important thought leadership and resource links and materials.

Robert B. Milligan is Co-Chair and Daniel P. Hart is an associate of the Trade Secrets, Computer Fraud & Non-Compete Practice Group. If you have any questions, please contact Robert B. Milligan at rmilligan@seyfarth.com/(310) 201-1579, Daniel P. Hart at dhart@seyfarth.com/(404) 885-1500, the Seyfarth Shaw attorney with whom you work or any Trade Secrets, Computer Fraud & Non-Compete attorney on our website (www.seyfarth.com/tradesecrets). You may also access our blog, Trading Secrets, at www.tradesecretslaw.com.