



# Trade Secret Protection Best Practices

Hiring Competitors' Employees  
and Protecting the Company  
When Competitors Hire Yours

## Presented By:

---



**D. Joshua Salinas**

**Los Angeles**

(310) 201-1514

[jsalinas@seyfarth.com](mailto:jsalinas@seyfarth.com)

**Areas of Practice:**

Trade Secrets, Computer Fraud & Non-Competes

Intellectual Property

Patent, Internet & Privacy, Trademark, Copyright

Commercial Litigation

Alternative Dispute Resolution, Business Torts, Contract Disputes

---



**Robert B. Milligan**

**Los Angeles**

(310) 201-1579

[rmilligan@seyfarth.com](mailto:rmilligan@seyfarth.com)

**Areas of Practice**

Trade Secrets, Computer Fraud & Non-Competes

Intellectual Property

Copyright; Internet & Privacy; Patent; Trademark

Commercial Class Action Defense

Commercial Litigation

Labor and Employment

---



**Michael Wexler**

**Chicago**

(312) 460-5559

[mwexler@seyfarth.com](mailto:mwexler@seyfarth.com)

**Areas of Practice:**

Trade Secrets, Computer Fraud & Non-Competes

Commercial Litigation

Intellectual Property

White Collar Criminal Defense

---

## Table of Contents

1. **Summary of law on key issues**
2. **Appendix A - Sricom, Inc. case**
3. **Appendix B - Management Alert on new California non-competes case**
4. **Appendix C - Hartstein case**
5. **Appendix D - Unhealthy Competition article**
6. **Appendix E - Management Alert on social media laws**
7. **Appendix F - Trade Secret Audit article**
8. **Appendix G - BYOD tips and example policies**
9. **Appendix H - Trade secret blog article on trade secret injunctions**
10. **Appendix I - Article on threat to trade secrets posed by cloud computing and social media**
11. **Appendix J - Exit Interview Certification**
12. **Appendix K - Presenters' biographies**

# Summary of Law on Key Issues

# Trade Secret Protection Suggestions for Handling the Hiring of a New Employee from a Competitor

## Interviewing and Assessing Existing Restrictive Covenants

1. Advise company personnel who are interviewing the recruit not to ask about a competitor's confidential information during the hiring process. Focus the interview on the recruit's general skills and experience in the industry.
2. Ask the recruit if he or she has signed any restrictive covenants or confidentiality agreements with current or previous employers. Review these agreements before extending an offer or make any offer conditional upon such review.
  - *Silguero v. Creteguard*, 187 Cal. App. 4th 60 (2010) - An employer's ratification of an employee's unlawful non-compete agreement with a former employer may give rise to a wrongful termination claim.
3. Make it clear that the employee should not, under any circumstances, bring any of his or her former employer's information or solicit former co-workers. Your company could be held liable for the recruit's misappropriation or solicitation.
4. Evaluate restrictive covenants and determine the risk of the employer instituting suit, particularly out of state employers with history of enforcing covenants.
5. Do not allow the recruit to do any work for your company until he or she has left his or her prior employer.
6. Instruct the employee not to bring any of the former employer's property.
7. Assist the employee in announcing the change in employment upon commencement of employment. Focus on making the transition as smooth as possible for the current employer and encourage the departing employee to give proper notice and work out a mutually agreeable transition schedule with his or her current employer.

## Hiring and Onboarding - Key Agreements / Policies

1. Invention assignment agreements - Ensure that they are written in the present tense, do not use overly broad language, include assignment of ideas, and contain the required

notification that inventions which are created using the employee's own time and resources are not assignable to the employer.

- *Applied Materials, Inc. v. Advanced Micro-Fabrication Equipment*, 630 F. Supp. 2d 1084 (N.D. Cal. 2009) - The court found the presumption language to be mandatory (not rebuttable) and overbroad as to subject matter. Thus, the post-employment invention assignment language violated the California public policy codified in Business and Professions Code section 16600.
  - *Preston v. Marathon Oil*, 277 P. 3d 81 (2012) Case No. 2011-1013 (Fed. Cir. July 10, 2012)
  - *Mattel v. MGA*, 2011 WL 1114250 (C.D. Cal. 2011).
  - Labor Code sections 2870, 2871, and 2872
2. Non-disclosure and trade secret protection agreements
  3. Non-solicitation of employee agreements
    - *Thomas Weisel Partners LLC v. BNP Paribas*, 2010 WL 546497 (N.D. Cal. Feb. 10, 2010) - The court found that an agreement stating that an employee, after his termination, would not hire his former employer's employees was void under Business and Professions Code section 16600. However, other language in the agreement pertaining to confidentiality and "no solicitation" of employees was permissible.
    - *Sircom, Inc. v. eBisLogic, Inc. et al.*, Case No.: 12-CV-00904-LHK (N.D. Cal. Sept. 13, 2012) - Judge Koh found a no-hire and non-solicitation provision of an employment agreement to be unenforceable under California Business and Professions Code section 16600. See Order attached as Appendix A.
  4. Computer use and access agreements - Recent developments in the Computer Fraud and Abuse Act have called into question whether a violation of a traditional computer use policy can serve as a basis for a CFAA claim. Thus, rather than relying solely on computer use policies, it is often wiser to limit employee access to company databases on a need-to-know basis, as well as having robust computer access policies.
  5. Social media policy and social media ownership agreements
  6. Employee handbook provisions regarding monitoring and code of conduct - Remember that they are typically not contracts.

7. Agreements relating to former employers' trade secrets - Advise the new employee in writing that your offer of employment is not based on his or her knowledge or possession of any previous employer's confidential information. Consider having the new employee sign an acknowledgement (free standing or in a non-disclosure agreement) affirming that:
  - Employee will neither use nor disclose any confidential or proprietary information of any former employer or others in performing his or her job duties for the company.
  - Employee agrees that he or she will not access his or her former employer's e-mail, voicemail, or other computer systems for any purpose.
  - Employee agrees that he or she is not in possession of any property of his or her former employer.

### Hiring and Onboarding - Key Procedures

1. Conduct new hire training on the importance of protecting your company's assets. Be sure to cover obvious topics, such as following computer access policies and your company's data encryption system, and less obvious topics, such as the possibility of accidental trade secret disclosure from holding business discussions in public places. Engrain a culture of protection of company assets through respect for confidentiality.
2. Separate out trade secret agreements and training from the piles of paperwork and training that new employees receive so that they are not glossed over or disregarded as "just another piece of paper to sign."
3. If the new employee's position at your company is going to be substantially similar to his or her previous position, consider initially assigning the employee to different projects. Also consider temporarily modifying the new employee's job responsibilities.
4. Periodically review the new employee's work to confirm that he or she is not utilizing confidential and proprietary information belonging to previous employers. Monitor the employee's computer to ensure that confidential and proprietary information belonging to previous employers is not uploaded to company computers.
5. Periodically follow up with all employees to ensure continued compliance with policies and agreements put in place to protect confidential information. Always emphasize the importance of protecting company trade secrets. Training employees solely at the new hire stage is not sufficient in the long run.

# Trade Secret Protection Suggestions for Handling a Departing Employee Who Is Joining a Competitor

## Exit Interviews

1. Make sure you have an exit interview.
2. Question the departing employee in detail about his or her new job, including identifying the new employer, position, duties, and responsibilities. Ask the employee why he or she is leaving. Question the employee on his or her access to company trade secrets during his or her employment. Question the employee on his or her possession of company property and his or her return of such property.
3. Question the employee concerning any suspicious activities related to company property and computer access / usage.
4. Consider using an exit interview certification in which the departing employee acknowledges or certifies his or her understanding of his or her obligations. At the very least, provide the departing employee with a copy of his or her employment agreement. Inform the employee that the company expects departing employees to conform their conduct accordingly and instruct the employee to provide a copy of the agreement to his or her new employer. Give the employee an opportunity to ask questions. Confirm this in writing.
5. Make sure that the departing employee has returned all company documents, notebooks, files, thumb drives, and other tangible company property, including badges, cell phones, Blackberries, laptops, etc.
6. Assess the credibility of the employee during the interview.
7. Follow-up with business team regarding the exit interview and any special handling.

## Further Steps to Protect Your Company

1. Interview co-workers to gather additional information regarding the departing employee's intentions and any suspicious activities.
2. Disable the departing employee's access to the facility and company computers. If your company permits employees to use personal electronic devices, you may have to take extra steps to ensure that these devices do not provide the employee with continued access to

company servers, email, etc. This is particularly a concern if company employs a BYOD policy or allows employees to save data on personal computers.

3. Inspect the employee's office and review hard copy files to ensure that company materials have not been compromised, taken, destroyed, or altered.
4. Review the employee's recent e-mail, computer system activity, and voicemail. Check recent computer activity for suspicious downloads or print jobs.
5. Review the employee's expense reports and cell phone records to determine if he or she is preparing to exit with any customers.
6. Follow up with customers that the departing employee was servicing. Determine if the departing employee has contacted them and tried to get them to switch their business.
7. Consider sending a letter to the new employer informing them of the employee's obligations to the company, as well as the employee.
8. Sequester the employee's computer and other electronic devices for forensic analysis. Use a professional. Also preserve the employee's emails.

A decorative graphic on the left side of the page, consisting of overlapping blue and green geometric shapes.

# Hot Topics in California Employment and Trade Secret Protection Law

## Strategies to Work Around California's Prohibition on Non-Compete Agreements

California Business and Professions Code §16600 states that “every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void.” The California Supreme Court, in *Edwards v. Arthur Andersen*, 44 Cal. 4th 937 (2008), interpreted this to mean that “noncompetition agreements are invalid...in California even if narrowly drawn, unless they fall within the applicable statutory exceptions of section 16601, 16602, or 16602.5.” Although the *Edwards* court did state in a footnote that they “do not here address the applicability of the so-called trade secret exception to section 16600,” this decision has rendered non-competition agreements in the typical employment scenario generally unenforceable in California.

Accordingly, under California law, employers are typically limited to using non-disclosure, invention assignment, and non-solicitation of employee covenants with employees.

However, under California law, a court may enjoin actual and threatened misappropriation of trade secrets. The CUTSA provides that “actual or threatened misappropriation may be enjoined.” See Cal. Civ. Code § 3426.2(a).

In *Central Valley General Hospital v. Smith*, 162 Cal. App. 4th 501 (2008), the defendant argued that California's rejection of the inevitable disclosure doctrine effectively preempted a court's ability to enjoin conduct that “threatened” the disclosure of a trade secret. The Court disagreed, stating that “the principle that threatened misappropriation of trade secrets may be enjoined is the law of California despite the rejection of the inevitable disclosure doctrine by California courts.”

The first application of the threatened misappropriation theory occurs where there is evidence that the former employer had protectable trade secrets, that those trade secrets remain in the knowledge of the former employee, and that the former employee has misused or disclosed some of those trade secrets in the past.

The second application of the threatened misappropriation theory occurs where there is evidence that the former employee “intends to improperly use or disclose some of those trade secrets.” This variant requires the moving party to establish the actual intent of the employee to misuse the trade secrets. Intent can be shown by circumstantial evidence.

A decorative graphic on the left side of the page consists of overlapping geometric shapes in shades of blue and green.

The third application of the threatened misappropriation theory occurs when the former employee and new employer wrongfully refuse to return the trade secrets after a demand for their return has been made. The *Central Valley* court did not formally adopt this approach as an acceptable means of proving threatened misappropriation; rather, it merely assumed that such evidence might be sufficient to support an injunction, but found no such facts in the record to support such a finding.

The *Central Valley* court rejected the application of the threatened misappropriation theory if the only factual showing is the defendant was in actual possession of the trade secrets. The court expressly found that a claim of threatened misappropriation requires a greater showing than mere possession by the defendant of trade secrets where the defendant acquired the trade secret by proper means.

Accordingly, California courts ordinarily only issue injunctive relief for the threatened misappropriation of trade secrets when there is actual evidence that the threatened misconduct is imminent. California courts have also expressly rejected the doctrine of inevitable disclosure – that is, the argument that, based on former employment responsibilities, it is inevitable the employee will misuse trade secrets during the course of his or her new employment. (See *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1143 (2002) and *Flir Systems, Inc. v. Parrish*, 174 Cal. App. 4th 1270 (2009)). Finally, as noted above, an employer's use of a non-compete agreement that is invalid under section 16600 may give rise to liability, as well as for a new employer's acquiescence to another's use of such an invalid agreement (See *Silguero v. Creteguard, Inc.*, 187 Cal. App. 4th 60 (2010)). In short, California is not a state where employers can routinely rely on non-competition agreements to protect their business from departing employees.

So how can employers work attempt to around California's prohibition on non-compete agreements?

- Threatened misappropriation of trade secrets theory.
- The trade secret exception to section 16600 - "Ample case law" supports enforcing noncompetition clauses "necessary to protect an employer's trade secret." *Brocade Communications Systems v. A10 Networks*, 2011 WL 1044899 (N.D. Cal.). But that does not mean including non-competes in employment agreements.
- Statutory exceptions to section 16600 exist for the sale or dissolution of a business, partnership, corporation, or LLC. See Appendix B for a Management Alert on recent a case.
- Including forum selection and choice of law clauses within an employment agreement may help ensure that any litigation arising under the agreement will occur in a forum that

is more accepting of non-competition agreements providing that the company has a significant connection to the forum. See *Hartstein v. Rembrandt IP Solutions*, 2012 WL 3075084 (N.D. Cal. 2012), but see *Application Group v. Hunter*, 61 Cal.App.4th 881 (1998). Are you prepared for a race to judgment? See Appendix C for the Order in *Hartstein v. Rembrandt*.

- Notice provisions?
- Garden leave?
- Consultant arrangements?
- Equity / stock option agreements - It is an open question whether ERISA preempts state law for qualified pension plans / “top-hat plans” for key executives following Edwards. See Appendix D for article concerning the issue.

### **Preemption Under the California Uniform Trade Secrets Act (CUTSA)**

CUTSA preempts “common law claims” that are “based upon the same nucleus of facts as the misappropriation of trade secrets claim for relief.” Such claims include common law claims for conversion, interference with contract, unjust enrichment, negligence, and Business and Professions Code section 17200 (See *K.C. Multimedia v. Bank of America*, 171 Cal. App. 4th 939, 958 (2009)). Additionally, in *Silvaco Data Systems v. Intel Corporation*, 184 Cal. App. 4th 210 (2010), the California Court of Appeal “reaffirm[ed] that CUTSA provides the exclusive civil remedy for conduct falling within its terms, so as to supersede other civil remedies ‘based upon misappropriation of a trade secret.’ (§ 3426.7, subs. (a), (b).)” *Id.* at 236. Preemption does not displace breach of contract claims.

In California state court, employers are forced, at the onset of litigation, to choose whether they will pursue a claim under CUTSA or various common law claims. The situation in federal court, however, can be quite different. In some California federal courts, an employer is not forced to choose until trial which of the claims that they will ultimately pursue. Think *Village-Kiwi LLC v. Adobe Systems*, 2009 WL 902337 (N.D. Cal. 2009) (rejecting preemption at the pleadings stage for claims of common law misappropriation and breach of confidence as premature, given that protectable interests may exist in confidential information); but see *Mattel, Inc. v. MGA Entertainment, Inc.*, 2011 WL 1114250 (C.D. Cal. 2011) (at the summary judgment stage, “in an effort to align with the California courts that have addressed this issue, the Court conclude[d] that UTSA supersedes claims based on the misappropriation of confidential information, whether or not that information meets the statutory definition of trade secret.”) *Id.* at \*46.

Thus, variety is the only certainty when it comes to preemption under CUTSA. This variety exists both between and within state and federal courts when it comes to the application and the breadth of preemption. There is no existing California Supreme Court decision on this matter.

Another issue that arises in this context is whether confidential information is protectable under a contract or tort theory in California. Information that may not rise to the level of a trade secret is protectable in California, isn't it? California grants protection against the misappropriation of a mere "idea," regardless of whether the idea is confidential or not. *Desny v. Wilder*, 46 Cal. App. 2d 715 (1956); *Bancroft-Whitney Co. v. Glen*, 64 Cal. App. 2d 327, 351 (1966) (unfair competition and breach of fiduciary duty claims involving the disclosure of employee's salary to competitor are actionable "even if the information regarding salaries is not deemed to be confidential.")

CUTSA does not affect "contractual remedies, whether or not based upon misappropriation of a trade secret" and does not affect "other civil remedies that are not based upon misappropriation of a trade secret." See Cal. Civ. Code § 3426.7(b); *Courtesy Temp. Serv., Inc. v. Camacho*, 222 Cal. App. 3d at 1292 (1990) ("the cases are legion holding that a former employee's use of confidential information obtained from his former employer to compete with him and to solicit the business of his former employer's customers is regarded as unfair competition"); *Ajaxo Inc. v. E\*Trade Group, Inc.*, 135 Cal. App. 4th 21, 62, fn. 38 (2005) ("In some cases, a breach of contract cause of action may be available where disclosed information does not qualify as a 'trade secret' under the UTSA (Civ.Code § 3426 et seq.) if the information is protected under a confidentiality or nondisclosure agreement, provided the agreement is not an invalid restraint of trade.")

However, the *Silvaco* case issued in 2010 has turned this well-established body of law on its head. *Silvaco Data Systems v. Intel Corp.*, 184 Cal. App. 4th 210, (April 29, 2010).

The *Silvaco* court held that if the only arguable property identified in the complaint is a trade secret, and the only basis for any property right is trade secrets law, then a conversion claim predicated on the theft of that property is unquestionably based upon misappropriation of a trade secret, and the conversion claim is preempted. The court stated that the only thing that might change this conclusion is the plaintiff's assertion of some other basis in fact or law on which to predicate the requisite property right. "But 'information' cannot be 'stolen' unless it constitutes property. And information is not property unless some law makes it so. If the plaintiff identifies no property right outside of trade secrets law, then he has no remedy outside that law, and there is nothing unsound or unjust about holding other theories superseded." *Id.* at 109.

The court in the *Mattel* matter reached a similar conclusion. "[C]UTSA supersedes claims based on the misappropriation of confidential information, whether or not that information meets

A decorative graphic on the left side of the page, consisting of overlapping blue and green geometric shapes.

the statutory definition of a trade secret.” *Mattel, Inc. v. MGA Entertainment, Inc.*, 2010 WL 5422504, \*45-46 (C.D. Cal. Dec. 27, 2010); but see *Leatt Corp. v. Innovative Safety Technology, LLC*, 2010 WL 2803947, \*6 (S.D. Cal. July 15, 2010) (“Plaintiffs’ unfair competition and tortious interference claims are not preempted by the UTSA to the extent they depend on the misappropriation of otherwise confidential or proprietary, but not trade secret, information as well as upon knowledge of Plaintiffs’ prospective business relationships.”)

The better reasoned view should be that confidential information is protectable under a contract and tort theory. A breach of non-disclosure of confidential information claim should be viable, but query whether “confidential information” of publically available information is really confidential and protectable or violative of section 16600. A tort theory of recovery for misuse of confidential information may be limited if the “confidential information” at issue is the same as the trade secrets and a trade secret misappropriation claim is alleged. Employers should continue to use non-disclosure of confidential information agreements despite the apparent ambiguity in law but tailor such agreement to protect non-public and valuable information and provide specificity and examples of genuine confidential information.

## **Developments Regarding the Computer Fraud and Abuse Act (CFAA)**

The CFAA originated in 1984 as a criminal statute designed to protect government and financial institution computers against “hackers.” In 1994, Congress added civil remedies to allow victims who suffer damages or loss resulting from a violation of the CFAA to maintain a civil action against violators and recover compensatory damages and injunctive relief. In 1996, the CFAA was further expanded to cover not only governmental computers but also any “protected computer,” which was defined to include any computer “used in interstate or foreign commerce or communications.”

In short, the CFAA allows a civil cause of action if a person “knowingly and with intent to defraud, accesses a protected computer without authorization, or [in excess of] authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value.” In order to qualify as a violation of Section 1030(a)(4), the thing of value obtained must be more than just the access to the computer, unless the value of the use amounts to or exceeds \$5,000. A company is not required to prove common law fraud to meet the fraud element of Section 1030(a)(4). Instead, it is sufficient to show wrongdoing by a person with respect to property rights by a dishonest method or scheme.

The CFAA has long stood as an employer-friendly statute because it does not require that the improperly accessed data or files be confidential or proprietary. This makes for a significant advantage over trade secret misappropriation, breach of duties of loyalty and

A decorative graphic on the left side of the page consists of overlapping geometric shapes in shades of blue and green.

confidence, and unfair competition claims. Employers can also recover their forensic expert fees and attorneys' fees spent on the investigation. See *Dental Health Prods. v. Ringo*, 2011 WL 3793961 (E.D. Wis. Aug. 25, 2011); *Animators at Law. v. Capital Legal Solutions*, 2011 WL 2022540 (E.D. Va. May 10, 2011).

However, the continued power of the CFAA to protect an employer's confidential information against employee misappropriation has recently been called into question. Starting with *United States v. Nosal*, 642 F. 3d 781 (2012), a circuit split has developed over whether the CFAA is applicable to both pure computer hacking and employee misappropriation. Currently, CFAA claims against employees are actionable in the following circuits:

- First Circuit: *EF Cultural Travel v. Explorica Inc.*, 274 F. 3d 577 (2001)
- Fifth Circuit: *U.S. v. John*, 597 F. 3d 263 (2010)
- Seventh Circuit: *International Airport Centers LLC v. Citrin*, 440 F. 3d 418 (2006)
- Eleventh Circuit: *U.S. v. Rodriguez*, 628 F. 3d 1258 (2011)

Such claims are generally not actionable in the following circuits:

- Fourth Circuit: *WEC Carolina Energy Solutions LLC v. Miller*, 2012 WL 3039213 (4th Cir. 2012)
- Ninth Circuit: *United States v. Nosal*, 642 F.3d 781 (2012)

The basis of this circuit split rests on each court's interpretation of "exceeds authorized access" or "without authorization." As judges in the Ninth and Fourth Circuits have pointed out, an employee could easily be exceeding authorized access to his employer's networks -- and thus committing a federal crime under the CFAA -- if he or she does something as simple as visit Facebook or shop online while at work, as such actions technically do violate many employers' computer use policies. On the other hand, the First, Fifth, Seventh, and Eleventh Circuits have not adopted a stricter construction of the CFAA and still permit employers to use it as a tool to combat employee misappropriation of company information on various theories, including violations of computer usage policies and breach of loyalty.

That said, all is not lost for California employers when it comes to the CFAA. Recently, in *Weingand v. Harland Financial Solutions*, 2012 U.S. Dist. LEXIS 84844 (N.D. Cal. June 19, 2012), the court distinguished the *Nosal* decision and indicated that the CFAA may still hold some power for employers in California. Specifically, the court allowed Harland to amend its counterclaim to include a CFAA claim against Weingand for accessing company files when Harland agreed to give Weingand post-termination access to his work computer only to copy his

A decorative graphic on the left side of the page, consisting of overlapping geometric shapes in shades of blue and green.

personal files. Despite this variety of interpretations both between and within circuits, there are presently no CFAA cases on the Supreme Court's docket that could resolve the current confusion and circuit split. There have been some proposals to amend the CFAA in Congress but none has gained any traction.

Taking into mind the current uncertainty surrounding the CFAA, human resource professionals, legal, and IT should consider preparing and implementing a strong, written policy regarding employees' access to the company's computers, the parameters and purpose of that access, what constitutes authorized access and what does not, and the consequences of abusing authority. As a threshold matter, a company needs to think critically about who gets access to what on its computer system and implement access policies accordingly. A company should also consider its protocols for issuing desktops, laptops, blackberries and other technology to new employees. It should also consider IT and HR protocols related to an exiting employee. Does your company inventory or image an employee's hard drive when he separates from employment? How does your company prepare a hard drive or laptop for a new employee? When an employee leaves your company, do IT and HR communicate about any valuable digital information the employee copied, transmitted, or deleted? Does your company carefully track the return of laptops, blackberries, and other portable devices capable of storing digital information? If your company allows a separating employee to retain laptops or such devices, what does it do to ensure that valuable information has been returned to the company? Creating and implementing a clear policy that answers all these questions can help protect a company from the volatility currently surrounding the CFAA.

## Social Media

Until recently, social media was far from the minds of employers and attorneys when it came to protecting trade secret and confidential information. Facebook, YouTube, and Twitter were websites that employees visited on their own time as an escape from work, not a forum for potential trade secret disclosure. However, as is so often the case with technology, the landscape of social media has changed rapidly over the past few years. Now, with so many businesses using social media as an advertising, networking, or idea sharing platform, the question of how to protect confidential or trade secret information in this age of social media has risen to the fore.

Given its rapid and somewhat haphazard growth, social media carries with it a set of issues that traditional avenues of trade secret disclosure do not. For instance, unlike the departing employee who knowingly takes with him a box of documents, the relaxed and non-professional environment of many social media sites could lead to employees disclosing confidential information without even realizing that they are doing so. Similarly, when an

employee departs, it is not always clear who will retain access and ownership to the information that a company has placed on a social media site.

With these issues in mind, what steps should an employer take to ensure that its confidential information remains adequately protected in this age of social media?

- First and most importantly, have a specific social media policy. Folding this policy into a general non-disclosure agreement is often not enough and leaves employers exposed.
- The policy should prohibit the disclosure of trade secret and confidential information by employees. However, take care that it is not overbroad and non-decipherable. The National Labor Relations Act section 7 protects an employee's right to engage in concerted activities, and social media policies that needlessly restrict what an employee can post on the internet are a sure way to run afoul of the National Labor Relations Board. The policy should provide a specific and comprehensible definition of trade secrets and confidential information and provide examples of trade secrets and confidential information and what disclosures are prohibited. You should also consider providing examples of what is permitted.
- Ensure that the policy is well-communicated and explained to employees. Training on the social media policy is a must.
- Make sure the policy stays current with the latest in social media developments. Some companies also include catch-all disclaimers. Some argue against such disclaimers because they argue that they don't work and they fail to encourage employers to have carefully thought-out policies and training that are understandable for employees.

A related issue involves the ownership of social media accounts. In the recent *PhoneDog v. Noah Kravitz* case, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011), one of the main issues concerns whether the employer or employee owned the subject Twitter account. The employee attempted to obtain an early dismissal of the employer's claims for ownership of the account. The court, however, found that these ownership issues lie "at the core of [the] lawsuit" and that, accordingly, an evidentiary record outside the pleading had to be developed before the court could resolve such fact-specific issues.

One federal court in Philadelphia recently ruled that an employer can claim ownership of its executive's LinkedIn profile. In *Eagle v. Morgan*, No. 11-4303, 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011), the court held that an employer may claim ownership of its former executive's LinkedIn connections where the employer required the executive to open and maintain the account, the executive advertised her and her employer's credentials and services on the account, and the employer had significant involvement in the creation, maintenance, operation,

A decorative graphic on the left side of the page consists of overlapping geometric shapes in blue, green, and white.

and monitoring of the account. The takeaway in *Eagle*, however, is that employers should consider getting more involved in their employees' social-networking activities that relate to company work and utilize contracts to assign ownership in company owned accounts.<sup>1</sup>

Social media can also be a powerful tool for employers when it comes to predicting and preparing for an employee's departure. Obvious, social media-based signs that an employee is thinking of leaving include:

- Any status updates in a social media profile where the employee announces or mentions their exit or new employment
- Any description of a new employer, business or venture in a social media profile
- A link to the new employer, business or venture posted in a social media profile
- General solicitations for business or leads
- An employee directly contacting or soliciting the employer's customers

That said, when it comes to using social media to predict employee behavior and demanding access to accounts, California employers must keep in mind the state's recent adoption of Assembly Bill 1844. Governor Brown signed this bill into law on September 17, 2012. At its core, this law "prohibit[s] an employer from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media." In other words, an employer may neither request nor require that an employee or an applicant divulge his or her personal social media account information. There are exclusions for workplace investigations. Given the newness of this law, it is not yet clear how it will affect trade secret protection. For additional details, see Seyfarth's recently released Management Alert attached in Appendix E.

---

<sup>1</sup> The Court also recently dismissed Plaintiff Eagle's Computer Fraud and Abuse Act claim for failure to prove damages regarding the alleged wrongful access of her LinkedIn account by her employer. *Eagle v. Morgan*, 2012 WL 4739436 (W.D. Pa. Oct. 4, 2012).

# Intellectual Property and Trade Secret Protection: Important Considerations

## You must act proactively using a preemptive plan.

1. All employees and consultants should be screened as part of the retention process.
  - a. All new hires must give you permission to obtain a credit report in order to comply with the Fair Credit Reporting Act.
  - b. Employees with access to confidential information and money must undergo more rigorous screening than other employees.
  - c. Officers and Directors should be subject to a due diligence investigation before coming aboard.
2. The company should do a non-periodic security assessment and IP audit which includes the following:
  - a. A review of its procedures used to protect its proprietary information;
  - b. A review of its procedures dealing with: (1) document disposal, (2) access to sensitive information, (3) remote access to company information, (4) system security, (5) patents and protection, (6) copyrights, (7) trade secrets and protection, and (8) trademark registration and protection;
  - c. A search of all company telephone numbers should be conducted in order to detect unauthorized modems;
  - d. Copy machines should be accessed by cards that identify the employee using the machine. Cards should be indexed to personal ID numbers to avoid card sharing and false claims that a card was borrowed; and
  - e. All IP should be catalogued. Trade secrets and proprietary information must be reasonably safeguarded in order to qualify for legal protection as proprietary information or as a trade secret. See Appendix F for an article regarding trade secret audits.
3. Conduct new employee orientations. Every employee should get written and oral instructions about the need to protect the company's IP and the need to avoid misusing IP belonging to others.

- 
- a. If an employee comes from a competitor, have counsel review their employment agreements with their prior employer and instruct the employee on compliance with their agreements. This meeting should be documented.
  - b. Execute proprietary information agreements. Written agreements should cover the business's code of business conduct and should include a statement whereby the employee commits to keeping the company's IP confidential. All allowable employment covenants should be included in this document.
  - d. Employees should receive annual training teaching them how to keep the company's IP confidential. This training should define what information is confidential and it should include instructions on the following: marking documents, document destruction, the maintenance of information, the use of laptops and e-mail, and the procedures used to safeguard trade secrets and other security procedures and policies. The training should include a reaffirmation of confidential obligations.
  - e. All employees should be notified that all information on the company's e-mail and voice mail and all work done on the company's computer system belong exclusively to the company and are subject to monitoring. Employees should be told that all such devices should be used for company business only (provided no personal use is permitted). If laptops are used and / or if remote access is allowed, employees should be specifically advised that these rules equally apply to these devices. It is advisable to give reminders of these policies as part of the sign-on process every time an employee signs onto the system. They should also be informed that it violates company policy to make intentional efforts to defeat company monitoring. Realistically, monitoring will catch some personal use, as this is very commonplace. The company should consider sending warning notices when excessive personal use is detected to avoid constructive waiver arguments. Computer access policies should be deployed and access should be circumscribed on an as needed access basis.
  - f. Companies should maintain a list of the company laptops and PDA's, and any remote access that is allowed. Periodic reviews to determine if anyone else is accessing the company's systems remotely should be done.
  - g. Consider maintaining computer backup tapes using the above guidelines, but seek advice of counsel because information contained on the tapes could be used to a litigation opponent's advantage in lawsuits.
  - i. Have security maintain after-hour sign-in logs for at least one year, and if the company's card access system records access by individual user (which it should), maintain these records for at least one year as well.

**If you suspect an employee is leaving to become a consultant or to join a competitor, you must act immediately.**

1. Review the employee's computer(s), including his or her laptop(s), before they leave to join a competitor or to become a consultant. Use forensic assistance. However, even forensic computer experts cannot recreate documents that are erased properly. In addition, even an unsophisticated user will be able to destroy documents so they cannot be recreated. Consequently, consider backing up or searching suspect employees' computer resources more often and more aggressively. Also image the hard drives of employees' computers before assigning them to other employees.
2. Review the employee's expense reports, cell phone records, and calls to and from their extension to determine if they are conducting company business or if they are instead preparing to exit with the company's clients, customers, or vendors.
3. Consider retaining the employee's refuse as a precautionary measure and check to see whether he or she is accessing information that he or she should not access in the ordinary course of business. A chain of custody should be maintained on all items collected.
4. Consider having an expert conduct an after-hours office search.
5. Some fax machines retain images of documents sent by them and can be downloaded on a periodic basis.
6. If circumstances demand it, do a nationwide corporation search to determine whether the employee is an officer or director of a competitive corporation.
7. If you determine that a key employee is leaving to join or form a competitive company, consult counsel and an investigative consultant before dismissing the employee. In some cases, you may choose to monitor the employee activities instead of firing them. You must balance the possible damage to the company and the morale of other employees against the need to gather evidence for possible future litigation. This is especially true when you believe that the employee may be conspiring with others, who have yet to be identified, to form a competitive company.

**Extra precautionary measures are appropriate if the departing employee had access to proprietary information or is leaving to join a competitor.**

1. When an employee gives notice, debrief the employee as to the status of his or her current work assignments, then consider taking the following precautionary steps on a reasonable time line that fits your company:
  - a. Reassign the employee's projects or name an interim replacement.

- 
- b. Take custody of all property belonging to the company, including documents, handbooks, data, logs, printouts, notes, calendars, laptops, cell phones, rolodexes, and software. If necessary, consider sending someone to his or her home to retrieve the company property.
  - c. Eliminate the employee's access to the company's systems, including his or her remote access.
  - d. Require everyone in the employee's group and / or other employees, who are friendly with the departing employee, to change their passwords. Also, consider reviewing the scope of his or her remaining friends' access to be sure that it is necessary for their business functions. This is also a good time to remind, either in a group or in writing, remaining employees of their obligations to the company.
  - e. Collect security passes, keys, and the like, and only allow future access while accompanied. Also, notify building security of the employee's departure, and provide a photo ID to lobby or gate guards.
  - f. Have the employee remove all personal items from his or her office or work area under supervision of someone else. A record should be kept of all items removed.
2. Although there are often extenuating circumstances that make it difficult to conduct an exit interview, try to conduct one as soon as possible. Prepare for the interview as follows:
    - a. Review the employee's employment file including all agreements the employee has with the company.
    - b. Review the employee's job description with his or her supervisor to determine whether the employee had access to Company proprietary information during his or her employment. Also, determine whether the employee has any computers, documents, lists, or other confidential materials belonging to the company.
3. Conducting an Exit Interview
    - a. Have the employee specifically identify what trade secrets, or other types of proprietary information he or she has had access to during his or her employment. Have the employee certify that he or she has returned all such information and that he or she has identified all systems to which they have password access.
    - b. Review the employee's continuing obligations to the company in writing. These should include his or her common law obligations as well as contractual obligations. Have the employee certify that he or she understands and will abide by his or her obligations.

- 
- c. Ask the employee to list all items / materials belonging to the company that he or she has in his or her possession. Later, once the items have been secured, have the employee certify that he or she has returned all of the items and has not made copies or given this information to unauthorized third parties.
  - d. Explain to the employee that the company will be sending a letter to his or her new employer explaining his or her continuing obligations to the company. This letter should be carefully drafted so as not to create liability for the company. In most cases, it should be drafted and signed by counsel.
  - e. The employee should be sent a document which specifically states all of his or her post-employment obligations to the company. It should also incorporate all relevant information derived from the exit interview, such as documents and information, which were returned to the company, and a listing of proprietary information, which must be protected. This letter too should be drafted by and signed by counsel, and it should include the name of a contact person if the employee has further questions.
4. In-House “Investigation”
    - a. Conduct an informal “investigation” into the employee’s future plans, and past activities.
      - (i). Seek to determine if the employee has accurately disclosed his or her future plans.
      - (ii). Seek to determine whether the employee has been recruiting other employees to join his or her new employer.

**If litigation is anticipated, you should take these precautionary steps immediately.**

1. Secure and establish a chain of custody for all items returned by the departing employee, including his or her laptop computer, desk computer, USB devices, notes, rolodexes, and calendars.
2. Secure and maintain a chain of custody of the employee’s office and the items in that office until it is searched by an independent party.
3. Retain outside counsel to investigate the departure and have outside counsel secure the services of an investigations firm with a good reputation.
4. If the employee is computer savvy, do an immediate search of the internet for material posted to social media sites. Be sure to include LinkedIn and other social media.

**An in-depth investigation may be necessary. An in-depth investigation may include all of the steps already detailed but may also include:**

1. Resume Check - A complete resume verification should be done if it was not done as a condition of employment;
2. Covert tracking of the departed employee's contact with current employees, company clients or customers;
3. Covert collection of the employee's refuse;
4. A complete analysis of the departed employee's expense reports and telephone records (i.e. his or her company cell phone and calls to and from his or her office extensions);
5. A search of the employee's office and that of his or her assistant (if it was not done before the employee departed);
6. Pre-textual overtures to the employee if he or she has established a competing concern or has joined a competitor. This can only be done before litigation is initiated and before the employee retains counsel;
7. Internet / social media monitoring (but do not violate wiretap / privacy laws);
8. A complete public records search seeking to obtain information regarding financial condition and legal violations;
9. Obtaining information from sources within the relevant industry; and
10. Overt interviews with employees.

## Departing Employee Issues to Consider

**While not exhaustive, this list provides several issues to consider when an employee leaves your company**

1. Review and retain all records and files in the departing employee's control.
2. Collect all company property issued to the departing employee (laptops, cell phones, Blackberries, flash memory drives / devices, etc).
3. Inspect the departing employee's office and files to ensure nothing is missing.
4. Photograph departing employee's office to preserve record of its state at the time the employee left.
5. Ensure ongoing access by the departing employee (remotely or otherwise) to information, documents, computer servers, offices, etc. is denied.
6. Determine whether the departing employee's computer needs to be preserved / imaged.
7. Confirm that no unauthorized information, file, document, or e-mail transfers have occurred.
8. Review recent received, sent, archived, and trash e-mail folders for unusual or unauthorized use.
9. Review computer access and print logs to determine if there has been any unusual or unauthorized use.
10. Provide the departing employee with any previously signed agreements pertaining to confidential, proprietary, and/or trade secret information.
11. Confirm return by the departing employee of all confidential, proprietary, and/or trade secret information.
12. Ascertain why the departing employee is leaving and where he or she is going.
13. Request that the departing employee sign a statement acknowledging that he or she understands what constitutes confidential, proprietary, and/or trade secret information belonging to the company.
14. Request that the departing employee sign a statement acknowledging that he or she no longer has access in any manner (electronic, dial-in, or otherwise) to any company e-mail,

computer system, and / or network, materials, information, documents/writings, or offices belonging to the company.

15. Request that the departing employee sign a statement acknowledging that he or she has not made, forwarded, or retained originals or copies of any document / writing, e-mail, text message, instant message, any other electronic or voicemail messages or information of any kind received at or sent from the company by any means, including, but not limited to, computer, wireless device, facsimile, or telephone.
16. Request that the departing employee execute an agreement acknowledging departing employee's continuing obligations to the company.
17. Ensure that the company has obtained social media passwords and user information from the departing employee for company owned accounts.



# Appendix A

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

SRICOM, INC.,	)	Case No.: 12-CV-00904-LHK
	)	
Plaintiff,	)	ORDER GRANTING IN PART AND
	)	DENYING IN PART DEFENDANTS'
v.	)	MOTION TO DISMISS
	)	
EBISLOGIC, INC.; ASTERIX CONSULTING,	)	
INC.; ELITE TECHNOLOGY PARTNERS,	)	
INC.; and VMWARE, INC.	)	
	)	
Defendants.	)	
	)	

Before the Court is the motion to dismiss Plaintiff's Complaint filed by Defendants eBisLogic Inc. (eBisLogic), Asterix Consulting, Inc. (Asterix), and Elite Technology Partners, LLC (ETP) (collectively "Defendants"). ECF No. 9. Also before the Court is Defendants' motion to strike portions of the Complaint, and Defendants' motion for a more definite statement. For the reasons set forth below, the Court GRANTS in part and DENIES in part Defendants' motion to dismiss with leave to amend. The Court DENIES Defendants' motion to strike and motion for a more definite statement as moot.

**I. BACKGROUND**

Unless otherwise noted, the following allegations are taken from the Complaint and are presumed to be true for purposes of ruling on Defendants' Motion to Dismiss. Plaintiff SriCom and Defendants eBisLgic, Asterix, and ETP are all in the business of providing highly skilled

1 workers and consultants to technology companies. Compl. ¶ 12. The events at issue in this lawsuit  
2 arose from a multi-layered arrangement whereby Asterix and ETP provided consultants to SriCom,  
3 who provided them to eBisLogic, who provided them to its client, VMware. *Id.* at ¶¶ 13-15.

4 On September 7, 2010, eBisLogic and SriCom entered into a contract whereby SriCom  
5 agreed to find consultants for eBisLogic’s clients. *Id.* at ¶ 13. Subsequently, SriCom engaged and  
6 entered into contracts with ETP and Asterix to locate the consultants that SriCom would provide to  
7 eBisLogic. *Id.* at ¶¶ 14, 15. Asterix then provided one consultant to SriCom, *id.* at ¶ 20, and ETP  
8 provided two. *Id.* at ¶¶ 18-19. SriCom identified one additional consultant on its own. *Id.* at ¶ 21.

9 VMware, the company that ultimately needed the consultants, then entered into a “General  
10 Services Agreement” with eBisLogic for the provision of these four consultants to perform work at  
11 VMware. *Id.* at ¶ 16. The consultants commenced work at VMware some time around September  
12 9, 2010. *Id.* at ¶ 20.

13 The trouble began on April 28, 2011, when eBisLogic presented SriCom with a “revised  
14 master services agreement,”<sup>1</sup> which contained a set of pass-down requirements for consultants  
15 placed at VMware. *Id.* SriCom refused to accept the new terms regarding the pass-down  
16 requirements, and informed eBisLogic that SriCom’s consultants would be ceasing their work for  
17 VMware through eBisLogic, under the terms of the “master services agreement.”<sup>2</sup> *Id.* at ¶¶ 24, 25.  
18 SriCom also informed eBisLogic that under the terms of their existing contract, neither VMware  
19 nor any third party could solicit the SriCom consultants; the consultants could not continue their  
20 work at VMware past May 15, 2011; and neither VMware nor eBisLogic could hire the consultants  
21 directly until December 2012. *Id.* at ¶ 25.

22 eBisLogic, Aserix, and ETP then terminated their relationships with SriCom and requested  
23 that SriCom allow the consultants to remain at VMware, *id.* at ¶¶ 26-28, but SriCom refused. *Id.* at  
24  
25

---

26 <sup>1</sup> The Complaint does not specify which contract this document purported to revise, but it appears  
27 that this April 28, 2011 contract was a proposed revision to the September 7, 2010  
SriCom/eBisLogic contract.

28 <sup>2</sup> Again, the Complaint is unclear on which contract SriCom was affirming in this communication,  
but it appears to be the September 7, 2010 SriCom/eBisLogic contract.

1 ¶ 28. The consultants have continued to work at VMware through eBisLogic, without involving  
2 SriCom. *Id.* at ¶ 36.

3 SriCom filed this lawsuit in state court on December 28, 2011, asserting six causes of  
4 action: (1) breach of contract against eBisLogic, (2) breach of contract against Asterix and ETP, (3)  
5 breach of the implied covenant of good faith and fair dealing against eBisLogic, Asterix and ETP,  
6 (4) fraud against eBisLogic, (5) unfair competition (Cal. Bus. & Prof. Code § 17200) against  
7 eBisLogic, and (6) intentional interference with contract relations against VMware. Asterix filed a  
8 Notice of Removal on February 23, 2012, ECF No. 1, and the case was reassigned to the  
9 undersigned judge on February 29, 2012. ECF No. 7. Defendants filed their motion to dismiss  
10 claims 1-5 (“Mot. to Dismiss”) on March 1, 2012. ECF No. 6. Plaintiff filed its opposition  
11 (“Opp.”) on March 15, 2012, and Defendants filed a reply (“Reply”) on March 22, 2012. Plaintiff  
12 filed a voluntary dismissal of the sixth claim, against VMware, on September 6, 2012. ECF No.  
13 24.

## 14 II. LEGAL STANDARD

15 A motion to dismiss for failure to state a claim under Rule 12(b)(6) tests the legal  
16 sufficiency of a complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). In considering  
17 whether the complaint is sufficient to state a claim, the court must accept as true all of the factual  
18 allegations contained in the complaint. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). However, the  
19 court need not accept as true “allegations that contradict matters properly subject to judicial notice  
20 or by exhibit” or “allegations that are merely conclusory, unwarranted deductions of fact, or  
21 unreasonable inferences.” *St. Clare v. Gilead Scis., Inc.*, 536 F.3d 1049, 1055 (9th Cir. 2008).  
22 While a complaint need not provide detailed factual allegations, it “must contain sufficient factual  
23 matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Iqbal*, 556 U.S. at  
24 678 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially  
25 plausible when it “allows the court to draw the reasonable inference that the defendant is liable for  
26 the misconduct alleged.” *Id.*

27 A complaint alleging fraud must “state with particularity the circumstances constituting  
28 fraud.” Fed. R. Civ. P. 9(b). Allegations of fraud must be stated with “specificity including an

1 account of the ‘time, place, and specific content of the false representations as well as the identities  
2 of the parties to the misrepresentations.’” *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007)  
3 (quoting *Edwards v. Marin Park, Inc.*, 356 F.3d 1058, 1066 (9th Cir. 2004)). To survive a motion  
4 to dismiss, “‘allegations of fraud must be specific enough to give defendants notice of the  
5 particular misconduct which is alleged to constitute the fraud charged so that they can defend  
6 against the charge and not just deny that they have done anything wrong.’” *Id.* (quoting *Bly-Magee*  
7 *v. California*, 236 F.3d 1014, 1019 (9th Cir. 2001)).

### 8 **III. ANALYSIS**

#### 9 **A. SriCom’s Capacity to Sue**

10 A corporation that is not incorporated in California is required to obtain a certificate of  
11 qualification from the Secretary of State before transacting business in California. Cal. Corp. Code  
12 § 2105(a). A corporation that fails to do so “shall not maintain any action or proceeding upon any  
13 intrastate business so transacted in any court of this state, commenced prior to compliance with  
14 Section 2105, until it has complied with the provisions thereof,” paid the requisite fees, and “has  
15 filed with the clerk of the court in which the action is pending receipts showing the payment of the  
16 fees and penalty and all franchise taxes. . . .” Cal. Corp. Code § 2203(c).

17 Defendants argue that SriCom cannot maintain this action under California law on these  
18 grounds. Mot. to Dismiss at 5. However, SriCom has now filed both its Certificate of  
19 Qualification and its receipts for payment of the fee for that certificate and its required franchise  
20 taxes. *See* Declaration of Chung S. Poon in Support of Plaintiff’s Opposition to Defendants’  
21 Motion to Dismiss Plaintiff’s Complaint, ECF No. 11, Exhibits B and C. Defendants have  
22 suggested that Plaintiff is required by statute to certify compliance with California Corporations  
23 Code § 2203(c). That section, however, requires only that the corporation file receipts indicating  
24 payment, which SriCom has done. Accordingly, the Court finds that SriCom does have capacity to  
25 bring this action.

#### 26 **B. Breach of Contract Claim Against eBisLogic**

27 To state a claim for breach of contract under California law, a plaintiff must plead facts  
28 establishing the following elements: “(1) existence of the contract; (2) plaintiff’s performance or

1 excuse for nonperformance; (3) defendant’s breach; and (4) damages to plaintiff as a result of the  
2 breach.” *CDF Firefighters v. Maldonado*, 158 Cal. App. 4th 1226, 1239, 70 Cal. Rptr. 3d 667  
3 (2008). Under California law, “a contract requires parties capable of consent, the consent of those  
4 parties, a lawful object, and sufficient consideration.” *ASP Props. Grp. v. Fard, Inc.*, 133 Cal.  
5 App. 4th 1257, 1268–69 (2005) (citing Cal. Civ. Code § 1550). In addition, for a contract “to be  
6 enforceable, a promise must be definite enough that a court can determine the scope of the duty[,]  
7 and the limits of performance must be sufficiently defined to provide a rational basis for the  
8 assessment of damages.” *Bustamante v. Intuit, Inc.*, 141 Cal. App. 4th 199, 209 (2006) (quoting  
9 *Ladas v. Cal. State Auto. Ass’n*, 19 Cal. App. 4th 761, 770 (1993)).

10 The contract at issue here is the September 7, 2010 contract between SriCom and  
11 eBisLogic. Compl. ¶ 30. That contract contains a provision preventing eBisLogic from soliciting  
12 or hiring SriCom employees who were “performing services through EBISLOGIC, INC. for  
13 Clients” for a period of one year. *Id.* at ¶ 31.

14 Defendants argue that SriCom’s claim must fail because SriCom has not pled facts showing  
15 the existence of a valid and enforceable contract. Mot. to Dismiss at 7. Specifically, Defendants  
16 argue that the contract purports to prevent eBisLogic from directly employing the consultants  
17 SriCom had provided, and is invalid and unenforceable under California Business and Professions  
18 Code § 16600.

19 Section 16600 states that “every contract by which anyone is restrained from engaging in a  
20 lawful profession, trade, or business of any kind is to that extent void,” subject to statutory  
21 exceptions not relevant here. Cal. Bus. & Profs. Code § 16600; *see also* Cal. Bus. & Profs. Code §  
22 16601–07 (codifying exceptions for non-compete agreements associated with the sale or  
23 dissolution of certain businesses and addressing other special circumstances). As Defendants point  
24 out, nonsolicitation and no-hire agreements are generally void under this provision. *See, e.g., VL*  
25 *Systems, Inc. v. Unisen, Inc.*, 152 Cal. App. 4th 708 (2007); *Thomas Weisel Partners LLC v. BNP*  
26 *Paribas*, C 07-6198 MHP, 2010 WL 546497 (N.D. Cal. Feb. 10, 2010), at \*5-6. In its recent  
27 decision in *Edwards v. Arthur Andersen LLP*, 44 Cal.4th 937, (2008), the California Supreme  
28 Court confirmed the continued viability and breadth of Section 16600. The Court explained that by

1 enacting Section 16600, the California legislature intended to further “a settled legislative policy in  
2 favor of open competition and employee mobility.” *Edwards*, 44 Cal.4th at 946. Thus, Section  
3 16600 is a broad prohibition on “every contract by which anyone is restrained from engaging in a  
4 lawful profession, trade, or business of any kind.” Cal. Bus. & Profs. Code § 16600.

5 This broad prohibition has, however, been occasionally subjected to specific exceptions. In  
6 particular, SriCom relies on *Webb v. West Side District Hospital*, 193 Cal. App. 3d 946 (1983), in  
7 which the Court held that an agreement requiring a hospital to pay an additional fee if it directly  
8 hired any doctors originally placed there by a staffing agent was not void under Section 16600. In  
9 *Webb*, the Court noted that the staffing agent’s “economic interest was . . . valuable and  
10 protectable: without recoupment of the recruitment expenses he had incurred, [the consultant]  
11 became vulnerable to unfair exploitation of his labors.” *Id.* at 954. SriCom argues that *Webb*  
12 created an exception to Section 16600 where staffing agencies are involved.

13 Defendants rely on *Edwards* for the proposition that even if that were once a generally  
14 applicable exception, now, “[n]oncompetition agreements are invalid under section 16600 in  
15 California even if narrowly drawn, unless they fall within the applicable *statutory* exceptions.” *Id.*  
16 at 955 (emphasis added). Since the *Webb* exception was judicially created, Defendants argue, it  
17 cannot continue to exist post-*Edwards*. Reply at 2. The contract term at issue here, however, is not  
18 a noncompetition agreement like that discussed in *Edwards*, but rather a nonsolicitation and no-hire  
19 provision. *See Thomas Weisel Partners LLC v. BNP Paribas*, C 07-6198 MHP, 2010 WL 546497  
20 (N.D. Cal. Feb. 10, 2010) (distinguishing among five separate types of provisions potentially  
21 implicating Section 16600). The plain language of *Edwards*, then, does not necessarily eliminate  
22 the exception recognized in *Webb*.

23 The reasoning in *Edwards*, however, forecloses continued reliance on *Webb*. Specifically,  
24 *Edwards* rejects the contention that Section 16600 “embrace[s] the rule of reasonableness in  
25 evaluating competitive restraints.” 44 Cal. 4th at 947. *Webb* is premised on the notion that  
26 restraints on direct hiring in the staffing agent context were unreasonable when weighed “by  
27 balancing, in the light of all the circumstances, the respective importance to society and the parties  
28

1 of protecting the activities interfered with on the one hand and permitting the interference on the  
2 other.” *Webb*, 144 Cal. App. 3d at 951. Without the rule of reasonableness, *Webb* cannot stand.

3 Thus, the question here is whether, under the literal terms of the statute, “anyone is  
4 restrained from engaging in a lawful profession, trade, or business of any kind.” Cal. Bus. & Profs.  
5 Code § 16600. The contract at issue here unequivocally purports to restrain the consultants  
6 SriCom had placed with eBisLogic from working directly for eBisLogic. Accordingly, Section  
7 16600 voids the provision. Because SriCom’s claim is based entirely on this provision,<sup>3</sup> SriCom  
8 has not alleged the existence of a valid and enforceable contract. Defendants’ motion to dismiss is  
9 GRANTED.

### 10 C. Breach of Contract Claim Against Asterix and ETP

11 SriCom asserts breaches of two distinct contract provisions: breach of a non-competition  
12 clause in the contracts SriCom had with Asterix and ETP, and breach of a confidentiality clause in  
13 the same contracts.<sup>4</sup>

#### 14 Noncompetition Clause

15 SriCom has alleged that its contracts with Asterix and ETP contained a clause that  
16 “prevents Asterix and ETP and its employees from providing, developing, or implementing  
17 software solutions, systems, integration services or information technology service for any client or  
18 entity which it has provided services in any capacity on behalf of SriCom.” Compl. ¶ 45.

19 As established above, to state a claim for breach of contract, a plaintiff must allege the  
20 existence of a valid and enforceable contract. Section 16600, read in light of *Edwards*, is a clear  
21 prohibition on any noncompetition clause that does not fit into one of the statutory exceptions.

22 \_\_\_\_\_  
23 <sup>3</sup> To the extent that SriCom intends to assert breach of any other term of this contract, SriCom has  
24 failed to identify the relevant contract provision or the act that constitutes breach. The only  
25 contract term discussed in the Complaint is the nonsolicitation/no-hire clause. *See* Compl. ¶¶ 31,  
26 38. SriCom has not specified whether its claim that eBisLogic “refuses to then pay the full amount  
27 owed,” *id.* at ¶ 32, refers to what is owed under the invalid noncompetition clause, or owed under  
28 some other part of the contract. Accordingly, SriCom has not stated a claim for violation of any  
other contract term.

<sup>4</sup> The complaint does not specify whether the two contracts—the SriCom/Asterix contract and the  
SriCom/ETP contract—were identical. They are, however, described in identical terms. Compl. ¶¶  
14-15. Accordingly, the Court will assume that Plaintiff is alleging that each of the two identical  
contracts was breached in two ways: a non-competition clause breach and a confidentiality clause  
breach.

1 SriCom has not, and cannot, argue that any of the statutory exceptions apply here. As the clause is  
2 undeniably a noncompetition clause that restrains employees from engaging in a lawful profession,  
3 trade, or business, it too is void under Section 16600. Accordingly, SriCom has not alleged the  
4 existence of a valid and enforceable contract, and Defendants’ motion to dismiss this claim is  
5 GRANTED as to the noncompetition clause.

6 Confidentiality Clause

7 SriCom has alleged that its contracts with Asterix and ETP contain a clause that requires all  
8 parties to “regard and preserve as confidential any and all informed [sic] shared by each other” and  
9 acknowledges that “any information received from BUYER [i.e. SriCom] or its clients is the sole  
10 property of BUYER of [sic] its clients as the case may be, and SELLER [i.e. ETP and Asterix] or  
11 its representatives, will not utilize such information except in the performance of this Agreement.”  
12 Compl. ¶ 50. This allegation is sufficient to satisfy the first element of the breach of contract  
13 claim, the existence of a valid contract. SriCom has also alleged that it has fully performed under  
14 the contract, in satisfaction of the second requirement. *Id.* at ¶ 53.

15 The third requirement is that Plaintiff must allege Defendant’s breach. Here, SriCom has  
16 asserted that Asterix and ETP revealed “customer information, employee information, and pricing  
17 information.” *Id.* at ¶ 51. However, the Complaint does not allege any facts concerning what  
18 specific information was revealed, when, how, or to whom it was revealed, or whether or how  
19 Asterix and ETP used this information. A complaint does not suffice “if it tenders “naked  
20 assertion[s]” devoid of “further factual enhancement.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)  
21 (citing *Twombly*, 550 U.S. at 557). SriCom’s allegations amount to a conclusory assertion that  
22 there has been a breach, with no factual support. Though SriCom attempts to provide more facts in  
23 its opposition, “[a]llegations raised for the first time in the briefing are not considered in  
24 determining the sufficiency of the complaint. *Nat’l Union Fire Ins. Co. of Pittsburg, PA v. Res.*  
25 *Dev. Services, Inc.*, 5:10-CV-01324-JF PVT, 2010 WL 4774929 (N.D. Cal. Nov. 16, 2010). The  
26 Complaint as filed does not allege sufficient facts to state a claim for breach of the confidentiality  
27 clause. Defendants’ motion is GRANTED as to the confidentiality clause.

28 **D. Breach of Covenant of Good Faith and Fair Dealing**

1 California law recognizes that “every contract contains an implied covenant of good faith  
2 and fair dealing that neither party will do anything which will injure the right of the other to receive  
3 the benefits of the agreement.” *Wolf v. Walt Disney Pictures and Television*, 162 Cal.App.4th  
4 1107, 1120 (2008). Breach of an express contractual provision is not a necessary prerequisite to a  
5 claim for breach of the implied covenant. *Brehm v. 21st Century Ins. Co.*, 166 Cal.App.4th 1225,  
6 1235–36 (2008). Rather, “the covenant is implied as a supplement to the express contractual  
7 covenants, to prevent a contracting party from engaging in conduct which (while not technically  
8 transgressing the express covenants) frustrates the other party's rights to the benefits of the  
9 contract.” *Love v. Fire Ins. Exchange*, 221 Cal.App.3d 1136, 1153 (1990). “The precise nature and  
10 extent of the duty imposed will depend on the contractual purposes.” *Egan v. Mutual of Omaha*  
11 *Insurance Co.*, 24 Cal. 3d 809, 818 (1979).

12 Based on this legal framework and the facts alleged in its Complaint, SriCom has stated a  
13 plausible claim for breach of the implied covenant of good faith and fair dealing. SriCom has  
14 alleged that it had written contracts with eBisLogic, ETP, and Asterix. Compl. ¶¶ 13-15.  
15 Therefore, Defendants had a duty to execute the contracts’ purposes in good faith. The exact  
16 nature and scope of this duty is a factual inquiry and is based on the purposes of the contracts, the  
17 express terms of the contracts, and the reasonable expectations of all parties.

18 SriCom has alleged that Defendants acted to deprive SriCom of the benefits under its  
19 contracts by directly hiring the consultants SriCom had placed, without compensating SriCom. *Id.*  
20 at ¶ 58. Such conduct could violate the implied covenant of good faith and fair dealing even if it  
21 does not violate the literal terms of valid contracts, as it could frustrate SriCom’s rights to the  
22 benefits for which it contracted under terms of the contracts that remain valid, specifically,  
23 continued compensation for the consultants SriCom identified for placement at VMware. Even  
24 though the facts may eventually show that Defendants did not violate the implied covenant of good  
25 faith and fair dealing, SriCom’s Complaint contains sufficient facts to state such a claim at this  
26 stage of the litigation. Defendants’ motion to dismiss this claim is DENIED.

27 **E. Fraud**

1 To state a cause of action for fraud, a plaintiff must allege “(a) misrepresentation (false  
2 representation, concealment, or nondisclosure); (b) knowledge of falsity (or ‘scienter’); (c) intent to  
3 defraud, i.e., to induce reliance; (d) justifiable reliance; and (e) resulting damage.” *Engalla v.*  
4 *Permanente Med. Group, Inc.*, 15 Cal. 4th 951, 974 (1997). This cause of action must meet Rule  
5 9(b)’s heightened pleading requirements. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir.  
6 2009). Rule 9(b) demands that “[a]verments of fraud must be accompanied by ‘the who, what,  
7 when, where, and how’ of the misconduct charged. A plaintiff must set forth more than the neutral  
8 facts necessary to identify the transaction. The plaintiff must set forth what is false or misleading  
9 about a statement, and why it is false.” *Vess v. Ciba–Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th  
10 Cir. 2003) (internal quotation marks and citation omitted).

11 Here, SriCom has alleged that eBisLogic made a request for confidential pricing  
12 information from SriCom on March 12, 2011, claiming it was for one purpose when actually it was  
13 for another. Compl. ¶¶ 64, 65. SriCom has alleged that eBisLogic indicated that VMware had  
14 requested the information, when in fact, it was eBisLogic that wanted it for the purpose of  
15 depriving SriCom of its share of the profit from placing the consultants. SriCom has identified  
16 what was misleading and why, when the misrepresentation was made, and in what context. *Id.* at  
17 ¶¶ 63, 64. These allegations are sufficient to satisfy the misrepresentation and scienter  
18 requirements for a fraud claim.

19 SriCom has further alleged that eBisLogic was “seeking to find a way around SriCom in  
20 order to directly hire SriCom’s consultants.” *Id.* at ¶ 66. This allegation suffices to establish intent  
21 to defraud. SriCom also alleges that “[h]ad plaintiff known the actual facts it would not have taken  
22 such action. Plaintiff’s reliance on defendant eBisLogic’s representations was justified because of  
23 the general service agreement the parties had entered into.” *Id.* at ¶ 69. These allegations satisfy  
24 the justifiable reliance requirement for a fraud claim. Finally, SriCom has alleged resulting  
25 damage. *Id.* at ¶ 70.

26 In sum, SriCom has alleged facts establishing all five of the required elements for fraud.  
27 Further, SriCom has identified the “who, what, where, when, and why” of the specific misconduct  
28

1 charged. Accordingly, SriCom has stated, with sufficient particularity, a claim for fraud, and  
2 Defendants’ motion to dismiss this claim is DENIED.

3 **F. Unfair Competition**

4 California’s Unfair Competition Law (“UCL”) prohibits “any unlawful, unfair or fraudulent  
5 business act or practice and unfair, deceptive, untrue or misleading advertising.” Cal. Bus. & Prof.  
6 Code § 17200. Accordingly, “[a]n act can be alleged to violate any or all of the three prongs of the  
7 UCL—unlawful, unfair, or fraudulent.” *Berryman v. Merit Prop. Mgmt., Inc.*, 152 Cal. App. 4th  
8 1544, 1554 (2007).

9 Defendants argue that the UCL requires a plaintiff to make a claim for either a  
10 restitutionary or an injunctive remedy. Mot. to Dismiss at 11. Defendants are correct that  
11 California law requires the dismissal of a complaint under the UCL that fails to demand either  
12 injunctive or restitutionary relief. *See Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4<sup>th</sup>  
13 1134, 1152 (2003). Thus, the question here is whether the relief SriCom has requested can be  
14 categorized as restitutionary, in which case SriCom may have stated a claim, or whether, instead,  
15 SriCom is seeking damages or disgorgement of Defendants’ profits, neither of which would state a  
16 claim for relief under the UCL.

17 Under the UCL, “the concept of restoration or restitution . . . is not limited only to the  
18 return of money or property that was once in the possession of that person. Instead, restitution is  
19 broad enough to allow a plaintiff to recover money or property in which he or she has a vested  
20 interest.” *Lozano v. AT & T Wireless Servs. Inc.*, 504 F.3d 718, 733–34 (9th Cir. 2007) (quoting  
21 *Juarez v. Arcadia Fin., Ltd.*, 152 Cal.App.4th 889 (2007)). For example, a plaintiff has a vested  
22 interest in unpaid wages and therefore may state a restitution claim under the UCL to recover such  
23 lost money or property. *See Cortez v. Purolator Air Filtration Prods. Co.*, 23 Cal.4th 163, 177–78  
24 (2000). The California Supreme Court has made clear, however, that a mere “expectation interest”  
25 is not a “vested interest” for purposes of stating a claim for restitution under the UCL. *See Pineda*  
26 *v. Bank of America*, 50 Cal.4th 1389, 1401–02 (2010).

27 SriCom’s request for relief under the UCL states that “[a]s a direct and proximate result of  
28 the foregoing conduct, defendants have been unjustly enriched. Plaintiff SriCom is entitled to

1 \$105,714, plus interest, and an uncertain sum of fees it is owed from the consultants continued  
2 work for VMware.” Compl. ¶ 78. SriCom has not explained why it believes it is entitled to the  
3 stated amount—whether it is the amount of money Defendants allegedly made by illegally  
4 employing the consultants, or whether it is the amount owed under one of the contracts at issue for  
5 work already performed, or some other source entirely. Further, SriCom has not specified from  
6 whom it is allegedly owed fees for the consultants’ continued work, whether its claim is for pre- or  
7 post-termination work, and whether it had a vested interest in those fees under any of its contracts  
8 with any party, or rather had simply been hoping to earn those amounts under its contracts in the  
9 future. Without further allegations concerning the specific relief requested, the Court cannot  
10 determine whether SriCom is claiming money in which it had a vested interest, a mere expectation  
11 interest, or no actual interest at all. Thus, SriCom has not sufficiently stated a claim for relief  
12 under the UCL, and Defendants’ motion to dismiss is GRANTED.

### 13 **G. Leave to Amend**

14 Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend “shall be freely  
15 given when justice so requires,” bearing in mind “the underlying purpose of Rule 15 to facilitate  
16 decision on the merits, rather than on the pleadings or technicalities.” *Lopez v. Smith*, 203 F.3d  
17 1122, 1127, 1140 (9th Cir. 2000) (en banc) (internal quotation marks and alterations omitted).  
18 When dismissing a complaint for failure to state a claim, “a district court should grant leave to  
19 amend even if no request to amend the pleading was made, unless it determines that the pleading  
20 could not possibly be cured by the allegation of other facts.” *Id.* at 1127 (quoting *Doe v. United*  
21 *States*, 58 F.3d 494, 497 (9th Cir. 1995)). If a court grants a motion to dismiss, leave to amend  
22 should be granted unless the pleading could not possibly be cured by the allegation of other facts.  
23 *Lopez v. Smith*, 203 F.3d 1122, 1130 (9th Cir. 2000). If amendment would be futile, however, a  
24 dismissal may be ordered with prejudice. *Dumas v. Kipp*, 90 F.3d 386, 393 (9th Cir. 1996).  
25 Similarly, leave to amend may be denied if allowing amendment would unduly prejudice the  
26 opposing party, cause undue delay, or if the moving party has acted in bad faith. *Leadsinger, Inc.*  
27 *v. BMG Music Publ’g.*, 512 F.3d 522, 532 (9th Cir. 2008).  
28

1 SriCom's claims fail because SriCom has not alleged sufficient facts to state a claim for  
2 each of the causes of action being dismissed. Further and more detailed allegations could  
3 potentially cure the defects in each of SriCom's dismissed claims.<sup>5</sup> Accordingly, SriCom's claims  
4 for breach of contract against eBisLogic, Asterix, and ETP, and for violation of the UCL are  
5 dismissed with leave to amend.

6 **III. CONCLUSION**

7 For the foregoing reasons, the Court GRANTS Defendants' motion to dismiss with leave to  
8 amend as to SriCom's breach of contract claims against eBisLogic, Asterix, and ETP, and UCL  
9 claim, and DENIES Defendants' motion as to SriCom's breach of the covenant of good faith and  
10 fair dealing and fraud claims. The Court also denies as moot Defendants' motion to strike and  
11 motion for a more definite statement, as they pertain only to the breach of contract claims, which  
12 have been dismissed. Plaintiff shall file an amended complaint, if any, within 21 days of this  
13 Order. Plaintiff may not add new claims or parties absent a stipulation of the parties or a Court  
14 Order pursuant to Fed. R. Civ. P. 15(a)(2). If Plaintiff fails to timely file an amended complaint or  
15 fails to cure the deficiencies identified in this Order, Plaintiff's claims will be dismissed with  
16 prejudice.

17 **IT IS SO ORDERED.**

18 Dated: September 13, 2012

19   
20 LUCY H. KOH  
21 United States District Judge

22  
23  
24  
25  
26  
27 <sup>5</sup> Though of course further factual allegations will not state a claim under contract terms that are  
28 void under California law, each of the contracts contained additional terms that may be valid, and  
under which SriCom may have been attempting to allege a violation. Accordingly, SriCom may  
still allege facts stating a claim for breach of these contracts, and amendment will not be futile.



# Appendix B

# Management Alert



## California Court Rules That Non-Competition Agreement Contained In Employment Agreement Is Unenforceable Against Former Seller Even Though It Was Executed In Connection With The Sale Of A Business

Non-competition agreements executed in connection with the sale of a business are typically enforceable as a limited exception under Business and Professions Code section 16601 and applicable case authority to California's general prohibition against non-competition agreements. A recent California Court of Appeal decision, however, further narrows this limited exception.

In *Fillpoint v. Maas*, 2012 WL 3631266 (Aug. 24, 2012), the California Court of Appeal, Fourth District, found that two separate agreements—a stock purchase agreement and employment agreement—executed pursuant to the sale of a business, must be read together when analyzing the restrictive covenants contained in each agreement. The Court then held that the non-competition covenant in the employment agreement, whose terms differed from the non-competition covenant in the purchase agreement, did not fall under the “sale of business” exception, and thus was unenforceable. The Court reasoned that the covenant was not focused on protecting the acquired company's goodwill. Rather, it impermissibly “targeted an employee's fundamental right to pursue his or her profession” in violation of Business and Professions Code section 16600, California's statute prohibiting non-competition agreements.

### Background Facts

Defendant Michael Maas was an employee of specialty video game publisher Crave Entertainment Group. When Handleman Company acquired Crave, Maas sold his company stock and signed a stock purchase agreement. The purchase agreement contained a three-year covenant not to compete, which restricted Maas from engaging in the business he sold, with the exception of working on behalf of Crave. Business was defined as “distribut[ion] and publish[ing] of interactive entertainment (videogames), software, hardware and accessories and provid[ing] videogame software, hardware and accessories category management services for certain game retailers.”

In the purchase agreement, Crave also agreed to ensure that Maas would execute an employment agreement at closing. In fact, the purchase agreement contained an integration clause that made a blank form employment agreement part of the purchase agreement.

A month after the purchase agreement was signed, Maas entered into an employment agreement with Crave by which he agreed to work for Crave for three years. The employment agreement contained a covenant not to compete or solicit paragraph. The non-compete provision contained therein was different than the covenant not to compete in the purchase agreement. It prevented Maas from participating, engaging or having an interest in any competitive business in any county

in which Crave does business. In addition to the covenant not to compete provision, the paragraph contained a covenant not to sell competitive products to customers and prospective customers of Crave, and a covenant not to employ or solicit employees or consultants of Crave –hereinafter this is referred to as the non-solicitation provision. Both the non-competition and the non-solicitation provisions lasted for one year after the expiration of the employment agreement or after the earlier termination of his employment. The employment agreement contained an integration clause specifying that the employment agreement and purchase agreement constituted the sole and entire agreements between the parties, that any prior agreements were of no force and effect, and that to the extent that there was any conflict between the two agreements, the purchase agreement shall prevail.

Maas resigned exactly three years after executing the purchase agreement, purportedly satisfying the three-year non-competition covenant contained within the purchase agreement. Shortly thereafter, Maas became the President and CEO of competitor Solutions 2 Go.

Plaintiff Fillpoint LLC is a videogame distributor that acquired Crave's assets from Handleman, including the rights to Maas' employment agreement. Because of Maas' employment with competitor Solutions 2 Go, Fillpoint filed suit against Maas for breach of the employment agreement and against Solutions 2 Go for tortious interference with the employment agreement. The defendants asserted, among other defenses, that the covenant not to compete or solicit paragraph in the employment agreement was unenforceable under California Business and Professions Code section 16600.

## Trial Court's Decision

After Fillpoint's opening statement at trial, the defendants moved for nonsuit (i.e. as a matter of law, the evidence presented by plaintiff was insufficient to permit a jury to find in its favor). The trial court granted the defendants' nonsuit motion and found the following: (1) Maas' non-competition covenants were assignable to Fillpoint, (2) the covenants were contained in separate agreements and should not be read together, and (3) the covenant not to compete or solicit in the employment agreement was unenforceable under section 16600. The court later decided to dismiss the tortious interference claim because it was based upon the covenant not to compete or solicit in the employment agreement, which the court found to be unenforceable.

## Court of Appeal's Holding

The Court of Appeal reversed the trial court's decision and held that the purchase agreement and employment agreement must be read together, adopting Fillpoint's argument. (See Cal. Civ. Code § 1642: "Several contracts relating to the same matters, between the same parties, and made as parts of substantially one transaction, are to be taken together."). The Court, however, affirmed the trial court's judgment and found that the covenant not to compete or solicit in the employment agreement was void and unenforceable under California law. The Court reasoned that the covenant not to compete or solicit did not fall under the "sale of business" exception (Business and Professions Code section 16601) because it was overly broad and not designed to protect the acquired company's goodwill.

### **(1) The Non-Competition Covenants in the Purchase Agreement and Employment Agreement Must Be Read Together**

The Court stated that neither party cited any case with the same facts presented by the instant case—a purchase agreement and employment agreement entered at roughly the same time and as part of a single transaction, but containing different non-competition covenants. The Court proceeded to discuss several California cases that addressed non-competition covenants located in different and/or multiple documents.

The Court referenced the Court of Appeal decision in *Hilb, Rogal & Hamilton Ins. Services v. Robb* (1995) 33 Cal.App.4th 1812, which held that the placement of a three-year post-termination non-compete in an employment contract, rather than a merger agreement, did not affect the covenant's enforceability under section 16601 when both agreements were executed pursuant to the same business acquisition.

The Court also referenced the Court of Appeal decision in *Alliant Ins. Services, Inc. v. Gaddy* (2008) 159 Cal.App.4th 1292, which held that a non-compete contained in a purchase agreement executed pursuant to the sale of a business was enforceable under section 16601 in the context of a motion for preliminary injunction. The *Fillpoint* Court noted that the language in the purchase agreement was identical to the covenant contained in the related employment agreement. The identical covenants applied to the entire state of California, for a period of five years after the stock purchase closing date or two years after the termination of Gaddy's employment with the new company, whichever was later.

The *Fillpoint* Court distinguished the two cases from the instant case because they essentially involved a single non-competition covenant, where the instant non-competition covenants were different—three years after the purchase of Maas stock (purchase agreement) vs. one year after the termination of Maas' employment (employment agreement), with differing language.

The Court ultimately agreed with Fillpoint's argument that the purchase agreement and employment agreements should be read together because both agreements were part of the same single business transaction, referenced each other, were between the same parties, and contained an integration clause, but the Court did not reach the result that Fillpoint expected would result from that conclusion.

## **(2) The Non-Competition Covenant in the Employment Agreement is Unenforceable Under Business and Professions Code Section 16600**

The Court recognized that section 16601 permits the enforcement of non-competition covenants, executed in connection with the sale of a business, to protect an acquired company's goodwill and guard the value of the property right that was acquired. *The Court noted that the burden is on the buyer to prove that this exception applies.*

The Court rejected Fillpoint's argument that the fact the purchase agreement and employment agreement should be read together automatically meant the non-competition covenant in the employment agreement was enforceable under section 16601.

The Court found that the non-competition covenants in the two agreements were different by their very nature. The Court explained that "the purchase agreement's covenant was focused on protecting the acquired goodwill of Crave for a limited time" and "[t]he employment agreement's covenant targeted an employee's fundamental right to pursue his or her profession."

In fact, the Court reiterated that the non-competition covenant in the purchase agreement was fully satisfied and expired when Maas resigned three years later. The Court found that Fillpoint conceded in its briefing that the two non-competition covenants were intended to "deal with the different damage Maas might do wearing the separate hats of major shareholder and key employee." Thus, the Court concluded that the non-competition covenant in the employment agreement was unenforceable under section 16600 and failed to fit within the limited exception under section 16601.

The Court also found the non-solicitation provision in the employment agreement too broad and inconsistent with the purposes and terms of section 16600 and 16601 because it gave overly broad protection to the seller and extended beyond the business sold by barring Mass from selling to or soliciting the buyer's potential customers. The Court cited with approval *Strategix, Ltd. v. Infocrossing West, Inc.* (2006) 142 Cal.App.4th 1068, which found that "nonsolicitation covenants barring the seller from soliciting all employees and customers of the buyer, even those who were not former employees or customers of the sold business, extend their anticompetitive reach beyond the business so sold" and that such "covenants would give the buyer broad protection against competition wherever it happens to have employees or customers, at the expense of the seller's fundamental right to compete for employees and customers in the marketplace."

The Court concluded that Maas satisfied his covenant not to compete for three years under the purchase agreement. The employment agreement's covenant not to compete for an additional year, including its broad non-solicitation provision, cannot be reconciled with California's strong public policy permitting employees the right to pursue a lawful occupation of their own choice.

## What *Fillpoint* Means: The Takeaways

(1) **Current agreements.** *Fillpoint* may have a significant impact on companies who currently have different non-competition covenants contained within separate agreements that were executed pursuant to the sale of a business with sellers/key employees. While *Fillpoint* does not foreclose the ability to enforce non-competition covenants under section 16601, California courts may not enforce these covenants under this statute if the language of the agreement does not reflect a clear purpose to protect business goodwill. Companies should evaluate their non-competition agreements and recognize the risk that covenants within employment agreements may not be enforceable to the extent that they conflict with or have a broader scope than the terms of the covenants in the purchase or merger agreements and are not clearly and expressly calculated to protect the business goodwill of the selling company. Companies should also recognize that, while not at issue in this case, they may still attempt to argue that such covenants are enforceable because they are necessary to protect trade secrets under the so called “trade secrets exception” to Business and Professions Code section 16600. There remains a dispute as to whether such an exception exists and if so, what it means.

(2) **Future agreements.** Going forward, at a minimum, companies should include all non-competition covenants within the terms of the purchase agreements with sellers/key employees. As seen in the *Gaddy* case, a non-competition agreement that contains a latent tail (i.e. additional post-termination covenant triggered at an undetermined future date) may possibly be enforceable if contained within the terms of the purchase agreement. Some legal commentators, however, believe that latent tails that become effective many years after the sale may now be unenforceable. Companies should consider maxing out the duration of a permissible non-competition covenants in the purchase agreement with sellers/key employees. To the extent that companies include the non-competition covenants in employment agreements or other agreements, the non-competition provision should be identical to the non-competition provision in the purchase agreement and should contain clear language indicating that the purpose of the provision is to protect the business goodwill in connection with the sale of business. Any non-solicitation covenants in connection with the underlying transaction should be limited to customers and employees of the seller under the *Strategix* decision. The purchaser/new employer should also be able to prohibit the solicitation of employees that the key employee has contact with after joining the company under *Loral v. Moyes* (1985) 174 Cal.App.3d 268, for up to one year post-termination.

(3) **This is only one Court of Appeal decision and other decisions may support a different result.** This case’s holding that the non-competition covenant in the employment agreement did not fall under section 16601 because it focused on the “right to pursue a profession” appears to conflict with the Idaho Supreme Court in *T.J.T., Inc. v. Mori* (Id. 2011) 266 P.3d 476 (applying California law) and other California decisions. The Idaho Supreme Court in *T.J.T.* found that a two-year non-compete agreement executed in connection with the sale of a business was enforceable under California law, despite the fact that the seller also became an employee of the purchasing company as a result of the sale. Even though the non-compete agreement referred to the employee/seller’s employment with the new employer/buyer to determine its duration and enforceability, the court found that such an “incidental” link does not necessarily mean the provision is unenforceable. Instead, the court reasoned that the employee’s employment only came about as part of the larger transaction—the sale of the business to a competitor—and was therefore enforceable. Interestingly, *T.J.T.* examined the same cases (*Hilb, Rogal & Hamilton Ins. Services v. Robb* (1995) 33 Cal.App.4th 1812 (containing a three year post-termination non-compete in employment agreement) and *Alliant Ins. Services, Inc. v. Gaddy* (2008) 159 Cal.App.4th 1292 (2008) (containing a five year non-compete and two year post-termination non-compete in asset purchase agreement and employment agreement) as *Fillpoint* but came to a different conclusion.

Also, the *Fillpoint* Court did not address two existing California Court of Appeal decisions that may also be instructive and lead to a different result. In *Newlife Sciences v. Weinstock* (2011) 197 Cal.App.4th 676, the California Court of Appeal, Second District, upheld a preliminary injunction based upon discovery issue sanctions entered against an employee who breached his non-competition agreement contained in an employment agreement with his new employer. The non-competition agreement was operative during his new employment and for five years after termination of that employment. The trial court determined that it was enforceable because it was part of the transfer of business and its goodwill by the selling employee.

Additionally, in *Monogram Industries, Inc. v. SAR Industries, Inc.* (1976) 64 Cal.App.3d 692, the California Court of Appeal, Second District, affirmed the entry of a preliminary injunction against an employee on a breach of a covenant not to

## Seyfarth Shaw — Management Alert

compete. The five year covenant not to compete was contained in a consultant agreement executed in a connection with a purchase agreement. The court upheld the provision under a previous version of section 16601 reasoning that the purpose of section 16601 is to permit the purchaser to protect himself or itself against competition from the seller which competition would have the effect of reducing the value of the property right that was acquired. Some may consider this interest as the same side of the coin compared to the *Fillpoint* Court's concern for the "employee's fundamental right to pursue his or her profession." The court also reasoned that there was an inference that business had a "goodwill" and that it was transferred where the covenant was executed as an *adjunct* of a sale of a business.

(4) **California is unique regarding the enforcement of non-competes.** This case reminds us that California is different from other states in its general prohibition and strong public policy against non-competes. In most states, the one-year non-competition covenant at issue in this case would likely be enforceable in whole or part. Companies may want to consider including out-of-state forum selection and choice of law provisions, coupled with consent to jurisdiction provisions, to attempt to increase the likelihood of successfully enforcing their non-competition agreements against business sellers/key employees provided the parties to the transaction have a sufficient connection to the outside forum state.

By: *Robert Milligan* and *Joshua Salinas*

*Robert Milligan* is a partner in Seyfarth's Los Angeles office and *Joshua Salinas* is an attorney in Seyfarth's Los Angeles office. If you would like further information, please contact your Seyfarth attorney, Robert Milligan at [rmilligan@seyfarth.com](mailto:rmilligan@seyfarth.com) or Joshua Salinas at [jsalinas@seyfarth.com](mailto:jsalinas@seyfarth.com). You may also visit our blog, Trading Secrets, at [www.tradesecretslaw.com](http://www.tradesecretslaw.com).



[www.seyfarth.com](http://www.seyfarth.com)

Attorney Advertising. This Management Alert is a periodical publication of Seyfarth Shaw LLP and should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have. Any tax information or written tax advice contained herein (including any attachments) is not intended to be and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on the taxpayer. (The foregoing legend has been affixed pursuant to U.S. Treasury Regulations governing tax practice.) © 2012 Seyfarth Shaw LLP. All rights reserved.

**Breadth. Depth. Results.**



# Appendix C

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

PHILIP C. HARTSTEIN,	)	Case No. 12-2270 SC
	)	
Plaintiff,	)	ORDER DENYING PLAINTIFF'S
	)	MOTION TO REMAND AND GRANTING
v.	)	<u>DEFENDANT'S MOTION TO DISMISS</u>
	)	
REMBRANDT IP SOLUTIONS, LLC,	)	
and DOES 1 through 25,	)	
inclusive,	)	
	)	
Defendants.	)	
_____	)	

**I. INTRODUCTION**

Plaintiff Philip C. Hartstein ("Plaintiff") brings this action for declaratory relief to invalidate the covenant not to compete in his employment agreement with Defendant Rembrandt IP Solutions, LLC ("Defendant"). Plaintiff asserts that the covenant is contrary to California Business and Professions Code section 16600. The case was initially filed in the Superior Court of the State of California in and for the County of San Mateo but was subsequently removed to federal court. ECF No. 1 ("Not. of Removal"). Plaintiff now moves to remand on the ground that the amount in controversy is less than the jurisdictional minimum of \$75,000. ECF No. 21 ("MTR"). Additionally, Defendant moves to dismiss for improper venue under Federal Rule of Civil Procedure 12(b)(3) on the ground that Plaintiff's employment agreement includes a mandatory forum selection clause which calls for exclusive

United States District Court  
For the Northern District of California

1 jurisdiction in Pennsylvania. ECF No. 5 ("MTD"). Both motions are  
2 fully briefed. ECF Nos. 22 ("MTR Opp'n"), 23 ("MTD Opp'n"), 24  
3 ("Reply ISO MTD"), 25 ("Reply ISO MTR"). Pursuant to Civil Local  
4 Rule 7-1(b), the Court finds this matter appropriate for  
5 determination without oral argument. As detailed below, the Court  
6 DENIES Plaintiff's Motion to Remand and GRANTS Defendant's Motion  
7 to Dismiss for improper venue.

8  
9 **II. BACKGROUND**

10 Defendant is a Delaware limited liability company ("LLC") with  
11 a principal place of business in Pennsylvania. ECF No. 3  
12 ("Compl.") ¶ 2. Defendant's sole member is its parent, Rembrandt  
13 IP Management, LLC ("RIPM"). RIPM also has only one member -- an  
14 individual who resides in and is a citizen of Pennsylvania. ECF  
15 No. 19 ¶¶ 2-3. Defendant identifies and develops business  
16 opportunities for RIPM, which is engaged in the management of funds  
17 focused on investing in intellectual property and related  
18 opportunities across a broad spectrum of industries, technologies,  
19 and business methods, including generating revenues from patents.  
20 Compl. Ex. A ("Empl. Agr.").

21 On December 23, 2009, Plaintiff, a resident of San Mateo,  
22 California, entered into the Employment Agreement with Defendant.  
23 Compl. ¶¶ 3, 7; Empl. Agr. The Employment Agreement contains a  
24 non-compete provision that restricts Plaintiff from directly or  
25 indirectly working for a competitor of Defendant for a period of  
26 one year from the termination of his employment unless he first  
27 obtains the written consent of the CEO or President of Defendant.  
28 Empl. Agr. ¶ 4(a). Additionally, the Employment Agreement bars

1 Plaintiff from disclosing Defendant's trade secrets and  
2 confidential information to third parties. Id. ¶ 9. The  
3 Employment Agreement also contains a forum selection clause which  
4 provides: "[Plaintiff] and [Defendant] submit to the exclusive  
5 jurisdiction of the state courts located in Montgomery County,  
6 Pennsylvania and to the Federal courts located in Philadelphia,  
7 Pennsylvania as to all actions and proceedings relating in any way  
8 to this Agreement and/or [Plaintiff]'s relationship with  
9 [Defendant]." Id. ¶ 15.

10 Plaintiff worked as Defendant's Managing Director of Business  
11 Development from January 1, 2010 through March 5, 2012. ECF No.  
12 22-1 ("Wood Decl.") ¶ 5.<sup>1</sup> In his last year of employment with  
13 Defendant, Plaintiff earned an annual salary "well in excess" of  
14 \$75,000. Id. ¶ 6; Not. of Removal ¶ 8. Plaintiff "was jointly  
15 responsible for all aspects of [Defendant's] business development  
16 efforts, including interaction with patent owners located  
17 throughout the United States and the identification of prospective  
18 patent investment opportunities." Wood Decl. ¶ 5. Plaintiff was  
19 one of only two employees at the company with direct responsibility  
20 for generating patent investment leads and opportunities. Id.  
21 From March 2011 through February 2012, Plaintiff managed or  
22 generated more than one hundred unique investment leads. Id. ¶ 9.  
23 The potential expected profit from Plaintiff's leads is in the  
24 millions of dollars. Id. ¶ 10.

25 On March 5, 2012, Plaintiff informed Defendant that he was  
26 resigning from the company and requested that Defendant waive the

---

27 <sup>1</sup> Derek Wood ("Wood"), corporate counsel and secretary for RIPM,  
28 filed a declaration in opposition to Plaintiff's Motion to Remand.  
ECF No. 22-1 ("Wood Decl.").

United States District Court  
For the Northern District of California

1 non-compete provision in the Employment Agreement. Compl. ¶ 9.  
2 Defendant indicated that it intended to enforce the provision. Id.  
3 After leaving Defendant, Plaintiff began employment as Vice  
4 President and Portfolio Manager at IPNav. Wood Decl. Ex. A.  
5 ("IPNav Press Release"). Plaintiff's new job responsibilities are  
6 similar to his responsibilities with Defendant. See id. Defendant  
7 and IPNav compete for many of the same patent portfolios and  
8 investment opportunities. Id. ¶ 15.

9 Also on March 5, 2012, Plaintiff filed the instant action in  
10 the Superior Court of the State of California in and for the County  
11 of San Mateo. Plaintiff seeks a judicial declaration that the non-  
12 compete provision is invalid and contrary to section 16600 of the  
13 California Business and Professions Code. Compl. ¶ 14. He also  
14 seeks a preliminary and permanent injunction barring Defendants  
15 from enforcing the non-compete provision. Id. ¶ 19. In the  
16 Complaint, Plaintiff alleges that he intends to comply with all  
17 other provisions of the Employment Agreement and that he has not  
18 misappropriated and has no intention of misappropriating  
19 Defendant's trade secrets or confidential information. Id. ¶ 10.

20 On May 4, 2012, Defendant removed the action to federal court  
21 on diversity grounds. In the Notice of Removal, Defendant asserts,  
22 on information and belief, that Plaintiff is earning an annual  
23 salary in excess of \$75,000 with his new employer. Id. Defendant  
24 also asserts that the value of its trade secrets and other  
25 confidential information known to Plaintiff exceeds \$75,000. Id. ¶

26 9.

27 ///

28 ///

1 **III. DISCUSSION**

2 The Court first addresses Plaintiff's Motion to Remand to  
3 determine whether it has subject-matter jurisdiction to hear this  
4 case. Concluding that the exercise of subject-matter jurisdiction  
5 is proper, the Court then considers Defendant's Motion to Dismiss.

6 **A. Motion to Remand**

7 Plaintiff moves to remand this action back to state court on  
8 the ground that Defendant has failed to establish that the amount  
9 in controversy exceeds the jurisdictional minimum of \$75,000. For  
10 the reasons set forth below, the Court finds that Defendant has met  
11 its burden.

12 A defendant may remove a civil action filed in state court if  
13 the action could have been filed originally in federal court. 28  
14 U.S.C. § 1441(a). A plaintiff may seek to have a case remanded to  
15 the state court from which it was removed if the district court  
16 lacks jurisdiction or if there is a defect in the removal  
17 procedure. Id. § 1447(c). The general removal statutes are  
18 construed restrictively so as to limit removal jurisdiction.  
19 Shamrock Oil & Gas Corp. v. Sheets, 313 U.S. 100, 108-09 (1941).  
20 Federal jurisdiction "must be rejected if there is any doubt as to  
21 the right of removal in the first instance." Duncan v. Stuetzle,  
22 76 F.3d 1480, 1485 (9th Cir. 1996) (quotations omitted). The  
23 burden of establishing federal jurisdiction for purposes of removal  
24 is on the defendant. Valdez v. Allstate Ins. Co., 372 F.3d 1115,  
25 1117 (9th Cir. 2004).

26 District courts may exercise diversity jurisdiction in the  
27 first instance where "the matter in controversy exceeds the sum or  
28 value of \$75,000, exclusive of interest and costs" and there is

1 complete diversity of citizenship between the plaintiff and  
2 defendants. 28 U.S.C. § 1332(a). Upon removal, the defendant  
3 bears the burden of showing that it is more likely than not that  
4 \$75,000 is in controversy. See Singer v. State Farm Mut. Auto.  
5 Ins. Co., 116 F.3d 373, 377 (9th Cir. 1997).

6 "In actions seeking declaratory or injunctive relief, it is  
7 well established that the amount in controversy is measured by the  
8 value of the object of the litigation." Hunt v. Wash. State Apple  
9 Adver. Comm'n, 432 U.S. 333, 347 (1977). "The value of an  
10 injunction may not be capable of precise determination, but  
11 precision is not required." Mailwaukee Mailing, Shipment and  
12 Equip., Inc. v. Neopost, Inc., 259 F. Supp. 2d 769, 772 (E.D. Wis.  
13 2003). Where, as here, a plaintiff seeks to invalidate a non-  
14 competition clause, courts sometimes "look to the profits earned by  
15 the employer on business generated by the employee during the  
16 period immediately preceding his termination to determine the  
17 amount in controversy." See Luna v. Kemira Specialty, Inc., 575 F.  
18 Supp. 2d 1166, 1172 (C.D. Cal. 2008) (quotations omitted).  
19 Alternatively, courts have considered the Plaintiff's salary or the  
20 likely financial impact of Plaintiff's competition during the non-  
21 compete period. See Davis v. Advanced Care Techs., Inc., CVS 06  
22 02449 DFL DAD, 2007 WL 1302736, at \*2 (E.D. Cal. May 2, 2007).  
23 Under any of these measures, the amount in controversy requirement  
24 is satisfied here.

25 With respect to the first measure -- the profits generated by  
26 the employee -- RIPM's corporate counsel and secretary declares  
27 that "the potential expected profit from many of Plaintiff's  
28 investment leads, if acquired and developed, was in the millions of

1 dollars." Wood Decl. ¶ 10.<sup>2</sup> Plaintiff essentially argues that  
2 because the profitability of these leads cannot be precisely or  
3 accurately measured until some future date, Plaintiff's value to  
4 Defendant's business is too speculative to be considered for the  
5 purposes of an amount in controversy determination. See Reply ISO  
6 MTR at 3. This argument is unavailing. It is often difficult to  
7 directly measure an employee's contribution to a business's profits  
8 and revenues. However, that does not mean the employee's value to  
9 the business is zero. Here, Plaintiff played a central and high-  
10 level role in Defendant's business operations since he was one of  
11 only two employees with direct responsibility for generating  
12 Defendant's patent investment leads and opportunities. See Wood  
13 Decl. ¶¶ 3, 5. Based on Plaintiff's job responsibilities, the  
14 estimate provided by RIPM's corporate counsel, and Plaintiff's  
15 salary, see infra, the Court finds it more likely than not that  
16 Plaintiff was worth over \$75,000 to Defendant.<sup>3</sup>

17  
18 <sup>2</sup> Plaintiff makes a number of evidentiary objections to this and  
19 other statements in the Wood Declaration. Reply ISO MTR at 8-9.  
20 These objections are overruled. First, Plaintiff objects that a  
21 number of Wood's statements are "irrelevant," but offers no  
22 coherent explanation as to why evidence concerning the value of the  
23 non-compete agreement would be irrelevant to a dispute about the  
24 amount in controversy. Second, Plaintiff objects under Federal  
25 Rule of Evidence 602, which provides: "A witness may testify to a  
26 matter only if evidence is introduced sufficient to support a  
27 finding that the witness has personal knowledge of the matter."  
28 Here, the evidence shows that Wood is the corporate counsel and  
secretary for Defendant's parent company, and, thus, is in a  
position to have personal knowledge of Plaintiff's value to  
Defendant and his potential value to Defendant's competitors.

<sup>3</sup> If Plaintiff disagreed with this estimate, he was free to offer  
evidence of his own. See Kenneth Rothschild Trust v. Morgan  
Stanley Dean Witter, 199 F. Supp. 2d 993, 1001 (C.D. Cal. 2002)  
(once defendant submits "summary-judgment-type evidence" to  
establish the amount in controversy, plaintiff has the burden of  
rebutting that evidence). He declined to do so.

1 With respect to the salary-based approach, Defendant paid  
2 Plaintiff an annual salary well in excess of \$75,000. Wood Decl. ¶  
3 6. Based on this evidence, it is more likely than not that  
4 Plaintiff's new salary with IPNav or one of Defendant's other  
5 competitors would be comparable. Plaintiff's arguments against the  
6 salary-based approach are unpersuasive. Plaintiff contends that  
7 "reliance on a method that values the injunction to a future  
8 employer is misplaced." MTR at 7. But the salary-based approach  
9 assesses the value of the non-compete to Plaintiff, not his future  
10 employer.<sup>4</sup> The non-compete provision effectively bars Plaintiff  
11 from earning a salary in his chosen profession for one year. Thus,  
12 considering the salary that Plaintiff could command from one of  
13 Defendant's competitors is a simple and straightforward way to  
14 value the object of this litigation. Plaintiff also argues that  
15 this approach is difficult to apply because it requires Defendant  
16 "to present competent evidence of the salary [Plaintiff] would make  
17 if employed in a field outside the scope of the non-compete  
18 covenant, and then compare this hypothetical salary to what  
19 [Plaintiff] would make working in a field within the scope of the  
20 non-compete covenant . . . ." Reply ISO MTR at 5. But the Court  
21 need not compare hypothetical salaries. This is not an action for  
22 damages and, thus, the Court need not determine whether Plaintiff  
23 has attempted to mitigate his losses. The pertinent point is that  
24 the non-compete provision prevents Plaintiff from earning a salary  
25 in his chosen field.

26  
27  
28 <sup>4</sup> Alternatively, the salary-based approach could be used to value  
an employee's value to his or her employer.

1 The Court reaches the same conclusion as to the value of the  
2 trade secrets and confidential information known to Plaintiff. If  
3 Plaintiff breaches the Employment Agreement and offers Defendant's  
4 investment leads to a competitor, Defendant stands to lose millions  
5 of dollars in expected revenues and profits. See Wood Decl. ¶¶ 8-  
6 10. Further, Plaintiff has detailed knowledge of Defendant's  
7 business models, which could have significant value to its  
8 competitors. See id. at 11-12. Plaintiff argues that the value of  
9 the non-compete to Defendant is zero since Plaintiff has not  
10 misappropriated and has no intention of misappropriating  
11 Defendant's trade secrets or confidential information. Reply at 6.  
12 This argument lacks merit. Following his resignation, Plaintiff  
13 accepted a position with one of Defendant's direct competitors.  
14 See Wood Decl. ¶¶ 15-16; IPNav Press Release.<sup>5</sup> Regardless of  
15 Plaintiff's stated intention, the possibility that he will share  
16 Defendant's trade secrets and confidential information with this  
17 competitor is very real. In any event, Plaintiff's argument goes  
18 to the merits of his claims and, thus, should not be considered  
19 before determining whether the Court has subject-matter  
20 jurisdiction. See Davis, 2007 WL 1302736, at \*2.

21  
22  
23 <sup>5</sup> Plaintiff argues that the IPNav Press Release is not properly  
24 authenticated since it was printed from the internet. Reply ISO  
25 MTR at 9. The Court disagrees. The press release was published by  
26 GlobeNewswire and is self-authenticating under Federal Rule of  
27 Evidence 902(6). See Arachnid, Inc. v. Valley Recreation Products,  
28 Inc., 98 C 50282, 2001 WL 1664052, (N.D. Ill. Dec. 27, 2001); but  
see Trans-Tec Asia v. M/V HARMONY CONTAINER, 435 F. Supp. 2d 1015,  
1031 n.20 (C.D. Cal. 2005). Plaintiff also objects that certain  
statements in the press release constitute inadmissible hearsay.  
Reply ISO MTR at 9. The Court agrees and does not rely on those  
statements.

1 For these reasons, the Court finds that the jurisdictional  
2 amount in controversy requirement has been met and, therefore,  
3 DENIES Plaintiff's Motion to Remand.

4 **B. Motion to Dismiss for Improper Venue**

5 As the Court finds that it has subject-matter jurisdiction, it  
6 may properly consider Defendant's Rule 12(b)(3) Motion to Dismiss  
7 for improper venue. The gravamen of the motion is that the  
8 mandatory forum selection clause in the Employment Agreement  
9 requires that "all actions and proceedings relating in any way" to  
10 the agreement be litigated in a Pennsylvania court. MTD at 1.

11 "In diversity cases, federal law governs the analysis of the  
12 effect and scope of forum selection clauses." Jones v. GNC  
13 Franchising, Inc., 211 F.3d 495, 497 (9th Cir. 2000). A motion to  
14 dismiss for improper venue based upon a forum selection clause is  
15 governed by the rule set forth in M/S Bremen v. Zapata Off-Shore  
16 Co., 407 U.S. 1 (1972). Id. In Bremen, the Supreme Court held  
17 that a forum selection clause is presumptively valid and should  
18 control unless a party can "clearly show that enforcement would be  
19 unreasonable and unjust, or that the clause was invalid for such  
20 reasons as fraud or overreaching." 407 U.S. at 15. The court also  
21 stated that a forum selection clause should be held unenforceable  
22 "if enforcement would contravene a strong public policy of the  
23 forum in which suit is brought." Id. If the forum selection  
24 clause is enforceable, the Court may either dismiss the action or  
25 transfer the litigation to the parties' selected forum. See 28  
26 U.S.C. § 1406(a).

27 Plaintiff argues that enforcement of the Pennsylvania forum  
28 selection clause is unreasonable since it would contravene

1 California's strong public policy against covenants not to compete.  
2 MTD Opp'n at 3. Plaintiff's argument proceeds as follows:  
3 Plaintiff's case is sure to succeed in California because  
4 California law disfavors covenants not to compete. See id. at 6.  
5 On the other hand, if the Court enforces the forum selection clause  
6 and the case proceeds in Pennsylvania, then Plaintiff is likely to  
7 lose because Pennsylvania courts generally uphold covenants not to  
8 compete. See id. Thus, enforcing the forum selection clause  
9 "would deprive [Plaintiff] of the protection of his own  
10 jurisdiction's laws and remedies." Id.

11 The problem with Plaintiff's argument is that it does not  
12 challenge the reasonableness of the forum selection clause itself,  
13 only the reasonableness of its effect. A substantially similar  
14 argument was raised and rejected in Manchester v. Arista Records,  
15 Inc., 1981 U.S. Dist. LEXIS 18642 (C.D. Cal. Sept. 15, 1981). The  
16 court reasoned:

17 The plaintiff's analysis would unduly complicate the  
18 analysis of this issue in future cases. If the Court  
19 adopted plaintiff's argument, each court presented  
20 with a forum selection clause issue would be forced to  
21 make a determination of the potential outcome of the  
22 litigation on the merits in the transferee forum and  
23 to consider whether that outcome would conflict with a  
24 strong public policy of the transferor forum. Although  
25 such a course might seem relatively simple in a case  
26 such as this, in which there are no factual disputes  
27 presented, it would become complicated and uncertain  
28 in cases involving complex legal questions or  
voluminous amounts of disputed issues of fact. Thus,  
each Court presented with the issue would be involved  
in detailed speculation on the merits at the outset of  
the action.

26 Manchester, 1981 U.S. Dist. Lexis 18642, at \*15-16.

27 As Defendant points out, a number of other courts have  
28 followed this reasoning and rejected the argument that the

1 enforcement of a forum selection clause would contravene  
2 California's strong public policy against covenants not to compete.  
3 See Loughlin v. Ventraq, Inc., 10-CV-2624-IEG BGS, 2011 WL 1303641,  
4 at \*7 (S.D. Cal. Apr. 5, 2011); Mahoney v. Depuy Orthopaedics,  
5 Inc., CIVF 07-1321 AWI SMS, 2007 WL 3341389, at \*8 (E.D. Cal. Nov.  
6 8, 2007); Swenson v. T-Mobile USA, Inc., 415 F. Supp. 2d 1101, 1104  
7 (S.D. Cal. 2006); see also Besag v. Custom Decorators, Inc., CV08-  
8 05463 JSW, 2009 WL 330934, at \*4 (N.D. Cal. Feb. 10, 2009) ("a  
9 party challenging enforcement of a forum selection clause may not  
10 base its challenge on choice of law analysis"). The Court finds  
11 this line of authority to be persuasive.

12 Plaintiff unsuccessfully attempts to distinguish this  
13 authority from the instant action. MTD Opp'n at 7-9. While there  
14 are minor distinctions in the facts, the holdings of Manchester and  
15 Defendant's other cases clearly apply here. Plaintiff also argues  
16 that the Ninth Circuit's decision in Jones demands a contrary  
17 result. That case is inapposite. In Jones, the court found that a  
18 Pennsylvania forum selection clause in a franchise agreement  
19 contravened section 20040.5 of the California Business and  
20 Professions Code, which provides that "[a] provision in a franchise  
21 agreement restricting venue to a forum outside this state is void  
22 with respect to any claim arising under or relating to a franchise  
23 agreement involving a franchise business operating within this  
24 state." Jones, 211 F.3d at 498-99. Thus, in Jones, the issue was  
25 whether the forum selection itself was contrary to California law.  
26 In contrast, here, the issue is whether the Court should enforce  
27 the forum selection clause because some other provision of the  
28 Employment Agreement is purportedly contrary to California law.

1           Accordingly, the Court finds that the Pennsylvania forum  
2 selection clause in the Employment Agreement is valid and  
3 enforceable and GRANTS Defendant's Motion to Dismiss for improper  
4 venue.

5  
6 **IV. CONCLUSION**

7           For the foregoing reasons, the Court DENIES Plaintiff Philip  
8 C. Hartstein's Motion to Remand and GRANTS Defendant Rembrandt IP  
9 Solutions, LLC's Motion to Dismiss for improper venue. This action  
10 is DISMISSED without prejudice. Plaintiff may re-file the action  
11 in another venue consistent with the forum selection clause of the  
12 Employment Agreement.

13  
14           IT IS SO ORDERED.

15  
16           Dated: July 30, 2012



UNITED STATES DISTRICT JUDGE



# Appendix D



---

## UNHEALTHY COMPETITION – Daily Journal

By Robert B. Milligan on April 3rd, 2009

April 02, 2009

***Daily Journal Reprinted and/or posted with the permission of Daily Journal Corp. (2009).***

By Robert Milligan and Nicholas Waddles

The California Supreme Court's decision in *Edwards v. Arthur Andersen LLP*, 44 Cal.4th 937 (2008), reaffirmed that employee non-competition agreements are void in California unless they fall within narrow exceptions to Business and Professions Code Section 16600.

Notwithstanding the *Edwards* decision, it may be possible for employers to enforce non-competition forfeiture provisions in California by including them in retirement plans subject to the Employee Retirement Income Security Act of 1974. ERISA is a federal statute that governs most employee benefit plans (except those provided by government entities and churches), including retirement plans. ERISA plans are protected by a well-formed pre-emption doctrine that applies to most state laws except those regulating insurance, banking or securities matters.

In a series of cases dating back as early as 1980, the 9th Circuit has examined the inclusion of non-competition forfeiture provisions in ERISA plans and has determined that such clauses are permissible under ERISA, with some limitation, and state law is pre-empted on this issue.

It is important to point out that a non-competition forfeiture provision in an ERISA plan cannot apply to any amount an employee voluntarily contributes to a plan because such amounts are always automatically 100 percent vested and not otherwise subject to forfeiture. Similarly, a forfeiture provision added to an ERISA plan could not apply to benefits earned prior to the adoption of the amendment.

Also, ERISA's vesting rules generally establish a maximum time period over which employer contributions to a plan must vest. At the time most of the relevant 9th Circuit cases were decided, ERISA permitted employers to choose between one of two vesting schedules for employer contributions. One schedule was a 10-year "cliff vesting" schedule whereby an employee was zero percent vested until he or she worked for the employer for 10 years, at which time the employee became 100 percent vested. The other schedule provided for a graduated vesting schedule that allowed an employee to vest in incremental percentages (usually 10-20 percent) over time, but not to exceed 15 years.

These vesting rules have been amended a number of times over the years, and currently, employer contributions to profit-sharing and 401(k) plans must vest under either a three-year cliff vesting schedule or a six-year graduated schedule at the rate of 20 percent, beginning with the second year of service.

Accordingly, including a forfeiture provision in a profit-sharing or 401(k) plan may not be as effective as it was when the relevant cases were decided. Now, however, it may be more effective to include non-competition forfeiture provisions in top-hat or other executive compensation plans (which are generally ERISA plans that are exempt from the vesting rules). And there are others commentators who have suggested adding forfeiture provisions to ERISA-covered severance plans as another way of achieving this goal. No 9th Circuit cases have examined whether a forfeiture provision could be included in a top-hat or ERISA-covered severance plan but the arguments in favor of ERISA pre-emption should be the same as in the relevant cases. Instructively, the 2nd Circuit has held that state law was pre-empted by ERISA in the context of a top-hat plan containing a non-competition forfeiture clause and found that the forfeiture provision was valid. One of the earliest cases to examine the inclusion of a non-competition forfeiture provision was the pre-ERISA case of *Muggill v. The Reuben H. Donnelley Corporation*, 62 Cal. 2d 239 (1965). In *Muggill*, the California Supreme Court analyzed the validity of a provision in a pension plan that provided that an employee's right to receive payments from the plan would be terminated if he went to work for a competitor. The court held that the pension plan became part of the employment contract and, therefore, the forfeiture provision was invalid under Section 16600 – "[e]xcept as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."

ERISA was enacted in 1974 and, thereafter, the 9th Circuit's first occasion to analyze a non-competition forfeiture provision in an ERISA plan was in *Hummell v. S.E. Rykoff & Co.*, 634 F.2d 446 (9th Cir. 1980). In *Hummell*, the court examined a plan provision that provided for the forfeiture of a percentage of the competing former employee's retirement benefits derived from employer contributions. The plan stated that the forfeiture provision only applied to former employees with less than 15 years of experience with the company who competed with the company (those with more than 15 years were fully vested, regardless of competitive activity).

In examining an issue of first impression, the court held that ERISA does not prohibit limited non-competition provisions that apply to amounts in excess of the minimum vesting requirements in ERISA. Ultimately, the court held that the forfeiture provision in the plan was invalid as to the plaintiff because he had more than the minimum years of service required to be 100 percent vested under that plan. Thus, the forfeiture provision was valid but it could not be applied by the company.

In *Lojek v. Thomas*, 716 F.2d 675 (9th Cir. 1983), the court examined a non-competition forfeiture provision contained in an ERISA-governed profit sharing plan sponsored by a law firm. The provision called for the forfeiture of all employer contributions made on behalf of an attorney who left the firm before completing 10 years of employment and engaged in competitive employment within two years of leaving within a five-county area.

The trial court granted partial summary judgment on a number of issues including that ERISA pre-empts Idaho state law on vesting and forfeiture of pension plan rights and non-competition forfeiture clauses are valid under ERISA. *Lojek* appealed arguing, inter alia, that Idaho common law on non-competition clauses should control and invalidated the provision. The court disagreed and held that the district court properly decided that ERISA pre-empted Idaho law and federal law governed the validity of the plan.

The plan at issue contained a vesting schedule more liberal than required by ERISA. It allowed attorneys to fully vest after completing five years of employment (the cliff vesting provision under ERISA at the time was 10 years). If an attorney worked for at least 10 years, the non-competition provision did not apply. As a result, the court held that the vesting schedule was valid.

Similarly, in *Clark v. Lauren Young Tire Center Profit Sharing Trust*, 816 F. 2nd 480 (9th Cir. 1987), the plaintiff argued that a forfeiture clause in an ERISA plan violated Oregon law and the plaintiff urged to the court to incorporate that law and invalidate the provision. In rejecting the plaintiff's argument, the court held that the reasoning in *Lojek*

applied and that state law played "no part in assessing the validity of [a non-competition forfeiture provision] in an ERISA plan."

The court in Clark further held that non-competition forfeiture clauses in ERISA plans are valid so long as the plan provides that benefits earned after 10 years of service cannot be forfeited. Because ERISA's vesting requirements have been reduced, it is likely that a court reviewing facts similar to Clark today would require that the plan provide that benefits earned after three years of service cannot be forfeited (assuming the court followed the ERISA preemption authority).

Finally, in *Weinfurther v. Source Services Corporation Employees Profit Sharing Plan and Trust*, 759 F.Supp. 599 (N.D. Cal. 1991), the court reiterated that non-competition forfeiture clauses in the Ninth Circuit are valid (citing *Lojek* and *Clark* with approval).

Accordingly, based on the 9th Circuit authorities discussed above, employers have a plausible argument that non-competition forfeiture provisions included in ERISA plans should be analyzed under ERISA and are not subject to Business and Professions Code Section 16600. Employers should consider including ERISA plan provisions providing that an employee forfeits employer contributions exceeding ERISA's minimum vesting rules if the employee violates a non-competition provision included in the plan. The non-competition forfeiture provisions should be limited in scope and duration to the extent necessary to protect legitimate business interests.

Additionally, employers may consider trying to extend the ERISA approach to top-hat plans and ERISA severance plans (with structured payouts over time).

These approaches are not without risk and counsel should be consulted before including any non-competition forfeiture provisions as there is always a possibility that notwithstanding ERISA preemption that a court may find that it does not apply based on the strong public policy of Section 16600.

###

---

Seyfarth Shaw LLP.

•

131 South Dearborn Street • Suite 2400

• Chicago, IL 60603-5577

Trade Secrets and Confidentiality Lawyers & Attorneys, the Trade Secrets, Computer Fraud, & Non-Competes practice group of Seyfarth Shaw LLP, offering services relating to corporate espionage, electronic information protection, non-compete agreements, non-disclosure, proprietary information, restrictive covenants, audits, protection policies, trade secrets litigation, with offices in Atlanta, Boston, Chicago, Los Angeles, New York, Houston, Sacramento, San Francisco.

Unless otherwise indicated, attorneys listed in this Web site are not certified by the Texas Board of Legal Specialization.

No reproduction of this site or its content without the express permission of Seyfarth Shaw, LLP

Copyright © 2012, Seyfarth Shaw LLP. All Rights Reserved.



# Appendix E

# Management Alert



## New Law Protecting Personal Social Media Of California Employees and Students Adopted In California

On September 27, 2012, California Governor Jerry Brown signed two bills, AB 1844 and SB 1349, into law, making California the third state in the country – Maryland and Illinois are the others – to regulate employers' ability to demand access to employees' or prospective hires' personal social media accounts. Appropriately enough, Governor Brown made the announcement via five major social media networks: Twitter, Facebook, Google+, LinkedIn and MySpace. Brown *tweeted*, "California pioneered the social media revolution. These laws protect Californians from unwarranted invasions of their social media accounts."

### California Assembly Bill 1844

*California Assembly Bill 1844* ("AB 1844") "prohibit[s] an employer from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media." In other words, an employer may neither request nor require an employee or an applicant to divulge his or her personal social media account information.

This law, however, allows for employers to request the employee divulge social media "reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding." Furthermore, this law prohibits employers from threatening or taking retaliatory measures against employees that fail to comply with employer requests or demands that violate the statute.

This law "does not prohibit an employer from terminating or otherwise taking an adverse action against an employee or applicant if otherwise permitted by law." Finally, unlike many other labor and employment laws, "the Labor Commissioner . . . is not required to investigate or determine any violation of this act."

### Senate Bill 1349

*Senate Bill 1349* ("SB 1394") prohibits public and private postsecondary educational institutions, and their employees and representatives, from requiring students or prospective students to disclose their personal user names or passwords, or to divulge personal social media information.

SB 1394 requires private nonprofit or for-profit postsecondary educational institutions to post its social media privacy policy on the institution's Internet website.

Both AB 1844 and SB 1394 define the term "social media" broadly to include "electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."

### Perspectives on the Bills

Proponents of these social media laws believe *the laws will benefit* the business community by providing California businesses with a shield from legal liability against plaintiffs who allege that these businesses have a legal duty to monitor

## Seyfarth Shaw — Management Alert

their employee's social media accounts. Additionally, they argue that this legislation could potentially save businesses millions of dollars by reducing costs related to monitoring social media accounts and cyber liability insurance premiums. Recently, both the California Chamber of Commerce and organized labor have expressed their support for the law.

Opponents of the bill argue that it will hurt employers by limiting their ability to regulate the workplace and investigate misconduct. Others *believe* the bill may make it more difficult for companies to identify workplace harassment. Members of the financial industry, including FINRA, argued that while the bill may have been well intended, it conflicts with the duty of security firms to record, supervise, and maintain business-related communications.

Some legal commentators have also expressed their *concern* that the definition of "social media" is far too broad because it governs effectively all digital content and activity. In fact, Illinois excludes "e-mail" from the definition of social media in its version of the statute.

## What These Laws Mean For Employers

Businesses in California should take steps to comply with these new laws which will go in effect on January 1, 2013. Employers should make sure that interviewers or other persons involved in the hiring process do not request personal user names or passwords from applicants. Additionally, employers will need to be careful with company social media accounts. While the laws only apply to personal accounts, the lack of definition of the phrase "personal" is problematic, particularly since it is not always clear who owns company social media accounts. We have previously blogged on cases concerning the ownership of "social media assets" on *Twitter*, *Facebook*, and *MySpace*. Some experts *recommend* that companies utilize ownership agreements governing the social media accounts and content created by employees on behalf of the company and that they always have the account name and password for the company social media account (certainly prior to the employee's termination). It may be helpful for employers to create clear policies on this issue to prevent future disputes.

Finally, employers should understand that the law does not constitute a complete ban on employers' access to their employees' social media sites. Employers are still permitted to require employees to divulge social media passwords when the information is used solely to investigate allegations of employee misconduct or employee violation of applicable laws and regulations. Similarly, employer-issued electronic devices do not fall under the umbrella of AB 1844; the bill specifically states that it shall not be construed to preclude an employer from requiring an employee to disclose passwords or usernames for such devices. Notwithstanding, an employer cannot ask for access to the "personal social media" that may be contained on the employer-issued electronic device.

There may also be additional issues for employers that employ BYOD (bring your own device) policies, where the employee uses their own personal device to access company email, applications, or other data. While the employer may not technically own the device, it still has an interest in its data and information that reside on the device. The broad definition of social media and lack of definition of "personal" in the new law may lead to some unintended consequences for employers.

By: *Robert Milligan*, *Jessica Mendelson* and *Joshua Salinas*

*Robert Milligan* is a partner in Seyfarth's Los Angeles office, *Jessica Mendelson* is an associate in the firm's San Francisco office and *Joshua Salinas* is an attorney in the Los Angeles office. If you would like further information, please contact your Seyfarth attorney, Robert Milligan at [rmilligan@seyfarth.com](mailto:rmilligan@seyfarth.com), Jessica Mendelson at [jmendelson@seyfarth.com](mailto:jmendelson@seyfarth.com) or Joshua Salinas at [jsalinas@seyfarth.com](mailto:jsalinas@seyfarth.com). You may also visit our blog, Trading Secrets, at [www.tradesecretslaw.com](http://www.tradesecretslaw.com).

[www.seyfarth.com](http://www.seyfarth.com)

The logo for Seyfarth Shaw LLP features the firm's name in a serif font. "SEYFARTH" is in a larger, bold font, with "ATTORNEYS" in a smaller font underneath it. "SHAW" is in a larger, bold font to the right of "SEYFARTH", and "LLP" is in a smaller font underneath it. The logo is set against a background of blue and green geometric shapes.

Attorney Advertising. This Management Alert is a periodical publication of Seyfarth Shaw LLP and should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have. Any tax information or written tax advice contained herein (including any attachments) is not intended to be and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on the taxpayer. (The foregoing legend has been affixed pursuant to U.S. Treasury Regulations governing tax practice.) © 2012 Seyfarth Shaw LLP. All rights reserved.

**Breadth. Depth. Results.**



# Appendix F

### In This Issue...

#### Featured Article

Your Company Cannot Afford Not to Adequately Protect Its Trade Secrets and Other Confidential Information  
*Kurt Kappes and Robert Milligan, Seyfarth Shaw LLP* ..... 1

#### Copyright Law

RIAA and Lionsgate Fail to Prove Loss for Mandatory Restitution in Internet Piracy Case..... 6

Court Denies Motion to Dismiss Coupons, Inc.'s DMCA Case against Pro Se Defendant..... 7

Court Grants TRO, Preventing Distribution of Pirated *Gears of War 2* Video Game ..... 8

#### Entertainment Law

Ninth Circuit Vacates Summary Judgment in Case Involving *Gone In 60 Seconds* Film ..... 9

#### Patent Law

Federal Circuit Affirms Rejection of Patent for Obviousness-Type Double Patenting During Reexamination..... 11

Federal Circuit Disqualifies Counsel Due to Prior Representation of Defendant in Related Litigation..... 12

D.C. Circuit Rejects 180-Day Exclusivity Period where Challenged Patent Had Been Delisted from FDA Orange Book..... 13

Finding Insufficient Notice of Plaintiff's Allegations, District of Columbia Dismisses Patent Infringement Complaint..... 14

Recent Hatch-Waxman Filings ..... 14

#### Technology Law

District Court Refuses to Dismiss Click Fraud Allegations against Internet Advertising Company..... 15

Ineffective County Spam Filters Do Not Infringe First Amendment Rights..... 16

New Hampshire Supreme Court Finds Defendant "Knowingly Possessed" Pornographic Images Located in Computer's Temporary Internet Files ..... 17

District Court Finds Employee Who Accessed Former Employer's E-mail System Violated Stored Communications Act..... 19

Internet Access Service Must Allege "Actual Harm" to Have Standing under CAN-SPAM Act..... 20

Domain Name Dispute Decisions: Posted Nov. 10–Nov. 16, 2008..... 21

#### Trademark Law

District Court Grants in Part, Denies in Part, Summary Judgment for Use of AUDI Trademarks by Parts Dealer ..... 26

TTAB Precedential Decisions..... 28

#### Bloomberg News: IP Moves

Nov. 17–Nov. 21, 2008..... 29

#### Bloomberg Law

Bloomberg Continuing Legal Education (CLE) ..... 31

## Featured Article

### Your Company Cannot Afford Not to Adequately Protect Its Trade Secrets and Other Confidential Information

*Article contributed by:*

*Kurt Kappes and Robert Milligan, Seyfarth Shaw LLP*

The convergence of our current downward economic trend and technological advances, especially in electronic communications and data transfer, has led to an increased need for companies to evaluate their trade secret protections.

Many businesses are increasingly relying on intangible or knowledge-based assets. In these economic times, when layoffs and mergers abound, the risk of trade secret theft is high.

To address this risk, it is imperative that companies adequately protect their most valuable assets. For many companies, the cost of losing their valuable intellectual property, including their trade secrets and other confidential information, could be immense and devastate them financially.

This article addresses the problem and provides a solution: a comprehensive trade secret audit.

#### *The Problem: Misappropriation of Trade Secrets and Other Confidential Information*

Trade secret theft continues to be a large and growing problem, with Fortune 1000 companies reporting that they have sustained losses of more than \$50 billion from thefts of their proprietary information.<sup>1</sup> In 2005, six percent of employees surveyed admitted to e-mailing company proprietary information to someone they should not have.<sup>2</sup> In 2002, in a survey of 130 businesses, 40 percent reported actual or suspected losses of trade secrets.<sup>3</sup> In 2000, the American Society for Industrial Security (ASIS) estimated that each year, losses and potential losses from economic espionage cost American companies over \$60 billion each year.<sup>4</sup> In February 1999, the FBI and the US Chamber of Commerce estimated that US companies lost approximately \$2 billion a month as a result of corporate espionage.<sup>5</sup> Additionally, companies that do not ensure that they have adequate protections for their trade secret and other confidential information can put management at risk of shareholder lawsuits and other litigation, including Sarbanes-Oxley violations.

According to the FBI, the Cold War has moved to a new arena: the global marketplace. The FBI estimates that every year billions of dollars are lost to foreign competitors who deliberately target proprietary economic information in U.S. companies.<sup>6</sup> The FBI sees this as such a growing problem that it identified the 10 highest-value corporate targets and met with executives about the potential threats they face.<sup>7</sup> The FBI is currently pursuing 143 cases of economic espionage.<sup>8</sup>

The FBI has identified three ways foreign competitors who seek economic intelligence generally operate to create their spy networks:

1. They aggressively target and recruit susceptible people (often from the same national background) working for U.S. companies and research institutions;
2. They recruit people to locate economic intelligence through operations like bribery, discreet theft, dumpster diving (in search of discarded trade secrets), and wiretapping; and
3. They establish seemingly innocent business relationships between foreign companies and U.S. industries to gather economic intelligence including classified information.<sup>9</sup>

The FBI also has identified six steps for protecting companies:

1. Recognize there is a real threat.
2. Identify and value trade secrets.
3. Implement a definable plan for safeguarding trade secrets.
4. Secure physical trade secrets and limit access to trade secrets.
5. Confine intellectual knowledge.
6. Provide ongoing security training to employees.<sup>10</sup>

As David Drab, a prior FBI employee who worked for 27 years fighting organized crime and economic espionage explained in a recent article in PCWorld Business Center, “[t]he payoffs are high and the risks of getting caught are low.”<sup>11</sup> Drab identified employee training and monitoring as key. Employees who have either a sudden change in lifestyle, make several trips overseas, have security infractions or disciplinary issues should be closely monitored. According to Drab, economic espionage is a “huge problem” and reliance on technology alone is not sufficient.<sup>12</sup>

Not all companies have taken these threats seriously enough, however. Earlier this decade, it was estimated that over half of

U.S. corporations had no established protocol for protecting trade secrets.<sup>13</sup>

Many companies are victims of trade secret theft at the hands of foreign governments and competitors *as well as former employees and domestic competitors*. For example, in the last few years:

- A former aerospace engineer was charged with stealing trade secrets related to confidential NASA projects and allegedly sending them to agents of a foreign government.<sup>14</sup>
- A NASA contractor was awarded \$2.1 million from one its subcontractors who misappropriated trade secrets and used the information to obtain two lucrative NASA service contracts.<sup>15</sup>
- A national communication company received a multimillion-dollar damage award and additional \$7 million in punitive damages where the defendants were accused of misappropriating trade secrets that included algorithms and computer code used in its audio conferencing equipment.<sup>16</sup>
- A technology company sued a competitor alleging that the competitor’s CEO and other high-ranking authorities stole proprietary software.<sup>17</sup>
- An engineer at an auto-parts maker allegedly stole hundreds of confidential computer files that would be used to set up a competing company in China. A federal grand jury indicted the engineer, his wife who worked in the sales department and their Chinese partner, a former metallurgist, on 64 counts of stealing trade secrets and related crimes.<sup>18</sup>
- The brokerage arm of a financial management and advisory company won a partial injunction to prevent a former employee from luring former clients to a competitor. The former employee was also accused of stealing confidential and proprietary customer data.<sup>19</sup>
- A foreign airline company was ordered to pay \$26.33 million for industrial espionage against another airline after the second airline allegedly continued to use its booking system.<sup>20</sup>
- An international aerospace corporation sued two former employees and their new employer claiming that they shared trade secrets with a company that then patented a process for making materials based on the stolen information.<sup>21</sup>
- A national home building contractor sued a former top executive for allegedly stealing a highly

confidential market study and strategic plan, which was allegedly used to create a market report for a major competitor.<sup>22</sup>

- A former executive of a chemical and plating company pleaded guilty to hatching a scheme to destroy trade secrets of a competing company in an attempt to prevent the loss of a business deal.<sup>23</sup>
- A former software engineer was accused of stealing trade secrets for a competitor and a search of his home by the FBI uncovered more of his former employer's confidential materials.<sup>24</sup>

The Internet and other advances in technology and telecommunications have enhanced the issues companies face in keeping their trade secrets and other confidential information protected. The widespread use of laptops, personal digital assistants, cell phones, wireless internet, pocket cameras, miniature flash drives, etc. make it so much easier for employees, especially disgruntled employees, to take confidential information. Employee mobility and company assets in the form of digital information, combined with fast and easy methods for transferring data, has increased the need for creative and thoughtful trade secret protections.

Additionally, the increasing popularity of social network sites has also added a new twist to protecting proprietary information. Employees visit online social network sites, such as Facebook®, MySpace®, and LinkedIn®. Online internet forums, such as listservs, chat rooms and blogs, where there is a free exchange of ideas, are also popular. These online forums provide numerous opportunities for employees to leak proprietary information—either intentionally or inadvertently. Employees also tap into these resources to learn about new job opportunities, adding to the ever increasing mobility of the workforce. Businesses are now faced with challenges that they would not have even dreamed of several years ago.

*The California Wrinkle.* While companies in many states attempt to protect themselves against unlawful competition by former employees through non-competition agreements, it is especially important for California companies to review their non-competition and non-solicitation agreements for compliance in the wake of the recent California Supreme Court decision *Edwards v. Arthur Andersen*,<sup>25</sup> which clarified that non-competition agreements are invalid in California. This leaves trade secret law as one of the last few refuges for companies to protect their proprietary data in California.

*The Solution: A Comprehensive Audit of Your  
Company's Policies and Practices Identify  
the Trade Secrets*

A trade secret is defined as information that generates economic value for its owner from not being generally known and that is subject to reasonable efforts to preserve its

secrecy. One of the key factors used to determine whether proprietary information is “trade secret” is the extent and nature of the precautions taken to preserve the information's secrecy. Absolute secrecy and heroic measures are not required; *however, if a trade secret is leaked, its value to the company may be severely compromised and lost forever.* There must be a substantial element of secrecy so that a third person would have difficulty acquiring the information without resorting to improper means. In order to maintain a claim for trade secret misappropriation, a company's efforts to maintain the confidentiality of its trade secrets need to be reasonable under the circumstances, depending on the value of the information and the risk of loss of the information. A trade secret misappropriation suit, however, may be a hollow option for some companies whose trade secrets are their life blood.

While traditionally we think of the KFC recipe and Coca Cola formula as the quintessential trade secrets, trade secrets come in many shapes and sizes. Customer lists, designs or drawings, business strategies, confidential marketing plans, research, and development activities, “negative know-how” (that something does not work), pricing information, sales forecasts, manuals, prototypes, and formulas could all be considered trade secrets depending upon the particular circumstances. Trade secrets can also be maintained in different formats such as computer files, formal or draft documents, working papers, scrap papers, appointment calendars, internal correspondence, newsletters, policy documents, minutes from meetings, and other records. Documents that are provided to public entities (e.g. sealed bids, request for proposal (RFP) responses to public entities) can also contain confidential, trade secret information.

*Audits Are Key.* The best way to assess a company's trade secrets is through a formal audit—a proactive and dynamic analysis of a company's proprietary assets and how such assets are protected. During an audit, outside counsel works closely with the appropriate business teams to identify the company's important information assets, including identifying what may qualify as a trade secret. Technical information, financial information, marketing information, compensation information, and organizational information are all reviewed. The audit team also helps to identify and classify the importance of the assets, the security precautions in place to protect such assets, and assesses how best to protect them.

The audit team can identify the company's assets that are valuable and worthy of protecting, as well as any existing security protections. The audit team considers any past trade secret issues and concerns, as well as the company's overall objectives related to the company's trade secrets. Sometimes a patent or other intellectual property attorneys are involved to tailor the most appropriate kind of protection for the particular intellectual property asset. Audits should be assisted by someone with experience with computer fraud and network security issues and computer forensics, including managing and protecting computer-stored data.

After identifying and classifying the company's proprietary information, the audit team can develop and implement procedures, including effective hiring and firing procedures, to: 1) reduce the risk that trade secrets will be improperly disclosed; 2) provide evidentiary support should the need for obtaining legal relief for trade secret theft become necessary; and 3) limit the risk of exposure to other companies to claims of misappropriation.

An audit should review physical and computer data security practices and make recommendations to help ensure adequate security and prevent theft. This often involves making recommendations concerning facility access, security layout, computer access, network system layout, and protections of electronic data. Special attention should be given to developing best practices for managing and protecting computer-stored data. Many businesses keep their confidential data on computers, making this aspect of the audit especially helpful.

Any trade secret audit must include a thorough review of the company's current protection agreements. Companies must make sure that their agreements are routinely monitored to keep them up-to-date with the current technologies and law. The audit team should review the company's various protection agreements—including employee confidentiality agreements, employment agreements and non-competition/non-solicitation agreements, blogging policies, anti-piracy agreements, technology use agreements, invention assignment agreements, as well as third party non-disclosure agreements (e.g. customer and vendor agreements)—to ensure that they appropriately safeguard the company's trade secrets.

*Putting a Plan in Place.* Effective trade secret protection plans should include: 1) effective procedures prohibiting the disclosure of company trade secrets; 2) an individual or committee responsible for overseeing the trade secret protection plan; 3) a workforce educated about the need to protect trade secrets; 4) a plan for maintaining confidentiality through training, agreements and security; 5) effective employee intake and outtake procedures related to trade secrets/confidential information; and 6) periodic audits of trade secret protection policies and practices.

The benefits of having more formal procedures and effective practices in place are: 1) they can help protect valuable trade secrets and prevent unnecessary loss; 2) they help to maintain a competitive edge in the marketplace; 3) they notify employees and third parties of interest about the company's desire to protect proprietary information; and 4) they educate employees on what constitutes trade secret and confidential information and how to protect it, and the consequences of failing to do so. An effective trade secret protection plan should foster a workplace culture where employees understand and appreciate the need to protect all of the company's trade secrets for the betterment of the company.

Although companies often have at least some policies in place to help protect their trade secrets, the policies are

often inadequate, difficult to implement or understand, or are ineffective. One survey even revealed that some policies can be counterproductive and lead to more information being divulged.<sup>26</sup> One study concluded that there are eight mistakes companies often make that hinder their ability to protect their trade secrets:

1. Policies signal to employees that they are not trusted.
2. Policies punish employees instead of helping them protect trade secrets.
3. Managers fail to practice what is preached.
4. Management gives short shrift to new employee orientation.
5. Management fails to communicate with staff regularly.
6. Companies forget to clarify ownership issues.
7. Companies define the scope of the business too narrowly.
8. Companies fail to adequately address departing employees.<sup>27</sup>

Through a comprehensive trade secret audit, the company can develop effective policies that fit the particular business and organizational culture. The resulting policies should be useful and easy to administer, and most importantly adequately protect the company's trade secrets.

In addition, companies should develop appropriate procedures for addressing trade secret theft claims, including effective screening procedures for employees who may be violating company policies as well as those of previous employers. Companies should also implement measures to instruct employees of their obligation to protect trade secrets, including departing employees.

Because many trade secret thefts occur from within by employees, companies must develop successful methods for handling departing employees by ensuring that there are effective policies requiring the return of all company property and exit interviews providing explicit instructions concerning their continuing duties to the company. Early detection capabilities in computer networks can advise employers of thefts early before any damage is done. Because of the significant role computers often play in trade secret thefts, a knowledge of computer forensics is key.

Third party, government, and consultant relationships involving trade secrets present a unique set of issues. Companies should ensure that they have effective processes and

agreements in place to protect the company's assets in these specific contexts.

The next step is for the company to develop and implement a comprehensive educational process to train employees about all aspects of the company's trade secret protections. Companies should provide training tailored to the particular business for management and other employees concerning effective procedures for maintaining security of the company's trade secrets. Training should include teaching management about particular warning signs and behavior to watch for: living outside of the employee's means, refusing to accept help or take vacations, particularly disgruntled employees, misplacing or failing to provide receipts.<sup>28</sup>

New employee training about the company's trade secrets is a must. Taking care to separate out the importance of trade secrets, so it does not get lost in the mounds of paper a new employee receives, is especially helpful. In addition, regular reminders about trade secrets not only sensitizes employees about the company's proprietary information, but also reminds employees about how important it is to safeguard the information.

However, companies should be aware that a proper balance needs to be struck. Too many cautions can backfire if employees do not feel trusted. This can hurt company loyalty. Furthermore, the goal of trade secret protections should be to help keep them confidential, not to punish. Above all, companies must make sure that management is setting a good example.

An effective audit also needs to take into account advances in technology. Technology changes rapidly, requiring companies to keep up with the latest trends. Five years ago, corporate firewalls was all the protection that many companies had. Now, there are multiple points of entry and numerous ways that someone can steal data or corrupt the accuracy of data. Cutting edge forensic computer analysis can detect the copying and deleting of proprietary information. Computer software can identify when USB mass storage devices are used to alert companies to unauthorized use and even completely disable a mass storage device. New software is being developed that uses data mining and social networking techniques to spot and stop insider security threats and industrial espionage. In the meantime, using computer forensics to recover personal e-mails of departing employees that have been sent on company computers can uncover and alert companies to employee misconduct.

Too often these issues are overlooked before a company's trade secrets and other confidential information have been compromised. Especially now, as companies face increasing competitive and financial pressures, management is understandably consumed with running the day-to-day operations of the business and working to achieve business objectives and maximize the bottom line. As a result, it is still

common for companies to find themselves in situations where important assets are taken for granted. Yet, those same assets can be lost or compromised in a moment through what is often benign neglect. At the same time, companies sometimes find themselves, through poor controls, exposed when they inadvertently obtain others' trade secrets. Experience has shown that companies gain tremendous value by taking a proactive, systematic approach to assessing and protecting their trade secret portfolios through a trade secret audit. There has rarely been a time where it has been more critical.

*Kurt Kappes is a partner and Robert Milligan is a senior associate in the Sacramento, California and Los Angeles, California offices of Seyfarth Shaw LLP, respectively. They focus their practice on commercial litigation and employment matters, including trade secret misappropriation and other intellectual property theft. They regularly assist businesses with non-competition and non-solicitation issues and have significant experience prosecuting and defending related actions in state and federal courts. They have advised companies how best to protect their trade secrets in a variety of industries, including financial services, retail, and manufacturing. Kurt Kappes can be reached at [kkappes@seyfarth.com](mailto:kkappes@seyfarth.com), (916) 448-0159, (877) 449-0410, and Robert Milligan can be reached at [rmilligan@seyfarth.com](mailto:rmilligan@seyfarth.com), (310) 277-7200, (800) 643-1583. Mr. Kappes and Mr. Milligan are regular contributors to Seyfarth Shaw LLP's Trading Secrets: A Law Blog on Trade Secrets, Non-Competes, and Computer Fraud, [www.tradesecretslaw.com](http://www.tradesecretslaw.com).*

<sup>1</sup> David R. Hannah, *Keeping Trade Secrets Secret*, MIT Sloan Mgmt. Rev., Spring 2006, at 17–20; Bradford K. Newman, *Protecting Trade Secrets, Dealing with the Brave New World of Employee Mobility*, Bus. Law Today, Nov./Dec. 2007 (citing 2007 survey by the American Society for Industrial Security).

<sup>2</sup> John Keville & Sheryl Falk, *Use Computer Forensics to Catch a Trade Secret Thief*, Legal Technology, Sept. 25, 2008.

<sup>3</sup> Hannah, *supra* note 1.

<sup>4</sup> Ira S. Winkler, *Case Study of Industrial Espionage through Social Engineering*, available at <http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF>.

<sup>5</sup> *Foreign Economic and Industrial Espionage Remains a Threat in 1999*, <http://www.fas.org/irp/ops/ci/docs/fy99.htm>.

<sup>6</sup> See Federal Bureau of Investigation, <http://www.fbi.gov/hq/ci/economic.htm>.

<sup>7</sup> David J. Lynch, *FBI Goes on Offensive Against China's Tech Spies*, USA Today, July 25, 2007.

<sup>8</sup> *Id.*

<sup>9</sup> See Federal Bureau of Investigation, *supra* note 6.

<sup>10</sup> *Id.*

<sup>11</sup> Jeremy Kirk, *Enterprises Face Losses from Trade Secret Thefts*, PCWorld Bus. Center, Oct. 28, 2008.

<sup>12</sup> *Id.*

<sup>13</sup> *Over Half of U.S. Companies Have No Protocol for Protecting Trade Secrets, Most U.S. Companies Unprepared for Digital Information Requests in Litigation*, Bus. Wire, May 15, 2000.

<sup>14</sup> *Ex-Boeing Engineer Charged in China Spying Case*, Reuters, Feb. 11, 2008.

<sup>15</sup> *Jury Hands NASA Contractor \$2M in Trade Secret Suit*, Emp. Law 360, Oct. 31, 2008.



# Appendix G

## Tips for BYOD Policies

1. Policy should specify what devices are permitted
2. Policy should include a stringent security policy for all devices
3. Policy should define a clear service policy for devices
4. Make clear who owns what apps and data
5. Decide what apps will be allowed or banned
6. Integrate your BYOD plan with your computer usage/access policies
7. Include an employee exit component into the policy



## DIGITAL GOVERNMENT

[About the Strategy](#) | [Strategy Milestones](#) | [Deliverables](#) | [Advisory Group](#)

# Bring Your Own Device

*A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs*  
August 23, 2012

Product of the Digital Services Advisory Group and Federal Chief Information Officers Council

## Contents

[Introduction](#)

[Key Considerations](#)

[Case Studies](#)

[Alcohol and Tobacco Tax and Trade Bureau \(TTB\) Virtual Desktop Implementation](#)

[U.S. Equal Employment Opportunity Commission \(EEOC\) BYOD Pilot](#)

[State of Delaware BYOD Program](#)

[Example Policies](#)

[Sample #1: Policy and Guidelines for Government-Provided Mobile Device Usage](#)

[Sample #2: Bring Your Own Device – Policy and Rules of Behavior](#)

[Sample #3: Mobile Information Technology Device Policy](#)

[Sample #4: Wireless Communication Reimbursement Program](#)

[Sample #5: Portable Wireless Network Access Device Policy](#)

## Introduction

The Digital Government Strategy (the Strategy) ([PDF/HTML](#)), issued by Federal Chief Information Officer (CIO) Steven VanRoekel on May 23, 2012, called for the establishment of a Digital Services Advisory Group (Advisory Group) to promote cross-agency sharing and accelerated adoption of mobile workforce solutions and best practices in the development and delivery of digital services. Milestone Action #3.3 of the Strategy requires the Advisory Group to work with the Federal CIO Council (CIOC) to develop government-wide bring-your-own-device (BYOD)<sup>[1]</sup> guidance based on lessons learned from successful BYOD programs launched at forward-leaning agencies. Through the BYOD Working Group, the Advisory Group and CIOC produced this document to fulfill the requirements of Milestone Action #3.3.

Implementing a BYOD program is not mandatory. This document is intended to serve as a toolkit for agencies contemplating implementation of BYOD programs. The toolkit is not meant to be comprehensive, but rather provides key areas for consideration and examples of existing policies and best practices. In addition to providing an overview of considerations for implementing BYOD, the BYOD Working Group members developed a small collection of case studies to highlight the successful efforts of BYOD pilots or programs at several government agencies. The Working Group also assembled examples of existing policies to help inform IT leaders who are planning to develop BYOD programs for their organizations.

Future Digital Government Strategy deliverables, such as the Mobile Security Reference Architecture encompassed in Milestone Action #9.1, will help inform agency considerations on BYOD. The National Institute of Standards and Technology (NIST) is also drafting several standards and guidelines focused on mobility, including: [Guidelines for Managing and Securing Mobile Devices in the Enterprise](#)<sup>[2]</sup>; [Security and Privacy Controls for Federal Information Systems and Organizations](#); and [Personal Identity Verification \(PIV\) of Federal Employees and Contractors](#). Each of these documents should provide further insight into issues associated with the implementation of BYOD solutions.

While the case studies and example policies that the BYOD Working Group has assembled are a great starting point for agencies considering BYOD programs, this work is not finished. The Federal Government still has more to do to address the more complicated issues related to BYOD. This includes how the government can reimburse Federal employees for voice/data costs incurred when they use their personal mobile devices instead of government-issued mobile devices, and additional security, privacy, and legal considerations including supply chain risk management and legal discovery.

## Key Considerations

The implementation of BYOD needs to be an iterative process – support of BYOD for commodity enterprise technologies like email and collaboration systems can lay the foundation for expanding to more diverse, mission-specific applications and a broader scope of enterprise offerings. BYOD can be facilitated through applications native to the device, downloaded or installable applications, or even a web browser. The private and public sector entities who have adopted BYOD solutions report that allowing

employees to use their personal mobile devices to access company resources often results in increased employee productivity and job satisfaction. From the Federal information security perspective, devices must be configured and managed with information assurance controls commensurate with the sensitivity of the underlying data as part of an overall risk management framework.

The BYOD Working Group observed additional characteristics about this growing trend:

- BYOD is about offering choice to customers. By embracing the consumerization of Information Technology (IT), the government can address the personal preferences of its employees, offering them increased mobility and better integration of their personal and work lives. It also enables employees the flexibility to work in a way that optimizes their productivity.
- BYOD can and should be cost-effective, so a cost-benefit analysis is essential as the policy is deployed. Such a cost-benefit analysis should take into account both potential increases in employee productivity and potential cost shifts. For example, providing employees access to government services on their personal devices should help reduce the number of government devices that are provided to staff as well as the life-cycle asset management costs associated with these devices. BYOD programs may, however, necessitate government reimbursement for voice/data costs incurred when employees use their personal mobile devices instead of government-issued mobile devices and additional enterprise infrastructure costs in handling the support of BYOD users. Additionally, overall costs may significantly increase for personnel who frequently communicate outside of the coverage area of their primary service provider and incur roaming charges.
- Implementation of a BYOD program presents agencies with a myriad of security, policy, technical, and legal challenges not only to internal communications, but also to relationships and trust with business and government partners. The magnitude of the issues is a function of both the sensitivity of the underlying data and the amount of processing and data storage allowed on the personal device based on the technical approach adopted. Generally speaking, there are three high-level means of implementing a BYOD program:
  - Virtualization: Provide remote access to computing resources so that no data or corporate application processing is stored or conducted on the personal device;
  - Walled garden: Contain data or corporate application processing within a secure application on the personal device so that it is segregated from personal data;
  - Limited separation: Allow comingled corporate and personal data and/or application processing on the personal device with policies enacted to ensure minimum security controls are still satisfied.

The growing trend of BYOD demonstrates that we as IT leaders have changed how we adopt technology. Gone are the days of long projects that address every demand. We must now integrate new technologies in a rapid, iterative, agile, interoperable, and secure method to meet changing market and customer needs. Device agnosticism is more important than ever. Our software, hardware, and applications must be compatible across common systems and personal devices. Our information security controls must also be consistent with existing law and standards to ensure confidentiality, integrity, and availability.<sup>[3]</sup> Because of these and other considerations, BYOD is not necessarily a good fit for all government agencies – it has to fit the agency’s environment, support mission requirements, and meet the specific needs of staff.

The business case for implementing BYOD programs vary from agency to agency, but often involve the following drivers: to reduce costs, increase program productivity and effectiveness, adapt to a changing workforce, and improve user experience. Below is a list of points to consider when determining whether a BYOD program is right for your agency and its staff. The list, which is by no means exhaustive, includes policy and process considerations for Chief Information Officers, Chief Technology Officers, Chief Information Security Officers, Chief Human Capital Officers, Chief Financial Officers, Chief Acquisition Officers, and others.

- Technical approach
  - Virtualization
  - Walled garden
  - Limited separation
- Roles and responsibilities
  - Agency
  - User
  - Help/service desk(s)
  - Carrier technical support
- Incentives for government and individuals
  - Survey employees on benefits and challenges
  - Consider voluntary vs. mandatory participation in BYOD program and impact on terms of service
- Education, use, and operation
  - Establish orientation, trainings, and user agreements
  - Establish associated policies collaboratively with union representative
  - Ensure compliance with Fair Labor Standards Act (FLSA) requirements (e.g., institute policies to ensure non-exempt employees do not conduct work after-hours unless directly authorized/instructed)
  - Consider impact of connectivity and data plan needs for of chosen technical approach (e.g., virtualization) on employee reimbursement
  - Implement telework agreements consistent with the Telework Enhancement Act and OMB implementation requirements
- Security
  - Assess and document risks in:
    - Information security (operating system compromise due to malware, device misuse, and information spillover risks)
    - Operations security (personal devices may divulge information about a user when conducting specific activities in certain environments)
    - Transmission security (protections to mitigate transmission interception)
  - Ensure consistency with government-wide standards for processing and storing Federal information
  - Assess data security with BYOD versus the devices being replaced
  - Securely architect systems for interoperability (government data vs. personal data)
- Privacy
  - Identify the right balance between personal privacy and organizational security
  - Document process for employee to safeguard personal data if / when government wipes the device
- Ethics / legal questions

- Define “acceptable use” from both government and individual perspective
- Address legal discovery (including confiscation rights) and liability issues (e.g., through pre-defined opt-in requirements in terms of service)
- Consider implications for equal rights employment (e.g., disparity in quality of personal devices)
- Service provider(s)
  - Identify companies that could offer discounts to government employees
  - Assess opportunities to leverage the Federal Strategic Sourcing Initiative
  - Assess tax implications for reimbursement
- Devices and applications (apps)
  - Identify permitted and supported devices to prevent introduction of malicious hardware and firmware
  - Define content applications that are required, allowed, or banned and consider use of mobile device management (MDM) and mobile application management (MAM) enterprise systems to enforce policies<sup>[4]</sup>
  - Adopt existing app development best practices to support device-agnosticism and data portability across platforms
  - Address app compatibility issues (e.g., accidental sharing of sensitive information due to differences in information display between platforms)
  - Recommend approach to content storage (cloud vs. device)
  - Clarify ownership of the apps and data
- Asset management
  - Disposal of device if replaced, lost, stolen, or sold, or employment is terminated (must remove government information before disposal)
  - Reporting and tracking lost / stolen personal devices
  - Replacement of personal lost devices if employee chooses not to replace with personal funds
  - Funding for service and maintenance

### Case Studies

In the right environment, BYOD programs can be an enormous success. The BYOD Working Group members developed a small collection of case studies that highlight the successful implementation of a BYOD pilot or program at a government agency. These studies include a brief synopsis which summarizes the specific challenges, approaches, and lessons learned of each. None of the BYOD programs discussed in these case studies involve the transmission of classified information. Agencies should consider the applicability of the discussed technical and policy approaches to their own environments.

- The Department of the Treasury’s Alcohol and Tobacco Tax and Trade Bureau (TTB) implemented a virtual desktop that allowed a BYOD solution with minimal policy or legal implications;
- The U.S. Equal Employment Opportunity Commission (EEOC) was among the first of several Federal agencies to implement a BYOD pilot that allowed employees to “opt out” of the government-provided mobile device program and install third-party software on their own smartphones that enabled the use of their device for official work purposes;
- The State of Delaware initiated an effort to not only embrace the concept of BYOD but to realize significant cost savings by having employees turn in their State-owned device in favor of a personally-owned device, which could save the State approximately half of its current wireless expenditure.

[Back to top](#)



### Alcohol and Tobacco Tax and Trade Bureau (TTB) Virtual Desktop Implementation

*Allowing Bring Your Own Device with Minimal Policy or Legal Implications*  
August 13, 2012

Robert Hughes  
Chief Information Officer  
Department of the Treasury  
Alcohol and Tobacco Tax and Trade Bureau (TTB)  
[robert.hughes@ttb.gov](mailto:robert.hughes@ttb.gov)

#### Executive Summary

The Alcohol and Tobacco Tax and Trade Bureau (TTB) decided to reduce the costs, time and effort required to refresh desktop and laptop computers used for client computing needs. TTB has a widely dispersed workforce with many personnel working from home full time and over 80 percent of the workforce regularly teleworking. Replacing desktop and laptop computers every 3 to 4 years cost TTB about \$2 million and disrupted the IT program and business users for several months. TTB determined that the best solution was to centralize all client computing power and applications, user data, and user settings and allow access to TTB resources by thin client computing devices. A thin client is a computing device or program that relies on another device for computational power. Currently about 70 percent of TTB personnel use thin client devices to access all TTB applications and data.

TTB desktop and laptop computers were due for refresh this year. However, the virtual desktop solution allowed TTB to avoid the expense of replacing hardware. The savings achieved paid for TTB’s virtual desktop implementation – which cost approximately \$800,000 – and saved TTB \$1.2 million.

TTB realized additional savings by developing a Linux USB device that can be used to turn old desktop and laptop computers into thin client computing devices for approximately \$10 per device. The TTB virtual desktop/thin client implementation uses a small browser plugin, freely available for almost every operating system, which simply turns the end user device into a viewer and controller of the virtual desktop running in the TTB computer rooms. No data touches the end user device. As a result, the TTB virtual desktop implementation has the significant additional benefit of delivering every TTB application, with user data, to a wide range of user devices without the legal and policy implications that arise from delivering data to or allowing work to be accomplished directly on a personal device.

### Challenge

TTB was created as an independent bureau in the Department of the Treasury on January 24, 2003, by the Homeland Security Act of 2002. When TTB was established, all information technology (IT) resources, including capital assets, IT personnel and the funding to procure equipment and to develop core business applications remained with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). TTB was funded at a level sufficient only to reimburse ATF for existing service. No funding was provided for the initial purchase or subsequent replacement of any of the equipment required to establish and operate TTB's IT Systems. In FY 2005 TTB established an independent IT operation with no base funding to refresh infrastructure equipment.

TTB has a very dispersed workforce with many personnel working from home full time and over 80 percent of the workforce regularly teleworking. Replacing desktop and laptop computers every 3 to 4 years cost TTB about \$2 million and disrupted the IT program and business users for several months. TTB decided to reduce the costs, time, and effort required to refresh client desktop and laptop computers. After considering several solutions, TTB determined that it would centralize all client computing power and applications, user data, and user settings to allow access to these resources through thin client computing devices. A thin client is a computing device or program that relies on another device for computational power.

### Approach

With limited funding to invest in a completely new infrastructure for the virtual desktop implementation, TTB examined its existing hardware, software and technical expertise to determine the path most likely to succeed and achieve the objectives of providing central access to all IT resources while achieving significant savings.

TTB attained considerable success with server virtualization. Approximately 80 percent of the Windows Servers and 20 percent of the Sun Solaris servers at TTB had been virtualized. With this success in hand, TTB was confident that a virtual desktop infrastructure could be built without purchasing numerous physical servers. The infrastructure required to deliver virtual desktop could itself be largely virtualized.

Because TTB was established in 2003 with a significant number of personnel working full time from home, it was imperative from the beginning to support those personnel with a robust remote access capability. Additionally, TTB wanted to take advantage of its investment in Citrix licenses and the significant expertise its technical personnel had gained with the Citrix product suite as they supported remote access. The Citrix virtual desktop offering uses a small browser plugin called Citrix Receiver, which is freely available for download and turns most any device into a thin device. This solution was selected because the Citrix Receiver allows TTB to create thin client devices and support BYOD (initially home computers).

The currently deployed solution has 2 active sites, each with 3 physical servers. Either site can support the entire customer base. The rest of the virtual desktop servers are virtualized. In essence, TTB supports the entire population (650 personnel total in TTB, CDFI, and contractors) with 6 physical servers. Figure 1 is a conceptual view of the TTB virtual desktop.

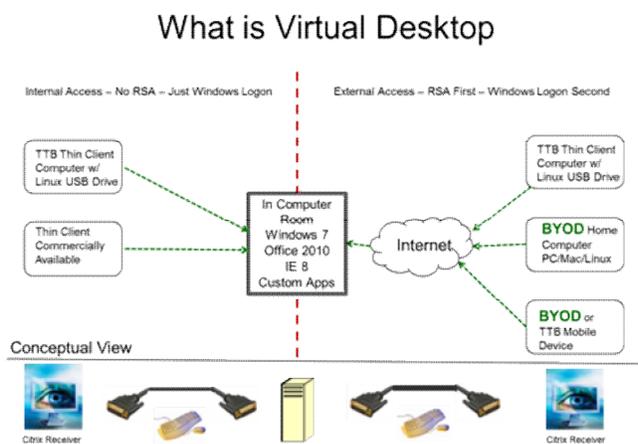


Figure 1

### Results

Today about 70 percent of TTB personnel access all TTB computing resources through thin devices, provided by TTB as well as BYOD. There is no typical user setup. If the desired user configuration works, TTB allows it. As an example, a TTB attorney uses a thin client device in the office, a BYOD Mac personal computer when working from home, and a BYOD iPad device when on the road. Several TTB personnel use BYOD Kindle Fire devices for occasional access, for example, if they need to check email when out of the office or they need to approve a time card that was not ready when they were in the office.

The rapid pace of change in the mobile device market makes the virtual desktop solution particularly attractive. Because no data touches the user device, there is no need for a mobile device management (MDM) solution on a non-TTB device. When a device is made available to the public it can be used to access TTB applications and data. The Droid Razr smart phone with a Motorola Lapdock 500 is an example of such a device. A user who has a government-provided smart phone (MDM installed) with a Lapdock would not need an additional computing device. Further, a user who had the same setup, minus the MDM, also could work full time with this BYOD. The ASUS Transformer is another example of a newly available mobile device that has a form factor usable for full-time work. The multiple-device access capability of virtual desktop allows TTB to move toward providing a single device per user.

The final result, which is likely the greatest benefit of the TTB Virtual Desktop solution relative to BYOD, is the minimization or elimination of complex legal and policy issues. Because no data touches the BYOD device and no work is physically accomplished on the BYOD equipment, all requests for discovery of information from a user's computer can be satisfied without having to recover anything from the user's personal device.

#### Lessons Learned

- The primary TTB BYOD lesson learned is to avoid allowing data to touch the personal device. Having all data, settings and processing in a central location and using the BYOD device simply as a viewer significantly simplifies the legal and policy implications.

#### Hardware/Software

- VMware for server virtualization
- 6 Dell R910 physical servers
- Citrix XenDesktop, XenApp, XenClient (pilot), Receiver, Citrix Provisioning Services
- Netscalers for remote access
- Robust Storage Area Network and Core Network required

#### Disclaimer

- References to the product and/or service names of the hardware and/or software products used in this case study do not constitute an endorsement of such hardware and/or software products.

[Back to top](#)



### U.S. Equal Employment Opportunity Commission (EEOC) BYOD Pilot

*Transitioning from Blackberry Usage to Bring-Your-Own-Device*

July 11, 2012

Kimberly Hancher  
 Chief Information Officer  
 U.S. Equal Employment Opportunity Commission  
[kimberly.hancher@eoc.gov](mailto:kimberly.hancher@eoc.gov)

#### Executive Summary

The U.S. Equal Employment Opportunity Commission (EEOC) recently implemented a Bring-Your-Own-Device (BYOD) pilot program to meet urgent IT budget challenges. Employees who want to use their own smartphone for official work purposes must agree to have third-party software installed. This allows the agency to manage security settings on the devices and remotely wipe devices clean of government emails and data if they are lost or stolen.

The EEOC is among the first Federal agencies to implement a BYOD pilot and the preliminary results appear promising. Last year, the EEOC was paying \$800,000 for its Government issued BlackBerry devices. Subsequently, the EEOC's FY2012 IT budget was cut from \$17.6 million to \$15 million, nearly a 15% reduction. The EEOC's Chief Information Officer, Kimberly Hancher, significantly reduced contractor services, eliminated some software maintenance, and slashed the agency's budget for mobile devices -- leaving only \$400,000 allocated for Fiscal Year 2012. Along with the other cost reduction measures, CIO Hancher took the issue to the agency's IT Investment Review Board. She suggested a two-pronged approach to cost reduction:

1. Optimize rate plans for agency provided mobile devices, and
2. Implement a BYOD pilot program.

In November 2011, EEOC's IT staff pressed the wireless carrier, a GSA Networkx contract provider, to help cut costs or risk losing the EEOC's BlackBerry business. Although the carrier was initially reluctant to work expeditiously, the EEOC stood firm in pursuing rate plan optimization. Zero-use devices were eliminated and all remaining devices were moved to a bundled rate plan with shared minutes. FY 2012 costs were reduced by roughly \$240,000 through these actions.

The next step was to launch a BYOD pilot program focused on enticing current users of Government provided BlackBerry devices to opt out. For months, EEOC's Hancher worked with information security staff, agency attorneys and the employees' union to draft rules that balanced employee privacy and Government security. By June 2012 many BlackBerry users "opted out" and voluntarily joined the BYOD pilot program.

EEOC's BYOD pilot focused on providing employees with access to agency email, calendars, contacts and tasks. With the mobile device management software, employees may read and write emails with or without Internet connectivity. A few senior executives who own Apple iPads will be provided "privileged" access to the agency's internal systems through the secure Virtual Private Network (VPN).

#### **BYOD Challenge**

The EEOC's BYOD program grew out of the necessity of meeting new budget challenges with limited resources. The agency was faced with a 15 percent reduction in its IT operating budget for FY 2012. At first, it was not evident there was much room for needed cuts. Therefore, EEOC decided to conduct research into how employees were using their agency-issued Blackberry devices – and the results were surprising:

*"Seventy-five percent of our users never made phone calls from their BlackBerrys," according to Hancher. "Email is the killer app. They either used the phone on their desk or they used their personal cell phone to make calls because it's just easier. We also found there were a number of zero-use devices. People have them parked in their desk drawer, and the only time they use it is when they travel."*

During the first quarter of FY 2012, initial efforts went into cutting the recurring costs of the nearly 550 agency-issued Blackberry devices. After conducting an analysis of device usage, the EEOC swiftly submitted orders to the carrier eliminating zero-use devices, demanded that disconnect orders were promptly terminated, and called for remaining Government devices to be moved to a bundled plan with shared voice minutes and unlimited data.

In December 2011, the EEOC launched the first official phase of its BYOD pilot. A BYOD advisory group was created to help the Office of Information Technology flesh out the new program. The advisory group was asked to identify cloud providers for mobile device management, identify security risks, research privacy concerns, draft Rules of Behavior, and create an internal website on the agency's intranet. The advisory group worked for months to socialize the concept of BYOD within the agency's workforce. In turn, nearly 40 employees volunteered to exchange EEOC-issued BlackBerry devices in favor of using their own personal smartphones.

#### **Alpha Phase**

During the alpha phase of the BYOD pilot, the EEOC's IT group worked with the mobile device management cloud provider to configure the exchange of electronic mail between the providers' host and the EEOC's email gateway. The IT staff was enthusiastic about the transition to a cloud provider, having managed the agency's BlackBerry Enterprise Services (BES) for many years. The cloud provider would assist with setup, configuration and end-user support. Under the BYOD pilot, the cloud provider conducts all technical support for pilot participants with iOS devices (iPhone and iPads), as well as all Android devices (smartphones and tablets). The EEOC decided to use its existing on-premise BES for additional support as needed.

Within the first few months of alpha pilot's launch, the advisory group reached out to other federal agencies to examine their BYOD programs. The EEOC's first draft of the BYOD Rules of Behavior was circulated among the advisory group, the technical team and the IT Security Officers.

After a number of revisions, the draft policy was ready to share with the union. The Deputy CIO and Chief IT Security Officer met with the union several times to discuss the issues. Again, the Rules of Behavior document was revised and improved upon. An "expectation of privacy" notice was written in bold on Page 1 of the four-page policy.

In March 2012, the BYOD team solicited feedback from the alpha team. A work breakdown structure was created to guide activities and tasks that needed to be completed before launching the next phase of the pilot -- the beta phase. Then, in June 2012, the EEOC provided several choices for the 468 employees who still used agency-issued BlackBerry devices:

- 1. Voluntarily return your BlackBerry and bring your own Android, Apple or BlackBerry smartphone or tablet to work.**
- 2. Return your BlackBerry and get a Government-issued cell phone with voice features only.**
- 3. Keep your BlackBerry with the understanding that EEOC does not have replacement devices.**

The BYOD pilot is expected to run through September 2012, or longer, depending on the agency's comfort level that all policy issues have been appropriately addressed. CIO Hancher projects between 10 percent and 30 percent of BlackBerry users will opt in for the BYOD program. The CIO examined incorporating an incentive to opt out, but could not find a precedent for offering a nominal stipend or reimbursement for business expenses and equipment allocation. Therefore, EEOC decided to proceed with the BYOD pilot and to revisit other outstanding issues once Government-wide BYOD guidance was released. In order to protect sensitive corporate data, EEOC is scheduling some BYOD orientation sessions to train its workforce on critical security ramifications and procedures.

One goal of EEOC's BYOD pilot is to obtain feedback and comment on the first version of the Rules of Behavior. The CIO fully expects modifications to the BYOD policy as the pilot evolves. Some outstanding questions, for example, include whether an enforceable waiver should be added exempting employees from holding the organization accountable. Can the agency offer an equipment allocation or reimbursement for a portion of the data/voice services?

#### **Acceptable Behavior Policy**

EEOC is currently in the process of reviewing and revising its Acceptable Behavior Policy for personal mobile devices. The policy document was developed as part of a working group that included the agency's Office of Legal Counsel. Employees who choose to opt into the BYOD program are required to read and sign the policy document first.

CIO Hancher said one thing agencies need to make sure of is that they have documented rules for what employees can and cannot do with Government data on personally-owned devices. Moreover, she said that employees must agree to let agencies examine those devices should it become necessary. EEOC's IT staff is meeting with employees to help decide which device or devices to use and what the likely effects will be. At the current time, personal smartphone devices are the only mobility option for new employees at EEOC.

#### BYOD Pilot Results

From 2008 to 2011, EEOC's BlackBerry provisioning program grew from about 100 devices to approximately 550 devices. By December 2011 about 23% of the workforce was provided with Government-issued smartphones. Realizing that this pattern was unsustainable, CIO Hancher, with support from the executive leadership and the union, set out to revamp the mobile device program.

The initial alpha pilot was launched with 40 volunteers who turned in their Government BlackBerry in favor of using a personally owned smartphone/tablet (Android, Apple iOS or BlackBerry). EEOC used cloud based, software-as-a-service for wireless synchronization of agency email, calendar and contacts, as well as mobile device management services.

Within the first three months of 2012, the number of BlackBerry devices was cut from 550 to 462 and monthly recurring costs were lowered by 20-30% by optimizing the rate plans. By June 2012, EEOC launched the beta pilot inviting all BlackBerry users to opt in to BYOD and return their BlackBerry. However, EEOC will allow employees to continue using an EEOC provided BlackBerry if they choose not to opt into BYOD.

The current BYOD program requires employees to pay for all voice and data usage, including those for official work purposes. This cost issue may prompt some users to keep the BlackBerry. However, for EEOC's younger employees, their personal devices appear to be an extension of their personalities, so to speak. For seasoned workers, their personal device allows them to do administrative work from home.

*"While I'm not advocating working 24 by 7, it is just more comfortable to sit and do timecard approvals on a Friday night in the comfort of your home instead of during the prime time work day when your attention should be on more complex and business-oriented issues,"* said CIO Hancher.

#### Lessons Learned

- **Socialize the concept of BYOD.** Since this a new concept and the acronym is taking time to be universally recognized, it is advisable to spend time explaining the BYOD concept to the workforce, including at senior staff meetings and executive council sessions.
- **Work with the agency's Legal Counsel and unions early in the process.** Allow input on the BYOD program and policies from leadership officials.
- **Select important security features for implementation.** Work to identify prioritized security settings or policies, implement them carefully, then cycle back to identify additional security measures after the first set are completed.

#### Hardware/Software

- Notifylink MDM – Cloud provider licensed at \$120 per user per year
- GW Mail and GW calendar – \$5 apps available through iTunes and Android Market

#### Disclaimer:

- References to the product and/or service names of the hardware and/or software applications used in this case study do not constitute an endorsement of such hardware and/or software products.

[Back to top](#)



#### State of Delaware BYOD Program

*Transitioning from State-owned Blackberries to a Personal Device Reimbursement Plan*  
July 16, 2012

William B. Hickox  
Chief Operating Officer  
Delaware Department of Technology & Information  
[William.Hickox@state.de.us](mailto:William.Hickox@state.de.us)

#### Executive Summary

In an effort to keep up with the pace of mobile technology, the State of Delaware initiated an effort to not only embrace the concept of BYOD but to realize significant savings by having state employees turn in their state owned device in favor of a personally owned device. In order to encourage the behavior, the State agreed to

reimburse a flat amount for an employee using their personal device or cell phone for state business. It was expected that by taking this action the State could stand to save \$2.5 million or approximately half of the current wireless expenditure.

There were several challenges including questions about whether a reimbursement was taxable or not, whether the personal device could be secured by the State for Freedom of Information Act (FOIA) requests, and whether utilization of personal devices could/should be mandated. In the end the state decided to make the program voluntary at this time. The state recognizes that not all employees have a personal device or are willing to utilize it for work purposes.

The State of Delaware experience to date has been positive with specific savings and device reductions. The State anticipates continuing to grow the program by limiting the number of state owned devices while encouraging the use of personal devices into the future.

### Challenge

The State's Blackberry infrastructure is reaching end of life and requires a lifecycle replacement. In addition, changes in technology are driving agencies to request devices that are not state standard or currently supported by the Department of Technology & Information (DTI). As such, the State is now at a decision point regarding the future direction of portable wireless devices and the ongoing support of the infrastructure.

Over the last 10 years the nature and use of portable wireless devices in the workplace has changed dramatically. Originally, only a handful of state owned devices (BlackBerrys) existed with the majority of staff relying on state owned cell phones. In addition, at that time very few state employees had personal cell phones and almost none had personal blackberry devices. Today, the proliferation of these state owned devices (approximately 2500 devices) results in significant costs associated with the infrastructure and support of the blackberry system. In addition, due to the changing needs of the agencies, more and different devices such as Droids and iPhones are being requested, which would expand the costs associated with infrastructure and support. The current Blackberry Enterprise Server (BES) which is managed by the state will reach its end of life within the next year and require replacement. However, replacing the BES will only address the state owned devices that are currently approved as standard (Blackberry). It does not address the request for additional portable devices such as iPhones.

### Approach

DTI decided that funds should not be expended to lifecycle the BES. Instead, the State should start a two year transition plan to migrate all users off of the existing infrastructure by June 30, 2013 and move them to either a personal device through a proposed reimbursement program or to a device that runs directly through the state's wireless carrier. By doing so, the state stands to save up to \$2.5 million dollars annually through the reimbursement program but also would save \$75K in lifecycle costs and \$120K in ongoing support. This direction would also allow agencies to utilize enhanced devices such as Droids and iPhones to support their business needs.

The above referenced reimbursement program would be as follows:

Beginning February 1, 2011 the Department of Technology and Information (DTI) will initiate a program aimed at reducing the number of state owned wireless communication devices, i.e. cellular phones, PDAs, portable devices, etc. The intended benefits of this program are twofold. Many employees carry personal devices in addition to the state issued device. With the advances in technology, efficiencies can be gained through the combination of these devices. In addition to end user efficiency, by combining devices, there is significant savings for the State.

Employees whose job duties require the frequent need for a cell phone or portable device as determined by their supervisor may receive a monthly voice/data plan reimbursement to cover the costs of state related business. Only in extenuating circumstances will further reimbursement for voice/data plan costs be available to employees who participate. All other employees may submit infrequent business-related cell phone expenses for individual reimbursement.

**Determining Employee Eligibility:** Employees with job duties that require the frequent need to use a cell phone/PDA for business purpose are eligible, typically include;

- Employees on the road or in the field, but required to remain in touch with others, typically out of the office on business 50 or more annual days.
- Employees available for emergency contact (e.g., duties require them to be contacted anywhere/anytime).
- Employees with 24/7 response requirements.

**Dollar Amount of Reimbursement:** Eligible employees will receive a reimbursement as follows:

- Voice only - \$10 per month
- Data only - \$30 per month
- Voice/Data - \$40 per month

### Results

For the employees that have participated, the State has reduced the expense associated with their devices by 45%. This has resulted in an overall reduction of departmental wireless costs of 15%. As the State continues to grow the program it expects its overall wireless cost savings to continue to grow. While it started out with only DTI participation, it now has Department of Corrections, Department of Transportation, Department of Health and Social Services, and the Governor's Office participation. Altogether the State of Delaware is currently reimbursing over 100 employees for utilizing their personal device and over 1,000 State of Delaware employees are using their personal devices in the BYOD program.

### Lessons Learned

- When discussing reimbursement, the State had to ensure that it was not providing a stipend, but in fact a reimbursement after the fact. As such, employees are required to submit an already paid wireless bill that is then processed for reimbursement under the monetary guidelines set above. This avoids the issue associated with stipends being taxable under the IRS regulations.
- Freedom of Information Act requests were another sticking point. However, the State has been able to avoid the issue since all of the state's e-mail is centralized and a copy of every transaction is maintained on the central servers which results in a clean copy being available for discovery if necessary.
- A current challenge is the State's inability to grow the reimbursement program as fast as it would like. This is due to the fact that the wireless carriers are now placing limits on data which has resulted in employees unwilling to agree to use their personal device for work since they no longer have unlimited data and the State will not provide additional reimbursement if employees go over the data maximum.

#### Disclaimer

- References to the product and/or service names of the hardware and/or software applications used in this case study do not constitute an endorsement of such hardware and/or software products.

#### Example Policies

The BYOD Working Group assembled sample policies in use at agencies to help inform IT leaders who are considering developing a BYOD program for their agencies.

Sample policies include:

- [Sample #1: Policy and Guidelines for Government-Provided Mobile Device Usage](#)
- [Sample #2: Bring Your Own Device – Policy and Rules of Behavior](#)
- [Sample #3: Mobile Information Technology Device Policy](#)
- [Sample #4: Wireless Communication Reimbursement Program](#)
- [Sample #5: Portable Wireless Network Access Device Policy](#)

#### Sample #1: Policy and Guidelines for Government-Provided Mobile Device Usage

Version X, [DATE]

The following policy and guidelines inform government-provided mobile device users of their allowable usage and features available for business and limited personal use. This document also serves to make clear the responsibility of mobile device users to take proper care of the government furnished equipment entrusted to them. Mobile device care is the responsibility of each mobile device user. Failure to adhere to the guidelines listed below may result in personal liability and/or retraction of device privileges.

The new standard monthly rate plans for [AGENCY NAME] issued Blackberry devices include:

- Voice - 300 "anytime" minutes within the Continental US (CONUS), per device.
- Data - unlimited data (e-mail and Internet access) within the CONUS.
- Unlimited Nights (9 pm – 6 am) and Weekends (9 pm Friday to 6 am Monday)
- Unlimited [PRODUCT NAME] to [PRODUCT NAME] Calling
- Unlimited Domestic Text Messaging
- Everyone is on a bundled voice/data plan with shared voice.

(Government-Provided Cell Phones follow same Voice/Text parameters, No Data)

[AGENCY NAME] expects mobile-device users to:

- Protect their government-issued device from theft, damage, abuse, and unauthorized use;
- If the device is lost or stolen, the user will notify the [AGENCY NAME] Help Desk ([AGENCY HELPDESK PHONE] or [AGENCY HELPDESK EMAIL]) within one hour, or as soon as practical after you notice the device is missing. [AGENCY OFFICE OF INFORMATION TECHNOLOGY] will lock and disable the device upon notification. A lost or stolen device will be replaced a maximum of three times, pending availability of devices and funding;
- Maintain usage within the plan parameters identified above. If your business use requirements are dramatically different than the standard plan, you must contact [AGENCY OFFICE OF INFORMATION TECHNOLOGY] to discuss other available options; Comply with [AGENCY NAME] appropriate use policies when using the device ([REFERENCE AGENCY APPROPRIATE USE POLICIES]);
- Abide by the law governing the use of mobile cell phones and/or smartphones while driving (e.g., hands-free use and/or texting); and
- Purchase any additional mobile device accessories (e.g., holsters, cases, car chargers, screen protectors, Bluetooth headsets, etc.) that the user may desire in addition to the items provided by the government.

#### Privacy Expectations:

Government employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at anytime, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed-through that device.

#### Additional Guidelines:

- [AGENCY NAME] Office of Information Technology (OIT) has complete oversight and management of device usage and expenses.
- The government-provided devices are being provided as a productivity tool for business use. OIT reserves the right to terminate services for non-use, limited business use, or excessive personal use. The policy for terminating voice and data services for non-usage is 30 days.
- Due to voice plan minute restrictions, employees should opt to use their work landline phone, when at their workstation, to make and receive calls.
- [AGENCY NAME] staff are permitted limited use of Government IT equipment for personal needs if the use does not interfere with official business and imposes no additional expense to the Government. Since voice minutes on the government's plan are limited, personal phone calls should be limited to brief occasional calls. Calls that are made during the weekend, evening (9 pm – 6 am), or to other [PRODUCT NAME] customers do not count against plan minutes. The government plan provides unlimited data, so limited personal Internet use is permitted, but should occur during non-work time. All limited personal use must be in compliance with [AGENCY NAME] appropriate use policies.
- Mobile device selection and issuance is based on availability on the GSA contract and certified FIPS 140-2 encryption standard compliance. At this time, only RIM Blackberry devices are certified as compliant with this standard.
- Assistance or support is handled by the [AGENCY NAME] Helpdesk by calling [AGENCY HELPDESK PHONE] or emailing [AGENCY HELPDESK EMAIL].
- International roaming services may be available on a temporary basis for business travel only. Data rate plans for e-mail and broadband cards are an additional cost to [AGENCY NAME] for mobile device users traveling outside the CONUS. Contact OIT 30 days prior to travel to request temporary international roaming feature if you have official government travel plans abroad. Failure to add the international roaming feature could result in cost overages for which the Agency will not be responsible.
- [AGENCY NAME] reserves the right to recall/disconnect government-provided mobile devices due to budget restrictions or changes to deployment priorities.

Questions related to the above Policy and Guidelines should be directed to the [AGENCY NAME] Helpdesk.

## Sample #2: Bring Your Own Device – Policy and Rules of Behavior

[AGENCY NAME]

(Version X, [DATE])

This document provides policies, standards, and rules of behavior (ROB) for the use of personally-owned smart phones and/or tablets by [AGENCY NAME] employees (herein referred to as users) to access [AGENCY NAME] network resources. Access to and continued use of network services is granted on condition that each user reads, signs, respects, and follows the [AGENCY NAME]'s policies concerning the use of these devices and services.

The Office of Information Technology (OIT) is piloting a "Bring Your Own Device" (BOYD) program to permit agency personnel to use personally owned smart phones and tablets for business purpose. The policy and ROB vary depending on service usage, as outlined below.

### Current Devices Approved for Use During BYOD Pilot:

Android Smart Phones & Tablets  
Blackberry Smart Phones & Playbook  
iOS iPhones & iPads

**Expectation of Privacy:** [AGENCY NAME] will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads government email/attachments/documents to their personal device). This differs from policy for government-provided equipment/services, where government employees do not have the right, nor should they have the expectation, of privacy while using government equipment or services. While access to the personal device itself is restricted, [AGENCY NAME] Policy and Rules of Behavior regarding the use/access of government e-mail and other government system/service remains in effect. If there are questions related to compliance with the below security requirements, the user may opt to drop out of the BYOD program versus providing the device to technicians for compliance verification.

With the use of [PRODUCT NAME] (standard [PRODUCT NAME] access via Internet/Web Browser) and/or [PRODUCT NAME] Products, business e-mails are accessed across the Internet and are NOT downloaded to the device; therefore, there are no additional security requirements other than the Overall Requirements noted in Section I.

The Notify-Link is a cloud based mobility solution that provides secure, real-time synchronization of email, calendar, and contacts to and from the Apple/Android devices. With Notify-Link, users have the ability to compose, reply, forward, or delete their email while mobile, as well as open a variety of email attachment formats. With the use of Notify Link Apps, business e-mails and appointments are downloaded and stored on the device, so additional security requirements are necessary.

Users of personally-owned Blackberry Devices can have their device incorporated into the [AGENCY NAME] BES environment, assuming the device meets compatibility requirements (to include Verizon service & model eligibility – contact [AGENCY NAME] OIT for specific requirements).

Document Transfer involves connecting the personal device to the user's work PC via USB connections for file-sharing (document transfer) or backup purposes. It also includes backing up data/documents to external sources, such as cloud storage services.

VPN BYOD access is available for senior executives or management and requires approval of the Chief Information Officer (CIO). Currently this access is only available for Apple iOS iPad devices. Access is not been approved for Android devices.

### I. Overall Requirements for all BYODs Accessing [AGENCY NAME] Network Services:

- User will not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or agency financial operations. This excludes government e-mail that is protected through the various security controls listed below;
- User will password protect the device;

- User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not “Jail Break” the device (installing software that allows the user to bypass standard built-in security features and controls);
  - User agrees that the device will not be shared with other individuals or family members, due to the business use of the device (potential access to government e-mail, etc);
  - User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments. [AGENCY NAME] OIT will provide instructions for identifying and removing these unintended file downloads. Follow the premise, “When in Doubt, Delete it Out.”
- II. Accessing [PRODUCT NAME] (e-Mail/Calendar) Services on BYOD
- a. Use [PRODUCT NAME] or [PRODUCT NAME]
- b. Use of Notify-Link Applications
- As a default, Notify-Link will be enabled to perform an e-mail wipe on the phone after 25 password failed attempts (please be advised that only e-mail on the device will be deleted);
  - If the device is lost or stolen, the user will notify the [AGENCY NAME] Help Desk ([AGENCY HELPDESK PHONE] or [AGENCY HELPDESK EMAIL]) within one hour, or as soon as practical after you notice the device is missing. [AGENCY NAME] OIT will lock the device, e-mail on the device will be deleted, and notify-link services will be deactivated;
  - Users must comply with all [AGENCY NAME] password policies, including use of strong passwords, password expiration (6 months), and password history (3).
  - [AGENCY NAME] reserves the right to terminate government-provided Notify-Link services for non-use. The policy for terminating Notify-Link services in 30 days.
- c. Use of Blackberry Enterprise Server (BES)
- User will allow [AGENCY NAME] to enforce standard [AGENCY NAME] BES policies on the personal device, with the exception that the user will be allowed to download third-party apps to personal device;
  - If the device is lost or stolen, the user will notify the [AGENCY NAME] Help Desk ([AGENCY HELPDESK PHONE] or [AGENCY HELPDESK EMAIL]) within one hour, or as soon as practical after you notice the device is missing. OIT will lock the device, e-mail on the device will be deleted, and BES services will be deactivated.
- III. Document Transfer
- a. USB Connection to Work PC
- Only BYODs that provide FIPS 140-2 device-level encryption may be connected to [AGENCY NAME] PCs for document transfer purposes (currently only Blackberry devices are certified as 140-2 compliant);
  - User will enable use of a second strong password for authentication upon connection to the PC. This password should be different from the primary device password;
  - User will maintain anti-virus (AV) protection on the device ([AGENCY NAME] - provided or other). The AV software in use will be identified at the end of this document for review/approval by OIT; and
  - User will not download/transfer business data that is considered sensitive or confidential to the personal device, including charge/case-related documents that contain personally identifiable information.
- b. Backing-Up / Storing documents on non-[AGENCY NAME] Servers
- User will not download/transfer sensitive [AGENCY NAME] business data/documents to any non-[AGENCY NAME] device.
- IV. Use of Virtual Private Network (VPN) to access Network Services
- Users must have a need to access internal [AGENCY NAME] resources, such as the Integrated Mission System, Document Management System, Network drives, etc., as required by her/his position and duties
  - Users may only use [AGENCY NAME] approved and configured VPN client software to access [AGENCY NAME]'s VPN;
  - Users must allow [AGENCY NAME] administrators to install Trend Micro security suite (firewall, antivirus, and web site protector applications) on their personal device;
  - Users must comply with all [AGENCY NAME] Password Policies on their device, including use of strong passwords, password expiration (6 months), and password history (3).
  - Users will immediately notify OIT if the device is lost or stolen, at which point [AGENCY NAME] will lock the device using Trend Micro and disable the user's VPN access.

#### USER ACKNOWLEDGMENT AND AGREEMENT

It is [AGENCY NAME]'s right to restrict or rescind computing privileges, or take other administrative or legal action due to failure to comply with the above referenced Policy and Rules of Behavior. Violation of these rules may be grounds for disciplinary action up to and including removal.

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of [AGENCY NAME] services. I understand that addition of government-provided third party software (such as Ghost-Pattern, Notify Link, Airwatch, Good, etc) may decrease the available memory or storage on my personal device and that [AGENCY NAME] is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program. I understand that contacting vendors for trouble-shooting and support of third-party software is my responsibility, with limited configuration support and advice provided by [AGENCY NAME] OIT. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that government reimbursement of any business related data/voice plan usage of my personal device is not provided.

Should I later decide to discontinue my participation in the BYOD Program, I will allow the government to remove and disable any government provided third-party software and services from my personal device,

Employee Name: \_\_\_\_\_

BYOD Device(s): \_\_\_\_\_

Services to be Used: \_\_\_\_\_

Anti-Virus or other Security Software installed on the Device: \_\_\_\_\_

Employee Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Sample #3: Mobile Information Technology Device Policy

Effective Date:[DATE]

Responsible Office:[OFFICE NAME]

Updated: (To accommodate access for personally owned devices - BYOD)

## 1.0 Purpose

This sets forth the security control standards for the issuance, administration, use, and security of mobile information technology (IT) devices that are used to conduct [AGENCY NAME] business. These standards are established to protect [AGENCY NAME] information on mobile IT devices, which consist of any non-stationary electronic apparatus with capabilities of recording, storing, and/or transmitting data, voice, video, or photo images and include laptops, personal digital assistants (PDAs), cellular phones, satellite phones, digital tablets, secure tokens, and any related storage media or peripheral devices (e.g. CDs, flash memory, Internet Air Cards, etc.).

## 2.0 Authorities

OMB Circular A-130, Clinger-Cohen Act, Federal Information Security Management Act, NIST SP 800-124, and NIST SP 800-53.

## 3.0 Policy

It is the policy of the [AGENCY NAME] to develop and maintain security control standards for all [AGENCY NAME] owned, mobile IT devices that create, access, process or store Agency information, and the information created, collected, and processed on behalf of [AGENCY NAME] on these devices. This policy also covers personally owned mobile IT devices that access or store Agency information. These standards are part of the overall [AGENCY NAME] Information Security Program authorized by [AGENCY SECURITY DOCUMENTATION NAME] and must be followed by all [AGENCY NAME] employees, contract personnel, Volunteers, and Trainees. The Chief Information Officer (CIO) directs and oversees compliance with the security control standards for mobile IT devices.

## 4.0 Roles and Responsibilities

### 4.1 The Chief Information Officer

The CIO has overall responsibility for establishing the security standards for mobile IT devices and must:

- a. Procure all [AGENCY NAME] owned mobile IT devices for [AGENCY NAME] issuance and approve the types of personally owned devices that will be used.
- b. Assure that [AGENCY NAME] issued mobile IT devices are available for staff members with job functions that are mission critical to [AGENCY NAME] operations, or that protect the safety and security of [AGENCY NAME] staff or Volunteers.
- c. Provide for the distribution, operation, and administrative support of issued mobile IT devices.
- d. Maintain an inventory of [AGENCY NAME] mobile IT devices by serial number, user's office, user's name, and service start/end dates.
- e. Maintain an inventory of licenses for [AGENCY NAME] owned software installed on each personally owned and [AGENCY NAME] owned mobile IT device.
- f. Establish and maintain security configurations for all issued mobile IT devices, including patching and upgrading of software/firmware.
- g. Log and monitor the activity on all issued devices for compliance with the Rules of Behavior for General Users.
- h. Develop the [AGENCY NAME] Remote Access and Mobile Information Technology User Guide.

### 4.2 Supervisors

Supervisors of [AGENCY NAME] staff who have applied for, or have been issued, mobile IT devices or wish to use personal mobile IT devices to conduct [AGENCY NAME] business must:

- a. Ensure compliance with managerial requirements as described in the [AGENCY NAME] Remote Access and Mobile Information Technology Guide.
- b. Sign and approve the Mobile IT Device User Agreement Form for each user that they supervise.
- c. Report the lost, stolen, damaged, destroyed, compromised or non-functional [AGENCY NAME] issued mobile device to the [PROPER AUTHORITY].
- d. Confirm that the lost, stolen, damaged, destroyed, compromised, or non-functional IT device has been reported to the [AGENCY NAME] Service Desk by the user.

### 4.3 Users

Users who conduct official [AGENCY NAME] business on a mobile IT device must:

- a. Sign the Remote Access and Mobile IT Device User Agreement Form.
- b. Operate the device in compliance with this policy, all applicable federal requirements, and the [AGENCY NAME] Remote Access and Mobile Information Technology Guide.
- c. Not process or access Classified information on the device.
- d. Use only approved and authorized [AGENCY NAME] owned devices to physically attach to [AGENCY NAME] IT systems.
- e. Store only the minimum amount, if any, of Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) necessary to do one's work, and immediately delete the PII or ePHI when no longer needed. Users shall receive written approval from their supervisor before accessing, processing, transmitting, or storing [AGENCY NAME] Sensitive Information such as PII or ePHI.
- f. Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.
- g. Immediately contact the [AGENCY NAME] Service Desk and their immediate supervisor if the IT device is lost, stolen, damaged, destroyed, compromised, or non-functional.

- h. Abide by all federal and local laws for using the device while operating a motor vehicle (e.g. users are banned from text messaging while driving federally owned vehicles, and text messaging to conduct [AGENCY NAME] business while driving non-government vehicles).

Users who are issued a [AGENCY NAME] owned mobile IT device must also:

- Comply with [AGENCY TECHNOLOGY POLICY].
- Not disable or alter security features on the device.
- Only use the [AGENCY NAME] owned device for official government use and limited personal use.
- Reimburse the OCIO for any personal charges incurred that are above the established fixed cost for the Agency's use of the device (e.g. roaming charges incurred for personal calls).
- Be required to reimburse the [AGENCY NAME] if the mobile IT device is lost, stolen, damaged or destroyed as a result of negligence, improper use, or willful action on the employee's part and if determined by the [PROPER AUTHORITY].

#### 5.0 Effective Date

The effective date is the date of issuance.

### Sample #4: Wireless Communication Reimbursement Program

#### POLICY STATEMENT

Beginning [DATE], the [AGENCY NAME] will initiate a program aimed at reducing the number of government-owned wireless communication devices (i.e. cellular phones, PDAs, portable devices, etc). The intended benefits of this program are twofold: Many employees carry personal devices in addition to the government-issued device. With the advances in technology, efficiencies can be gained through the combination of these devices. In addition to end-user efficiency, combining devices means significant savings for the government.

Employees whose job duties require the frequent need for a cell phone or portable device as determined by their supervisor may receive a monthly voice/data plan reimbursement to cover the costs of government-related business. Only in extenuating circumstances will further reimbursement for voice/data plan costs be available to employees who participate. All other employees may submit infrequent business-related cell phone expenses for individual reimbursement.

#### USE OF PERSONAL CELL PHONE/PORTABLE DEVICE FOR BUSINESS PURPOSES

**Determining Employee Eligibility:** Employees with job duties that require the frequent need to use a cell phone/PDA for business purpose are eligible, typically including:

- Employees with 24/7 response requirements.
- Employees available for emergency contact (e.g., duties require them to be contacted anywhere/anytime).
- Employees on the road or in the field (typically out of the office on business [XX] or more days annually) who are required to remain in touch with others.

**Dollar Amount of Reimbursement:** Eligible employees will receive a reimbursement as follows:

- Voice only - \$[XX] per month
- Data only - \$[XX] per month
- Voice/Data - \$[XX] per month

**Establishing the Payment of Reimbursement:** Complete the Mobile Device Reimbursement Request Form and submit to your supervisor for approval. Your supervisor will determine if the request meets the criteria and intent of the policy.

The reimbursement does not constitute an increase to base pay, and will not be included in the calculation of any salary adjustments.

**Payment to the Employee:** Payment will be made upon presentation of a completed Personal Reimbursement Form along with copies of the monthly device bill, but not more frequently than quarterly.

**Use of Device:** The employee must retain an active device as long as a device reimbursement is in place. The device may be used for both business and personal purposes. Extra services or equipment may be added at the employee's expense.

Users must agree to comply with [AGENCY NAME] security requirements for personal devices connecting to the government network. The specific requirements can be found at the following [link](#).

**Fees for Contract Changes or Cancellation:** The employee is responsible for all fees to change contracts and cancellation charges.

### Sample #5: Portable Wireless Network Access Device Policy

[AGENCY NAME]	
Doc Ref Number:	XXXX
Revision Number: XX	

<b>Document Type:</b>	Enterprise Policy	<b>Page:</b> 39 of 43
<b>Policy Title:</b>	Portable Wireless Network Access Device Policy	
<b>Synopsis:</b>	Establish rules for the use of the portable wireless network access device and its connection to the [AGENCY NAME] network.	
<b>Authority:</b>	LIST/CITE APPLICABLE FEDERAL/AGENCY RULES & REGULATIONS THAT ESTABLISH AUTHORITY	
<b>Applicability:</b>	All users of the [AGENCY NAME] communications and computing resources.	
<b>Effective Date:</b> [DATE]	<b>Expiration Date:</b> [DATE]	
<b>POC for Changes:</b> [AGENCY POC]		
<b>Approval By:</b> [AGENCY APPROVING AUTHORITY]		
<b>Approved On:</b> [DATE]		

## I. Policy

### POLICY SCOPE

This policy applies to all employees of the [AGENCY NAME] who use portable wireless devices capable of accessing [AGENCY NAME] computing resources. This policy describes the handheld wireless network access system implementation, recommends guidelines for usage and lists policies and procedures that apply to its use. Portable wireless network access devices are provided to improve customer service and enhance government efficiencies and will only be provided to employees whose Managers have determined that the employee has a demonstrated need.

The purpose of this policy is to establish rules for the use of portable wireless computing devices and their connection to the [AGENCY NAME] network. These rules are necessary to preserve the integrity, availability and confidentiality of the [AGENCY NAME] network.

### POLICY STATEMENT

Those employees of the [AGENCY NAME] who have a need for immediate notification and access to email, voice and web services while away from their office or in a mobile situation are candidates for use of a portable wireless network access device. All usage is covered by [AGENCY NAME]'s Acceptable Use Policy. Primary use of the portable wireless network access device is for official [AGENCY NAME] business. Personal use of government-owned portable wireless network access devices (for email, calendar, incoming and outgoing telephone calls) shall be limited to infrequent, incidental and/or emergency use.

### POLICY PROVISIONS

Within each department, agency and/or component, the determining authority and responsibility for issuance of portable wireless network access device shall rest with the [COMPONENT APPROVING AUTHORITY] or similar approving authority.

Final authority and wireless activation of each new wireless network access device shall rest with the [AGENCY NAME] Chief Information Officer or his/her designee.

[AGENCY NAME] shall implement appropriate process and controls over the common server, infrastructure, transport services and computing resources under its control. Deployment of the portable wireless network access devices will be limited dependent on available resources.

Network security controls must not be bypassed or disabled. To the extent possible, security capabilities of the wireless device should be employed that are consistent with the [AGENCY NAME] Acceptable Use Policy. Use of any Cellular Telephone access shall be governed by the [AGENCY NAME] Cellular Telephone policy.

Violation of this policy may result in disciplinary action, loss of access privileges to the common server infrastructure, or civil and criminal prosecution.

### POLICY OVERVIEW

The [AGENCY NAME] supports portable wireless network access as a line of service for customers. Support of full integration of e-mail, calendaring, contacts, etc. into a portable wireless network access device is provided only for those customers articulating a clear business need for their employees.

Acquisition of portable wireless network access devices by customers requires the prior written approval of their [COMPONENT APPROVING AUTHORITY] or similar approving authority. Concurrence of the [AGENCY NAME] Chief Information Officer (CIO) or designee is required for new service or transfers.

**Note:** Only devices provided by [AGENCY NAME] will be connected to the network and supported by [AGENCY NAME].

Deployment of wireless network access devices will be limited, and will be authorized based on the following criteria:

- **Program Focus:** The purpose of portable wireless network access devices are to provide continued access to resources deemed necessary for providing continued support in maintaining the functionality of their agency's program. Without such device decisions may be delayed and the effectiveness of the program shall be reduced.
- **Available Resources:** Funds for the purchase and monthly subscription costs for portable wireless network access devices are the responsibility of the customer. Customers seeking to deploy portable wireless network access devices should clearly articulate the source of funds to support the upfront and ongoing costs, and also demonstrate a commensurate reduction in costs for other services where applicable. (For example, to the extent that deployment of these devices obviates the need to have staff utilize other wireless services – e.g., a wireless network card for a laptop computer – customers should quantify expected savings in their written request.)
- **Technology Supported:** [AGENCY NAME] has chosen to support the portable wireless network access devices which employ the Code Division Multiple Access (CDMA) telecommunications standard and will evaluate the technology as market conditions warrant to determine the most effective options for deploying this service.

#### RESPONSIBILITY

The [AGENCY NAME] [AGENCY POC] is responsible for the development and maintenance of the procedures to implement this policy. The administration, procedural and enforcement responsibilities of this policy may be delegated to other [AGENCY NAME] staff.

The requestor (Customer) is responsible for using the portable device in a manner consistent with the Acceptable Use Policy in an effort to provide continued customer service and enhance Department program mandates.

#### PROCEDURES

##### ACTIVATION OF A WIRELESS SERVICE

When a [COMPONENT APPROVING AUTHORITY] or similar approving authority signifies a [AGENCY NAME] employee requires a portable wireless network access device, they may submit a written request (the [AGENCY NAME] Telecommunications Portable Wireless Network Access Device Request Form) to [AGENCY NAME]. Funds for the purchase and monthly subscription costs for the device(s), user training, upgrades and maintenance are the responsibility of the requesting component and not the [AGENCY NAME].

#### II. Definitions

None.

#### III. Development and Revision History

Initial version established [DATE]

Reformatted version established [DATE]

Updated [DATE]

Appendix removed [DATE]

#### IV. Approval Signature Block

On File	
[SIGNATURE OF AGENCY APPROVING AUTHORITY]	
Name & Title:	Date
[NAME & TITLE OF AGENCY APPROVING AUTHORITY]	[DATE]

#### V. Listing of Appendices

None.

[Back to top](#)

[1] BYOD is a concept that allows employees to utilize their personally-owned technology devices to stay connected to, access data from, or complete tasks for their organizations. At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal tablets/eReaders, smartphones, and other devices. This could include laptop/desktop computers; however, since mature solutions for securing and supporting such devices already exist, this document focuses on the emerging use case of mobile devices.

[2] *NIST SP 800-124 Revision 1 (Draft), Guidelines for Managing and Securing Mobile Devices in the Enterprise* was released for comment on July 10<sup>th</sup>, 2012, and includes recommendations for securing personally-owned mobile devices. Later this year, NIST will also release for comment *NIST SP 800-114 Revision 1 (Draft), User's Guide to Telework and Bring Your Own Device (BYOD) Security* which will provide recommendations for securing BYOD devices used for telework and remote access, as well as those directly attached to the enterprise's own networks. NIST is also preparing *NIST SP 800-46 Revision 2 (Draft), Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* which will provide information on security considerations for several types of remote access solutions.

[3] Under the Federal Information Security Management Act of 2002 (FISMA) and related OMB policies and circulars, Agencies are required to follow mandatory standards and guidelines for information and information systems developed by the National Institute of Standards and Technology (NIST). These standards and guidelines should be used throughout the implementation of any BYOD program.

[4] Additional functions of MDM and MAM solutions may include: security (e.g., enforce data-in-transit encryption, data-at-rest encryption, strong authentication); network (e.g., control mobile network access, network roaming, network routing, data import/export, and use of Government gateways); system (e.g., control peripheral (dis)enablement); software (e.g., restrict application installation and force use of enterprise app stores); app store (e.g., centrally store, inspect, and manage distribution of applications); asset management and security compliance audits (e.g., routine / real-time scan of functions against enterprise policies); device jailbreak / rooting detection, system performance monitoring (e.g., processor, memory, storage, battery); peripheral status monitoring (e.g., camera, GPS, network access); device lock (e.g., timeout lock / enterprise lock); remote wipe (e.g., selective wipe / comprehensive wipe); quarantine malware / applications; device (de)activation; device configuration, restoration, or migration of profiles, services, software, policies, and files; active peripheral control (e.g. activate GPS to track lost device); enforced separation of content (e.g., personal, enterprise, classified, tactical); restricted content transfer across domains; enterprise / Web-based partitioning; over-the-air (OTA) provisioning; role/group-based access; enterprise platform integration and certification authority; help desk self-service administration; enterprise dashboard visibility, alerting, logging, troubleshooting; contract, expense, service usage management.

WWW.WHITEHOUSE.GOV

En español | Accessibility | Copyright Information | Privacy Policy | Contact  
USA.gov | Developers | Apply for a Job



# Appendix H



A Law Blog on Trade Secrets, Non-Competes, and Computer Fraud

[Home](#)

[About](#)

[Contact](#)

[Resources](#)

[Webinars](#)

[Events](#)

Published by Seyfarth Shaw LLP

# California Appellate Court Holds That Non-Compete Restriction in Stipulated Injunction Is Enforceable Because There Was No Showing That It Was Not Necessary to Protect Trade Secrets

By Daniel Joshua Salinas on October 11th, 2012

By Joshua Salinas and Robert Milligan

A California Court of Appeal recently reversed a trial court ruling that found a stipulated injunction preventing the solicitation of customers was invalid and unenforceable under California Business & Professions Code section 16000.

In *Wanke, Industrial, Commercial, Residential, Inc. v. Sup. Ct.*, 2012 WL 4711888 (Cal.App. 4 Dist., October 4, 2012), the Court of Appeal held that since the trial court could not conclude, based on the language of the stipulated injunction, that it does not protect the plaintiff's trade secrets, the court erred in concluding that it was an unlawful business restraint.

## Facts

Plaintiff Wanke is a southern California company that installs waterproofing systems. Defendants Scott Keck and Jacob Bozarth are former employees of Wanke that left Wanke to start their own competing waterproofing company, WP Solutions. Wanke brought action in late 2008 against Keck and Bozarth alleging that they misappropriated and misused Wanke's trade secrets and confidential information, and used that information to actively target and recruit Wanke's customers.

The parties ultimately resolved the action in 2009 by entering into a settlement and mutual general release agreement. Pursuant to the settlement agreement, Keck, Bozarth and WP Solutions agreed to a stipulated injunction, in which they would refrain from contacting or soliciting any customers listed on an agreed customer list for five years subject to certain exceptions. The stipulated injunction also provided for liquidated damages in the amount of \$50,000 for initial violations of the order, with the amounts increasing in increments of \$10,000 for each subsequent violation of the order, plus Wanke's attorneys' fees, costs, and expenses.

## Proceedings to Enforce the Stipulated Injunction

A dispute arose the following year when the defendants allegedly contacted and/or supplied labor and materials to a customer on the prohibited customer list, Con Am Management. Wanke subsequently filed an application for an order to show cause requesting the trial court to hold the defendants in contempt for having violated the stipulated injunction. Wanke also filed a motion to enforce the settlement agreement related to Con Am Management and requested the court order defendants to pay liquidated damages as provided in the stipulated injunction.

The trial court held a combined trial/hearing on Wanke's order to show cause for contempt and motion to enforce the settlement agreement. The trial ultimately court found that Wanke failed to establish the "existence of a lawful order," which is required before a party may be held in contempt of that order.



Specifically, the trial court determined that the stipulated injunction was invalid to the extent it prohibited defendants from soliciting any entity merely because the entity appeared on the customer list attached to the stipulated injunction. Citing Business and Professions Code section 16600, the trial court viewed the stipulated injunction as a non-compete agreement, which could only prohibit customer solicitation if the employee was utilizing trade secret information to solicit those customers.

The trial court found that the identity and location of Con Am Management was easily identifiable and thus, not a trade secret. To avoid striking down the injunction in its entirety, and thereby unwind the entire settlement and resolution between the parties, the trial court narrowed the application of the injunction only to the extent it was used to prohibit defendants from undertaking or proposing to undertake jobs from customers on the customer list while defendants were employed by Wanke. The trial court explained that only on these jobs can defendants be said to be using information they learned while employed at Wanke to identify customers with particular needs or characteristics that would be protectable under California law.

With respect to the motion to enforce the settlement agreement, the trial court ruled that no liquidated damages may be imposed because the alleged violations were not in fact violations of the stipulated injunction as interpreted above by the court. Notwithstanding, the trial court awarded Wanke attorneys' fees on the motion to enforce the settlement agreement because it obtained a declaratory judgment regarding the scope and enforceability of the stipulated injunction.

A few months later, Wanke filed second motion to enforce the stipulated injunction with respect to a different customer identified in the customer list, AV Builders. This time, the trial court found the defendants violated the stipulated injunction because the AV Builders work involved jobs undertaken or proposed to be undertaken when defendants were employed by Wanke. The trial court awarded Wanke its attorneys' fees, along with \$50,000 in liquidated damages as provided in the settlement agreement.

#### Court of Appeal

Both parties appealed. Defendants appealed the trial court's findings that they violated the stipulated injunction as to AV Builders and the award of attorneys' fees to Wanke regarding the motion to enforce the settlement as to Con Am Management. Wanke appealed the trial court's order denying its motion to enforce the settlement as to defendants' work for Con Am Management. Additionally, Wanke filed a petition for writ of mandate challenging the trial court's order which refused to hold Keck and WP Solutions in contempt for violating the stipulated injunction. Wanke requested the Court of Appeal to enforce the entirety of the settlement agreement and stipulated injunction. Wanke also asked the appellate court to annul the trial court's order discharging the OSC for contempt and direct the trial court to hold Keck and WP Solutions in contempt.

#### A. Contempt Ruling

With respect to the contempt issue, the Court of Appeal concluded that the double jeopardy clause of the Fifth Amendment to the federal constitution precluded the court from reviewing the trial court's acquittal of Keck and WP Solutions on the contempt charges. Wanke argued that double jeopardy did not apply because the government did not prosecute the action. The Court found that there was no language in the binding U.S. Supreme Court decision of *United States v. Dixon* that limited application of the clause to the contempt proceeding here, which it characterized as a nonsummary criminal contempt proceeding, rather than civil contempt proceeding.

#### B. Validity of Stipulated Injunction Ruling

Notwithstanding its conclusion on the contempt issue, the Court then analyzed whether the trial court erred in determining the stipulated injunction was invalid and unenforceable. The Court reasoned that a party may successfully defend against the enforcement of an injunction that the trial court issued in excess of jurisdiction. The court, however, found that party may not defend against enforcement of a court order by contending merely that the order is legally erroneous. The Court reasoned that under existing authority an injunctive order enforcing an invalid contract, the invalidity of which is not apparent on its face, is not an injunction issued in excess of jurisdiction.

The Court then reasoned that the courts have repeatedly held a former employee may be barred from soliciting existing customers to redirect their business away from the former employer and to the employee's new business if the employee is utilizing trade secret information to solicit those customers. The Court also discussed *Morlife, Inc. v. Perry* (1997) 56 Cal.App.4th 1514, in which the court concluded that there was substantial evidence to support the trial court's finding that the employer's customer list constituted a protectable trade secret. And as a result, the *Morlife* court concluded that the trial court had not erred in enjoining former employees from soliciting any business from any entity that did business with *Morlife* before the former employees stopped working there, provided they obtained knowledge about the customer during the course of their employment at *Morlife*. The Court also reasoned that under the California Supreme Court's decision in *Edwards v. Arthur Andersen LLP* (2008) 44 Cal. 4th 937, section 16600 generally prohibits the enforcement of nonsolicitation agreements in all cases in which the trade secret exception does not apply. The Court also noted that there was a dispute among California appellate courts as to whether such an exception actually exists.

The Court held that Keck and WP failed to make a showing against the enforcement of the injunction on the ground that the injunction was beyond the trial court's jurisdiction to issue. The Court reasoned that at the time the trial court issued the injunction it had personal and subject matter jurisdiction over the parties. It was also undisputed that Wanke had filed a lawsuit alleging trade secret misappropriation and had requested an order enjoining Keck and WP Solutions from soliciting its customers and the trial court entered the stipulated injunction as part of final resolution of the case. According to the Court, each of these fact supported the validity of the stipulated injunction.

The Court also noted that Keck and WP Solutions did not claim that the Stipulated Injunction was obtained in an unauthorized manner or in violation of statutory procedures. Further, there was nothing on the face of the stipulated injunction that indicated that it was unconstitutional or that it violated a statute. On the contrary, the Court noted that Keck and WP Solutions had conceded that employee non-competition agreements could be enforceable to protect the former employer's confidential trade secret information and that the misuse of trade secret information may be properly enjoined by agreement. The Court highlighted the fact that defendants failed to oppose the existence of the so called "trade secret exception" to California's prohibition on the enforcement of non-compete agreements.

The Court held that, because the stipulated injunction was valid to the extent that it protects Wanke's trade secrets, and one cannot conclude from the face of the stipulated injunction that it does not protect Wanke's trade secrets, the stipulated injunction was facially valid. The court remarked that even assuming that Keck and WP Solutions could demonstrate that the trial court erred in issuing the stipulated injunction because the customer list attached to the stipulated injunction was not a protected trade secret, such a showing would be insufficient to avoid enforcement of the injunction. That is because the Court reasoned that demonstrating that the trial court erred in issuing the injunction would not be sufficient to demonstrate that it acted in "excess of its jurisdiction" in doing so.

Finally, the Court recognized that common sense and fundamental fairness support its ruling. The Court explained that parties cannot stipulate to injunctions that identify certain customers whom they will not solicit in order to resolve claims that they misappropriated trade secrets, then proceed to violate the injunction and claim that the customer list is not a trade secret. Even assuming that Keck and WP Solutions were permitted to collaterally attack the validity of the stipulated injunction, and that they could prove that the customer list attached to the stipulated injunction was not a trade secret, the Court found that they made no such factual showing in this case.

In short, since the trial court could not conclude, based on the language of the stipulated injunction, that it does not protect Wanke's trade secrets, the court erred in concluding that the stipulated injunction was an unlawful business restraint.

The defendants' two claims in their appeal both failed in light of the Court's conclusion that the trial court erred in determining that the stipulated injunction could not be enforced as drafted.

### Takeaways

This case reminds us that California's general prohibition on noncompetition agreements applies to all agreements that restrain anyone's engagement in a lawful profession, trade, or business (unless there is an applicable exception); not merely agreements in the employer-employee context. Indeed, even settlement agreements and stipulated injunctions as part of the resolution of a lawsuit are within the ambit of Business and Professions Code section 16600. While this case does not foreclose the ability to obtain injunctive relief when the settlement agreement and stipulated injunction contain restrictive covenants, it illustrates the difficulties in obtaining relief if the other side enters the agreement in bad faith. Thus, it is important to include language in any settlement agreement, which also contains restrictive covenants, and stipulated injunction references and stipulated findings as to the existence of trade secrets and how and why the agreement and/or injunction is necessary to protect trade secrets.

This case demonstrates that one possibility to increase the effectiveness of a settlement agreement, containing restrictive covenants, is to include a liquidated damages clause for any violations. Another possibility would be to require that money be placed in an escrow account for the life of the restricted period. While these remedies will not guarantee a party will not violate the terms of the agreement or ensure further injunctive relief, they may provide some relief for any damages suffered from a breach.

The case also demonstrates that the California appellate courts are presently split on whether there is a trade secret exception to Business and Professions Code section 16600, which may ultimately necessitate the California Supreme Court's guidance.

This case is significant as it provides insight for parties that are assessing the enforceability of restrictive covenants contained within settlement agreements, stipulated injunctions, and other agreements. Specifically, parties may attack such agreements on the grounds of the lack of trade secrets and/or language that the restrictive covenants are necessary to protect trade secrets. At least in the case, however, the Court placed some stock in the parties' agreed resolution to dissuade future collateral attack of the parties' agreed language. What is clear, however, based on this decision is that non-solicitation of customers provisions that are unnecessary to protect trade secrets or not otherwise subject to an applicable exception are void and unenforceable.



# Appendix I

**Protecting and Maintaining Trade  
Secrets and Confidential Information In  
The Age of Social Media and Cloud  
Computing**

**Robert B. Milligan  
D. Joshua Salinas**

Copyright © 2012  
All Rights Reserved

## **Biographical Information**

### Robert Milligan

Mr. Milligan is a Los Angeles, California based partner in the Litigation and Labor & Employment Departments of Seyfarth Shaw LLP. His practice encompasses a wide variety of commercial litigation and employment matters, including general business disputes, unfair competition, trade secret misappropriation and other intellectual property theft. Mr. Milligan has represented clients in state and federal courts in complex commercial litigation and employment litigation. Mr. Milligan also provides advice to clients concerning a variety of business and employment matters, including non-disclosure, non-competition, and invention assignment agreements, corporate espionage, and trade secret and intellectual property audits.

Mr. Milligan is a member of the State Bar of California Intellectual Property Law Section Executive Committee. He is an ITechLaw member as well as the Chair of the Intellectual Property section. He is also the Vice Chair of the ABA Trade Secrets and Interference with Contracts Committee. He also served as a contributing editor of Trade Secret Litigation and Protection in California and is an author of chapters in Continuing Education of the Bar's Trade Secrets Practice in California. He frequently lectures and writes on timely trade secret and other intellectual property issues. He is the editor of his firm's trade secret blog, [www.tradesecretslaw.com](http://www.tradesecretslaw.com).

### D. Joshua Salinas

Mr. Salinas is an attorney in the Los Angeles office of Seyfarth Shaw LLP, practicing in the areas of trade secrets, restrictive covenants, computer fraud, and commercial litigation. His experience includes the prosecution and defense of trade secret misappropriation and unfair competition claims. He is also an author on his firm's trade secret blog, [www.tradesecretslaw.com](http://www.tradesecretslaw.com).

## **Introduction**

The explosion of cloud computing has provided both large and small companies with many technological benefits; but with those well recognized benefits, there are incumbent risks to valuable company data, including prized trade secrets. Companies utilizing cloud computing must employ effective measures to protect and secure their intellectual property. Vendor agreements with cloud providers should be carefully scrutinized to ensure that appropriate contractual provisions are in place to protect company data, including provisions addressing ownership, access, protection, and privacy from both a national and international perspective. Companies should attempt to incentivize their contractual arrangements with vendors to ensure that their business objectives, including secure data protection are met. Social media, which uses cloud computing, has also provided companies with access to a dynamic platform for business growth. To effectively navigate in this new environment, companies must ensure that they adopt effective policies that foster creative expression yet protect company data and secrets, including employment policies with clear direction and guidance for employees. Sensible executives will seek advice from competent counsel to ensure that the cost savings and financial opportunities in cloud computing, including social media, are not outweighed by the potential legal and business risks.

Robert B. Milligan  
D. Joshua Salinas  
Los Angeles, California, October 22 ,2012

Cloud computing is the hot technology movement. Over 43% of Chief Information Officers expect to move their data and utilize cloud services within the next few years.<sup>1</sup> MarketsandMarkets estimates that the cloud computing market will grow from \$37.8 billion in 2010 to \$121.1 billion in 2015.<sup>2</sup> Cisco predicts that worldwide IP traffic in the cloud will increase twelvefold over the next five years and account for more than one-third of total data center traffic by 2015.<sup>3</sup> Verizon recently spent \$1.4 billion to acquire cloud services provider Terremark Worldwide, Inc., which is expected to stimulate other rival carriers to enter the cloud industry.<sup>4</sup> However, the new cloud computing buzz is not new technology to many industry insiders. In fact, as Larry Ellison of Oracle stated, it is “[e]verything that we already do.”<sup>5</sup>

Cloud computing is a metaphor for the internet. It comes from the early days when network engineers used a cloud in their network design illustrations to indicate unknown domains. The engineer knew the domain was there, but the details of that domain were unknown. This network of clouds is how we view the

---

<sup>1</sup> According to a 2010 survey,  
<http://www.gartner.com/it/page.jsp?id=1526414>.

<sup>2</sup> <http://www.marketsandmarkets.com/Market-Reports/cloud-computing-234.html>.

<sup>3</sup> Cisco Global Cloud Index: Forecast and Methodology, 2010–2015;  
[http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud\\_Index\\_White\\_Paper.pdf](http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf)

<sup>4</sup> <http://news.businessweek.com/article.asp?documentKey=1376-LFPBHT6JIJUX01-4B7UIEITJ82MA34J8V0CJMEHFP>.

<sup>5</sup> Quoted in the Wall Street Journal, September 26, 2008.

internet today. Cloud service users know their information is readily accessible, but generally lack any interest where that information is physically located. Cloud service users can generally access their information at any place, at any time, and on any device, as long as they have a network connection. Indeed, cloud computing is part of our every day lives. If you have performed a Google search, checked Yahoo email, or signed in to Facebook, Twitter, or LinkedIn, you have reached into the cloud.

Indeed, the number of social media users and the amount of content created and shared in the cloud continues to increase daily. As of October 2012, Facebook currently has over one billion users, with more than half of them accessing their accounts through mobile devices. Twitter has over 517 million users publishing over 340 million tweets daily. LinkedIn has over 161 million users with two new member accounts created every second. YouTube has hundreds of millions of users and over 800 million unique visits per month.

Cloud computing lacks a universal definition. Ask different individuals working in the IT industry what cloud computing is and you will get different answers. The National Institute of Standards and Technology (NIST) has provided the most widely accepted definition of cloud computing: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or

service provider interaction.”<sup>6</sup> The NIST also notes five essential characteristics of cloud computing services: On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.<sup>7</sup>

Cloud computing has numerous technical benefits. Users typically pay the cloud provider for the services and resources they use. This pay-as-you-go infrastructure allows companies to reduce costs. Companies can avoid paying for costly equipment, personnel, and maintenance. For example, if a company needs additional storage space for its data, it can purchase more from the cloud provider. Without cloud computing, the company may have to pay for additional servers, allocate space for bulky servers, and higher additional IT staff, among other costs. Cloud computing also provides scalability. The ability to adapt and quickly respond to increased market demands is invaluable to small companies who lack the finances to significantly invest in expensive IT infrastructure. The on-demand access provides access wherever a cloud user has a network connection. This mobility and convenience is one of the reasons low cost netbooks and tablet devices, such as iPads, have rapidly radically increased in popularity. Companies are embracing the cloud as a cost effective way to do business. Specifically, it provides smaller companies with a better chance to compete.

Cloud computing involves three general service models. The simplest model is Infrastructure as a Service (IaaS). This involves

---

<sup>6</sup> NIST Definition of Cloud Computing, v. 15, <http://csrc.nist.gov/groupsSN/Sloud-computing/>.

<sup>7</sup> Identified by NIST as part of its definition of Cloud Computing.

basic storage and data hosting. The second model is Software as a Service (SaaS). In this model, the cloud provider provides the software to access, manage, and utilize the data. For example, this is commonly seen with email (e.g. Gmail, Yahoo mail, Hotmail) and social media sites (e.g. Facebook, LinkedIn, Twitter). The third model is Platform as a Service. This model provides an operating system in which the company can develop and build its own applications. For example, Facebook allows third parties to build and distribute applications within its service. The main factor distinguishing the three models is the level of control the subscriber retains over its data.

While cloud computing is not new, expansive and accelerated network connectivity has fueled the ascent of this technology movement. Companies embracing cloud computing will move data previously stored in house, onto servers provided by third parties. However, moving confidential and proprietary information, such as trade secrets, raises numerous legal, security, and business concerns.

### **Trade Secrets**

A trade secret is any information not generally known, that is economically valuable, and subject to reasonable efforts to maintain its secrecy.<sup>8</sup> Many people think of secret formulas, such as the ingredients for Coca-Cola, KFC chicken, or WD-40. Yet trade secrets can also include a wide variety of technical and nontechnical information. Common trade secrets include

---

<sup>8</sup> See e.g. 18 U.S.C. § 1839 (3) (A), (B) (1996); Cal. Civ. Code § 3426.1(d).

manufacturing methods, formulas, techniques, business and marketing plans, customer lists, and computer programs. There is no requirement to register or publish a trade secret to receive protection. Additionally, a trade secret does not have to involve novel information. The heart of the trade secret's value is its secrecy.

A trade secret owner must take reasonable efforts to ensure the information's secrecy.<sup>9</sup> He or she must take actual efforts to protect the trade secret so that the trade secret is through improper, illegal, or unethical means. The burden is on the trade secret owner to keep the information secret. Furthermore, he or she cannot expect others to hold a higher obligation to keep the information secret.

Trade secret law protects against misappropriation, i.e., the illegal or unauthorized acquisition, disclosure, or use of information. Trade secrets are creatures of statute and protected under several laws such as the Uniform Trade Secrets Act (UTSA), Economic Espionage Act of 1996 (EEA)<sup>10</sup>, and the Computer Fraud and Abuse Act (CFAA).<sup>11</sup> Varying versions of the UTSA are enacted in forty six states in the United States.

Trade secret law holds third parties liable if they knew or had reason to know of misappropriation.<sup>12</sup> However, it does not generally protect against the accidental disclosure or the reverse

---

<sup>9</sup> *J. T. Healy & Son, Inc. v. James A. Murphy & Son, Inc.*, 357 Mass. 728, 730-31 (1970).

<sup>10</sup> 18 USC § 1831.

<sup>11</sup> 18 USC § 1030.

<sup>12</sup> See *Kozuch v. CRA-MAR Video Ctr., Inc.*, 478 N.E.2d 110 (Ind. Ct. App. 1985).

engineering of a trade secret.<sup>13</sup> For example, if a trade secret is accidentally disclosed by a cloud provider or third party, it could potentially lose its trade secret status if the data leak is not promptly and effectively addressed.

Unlike patent, trademark, or copyright protection, there is no set time period for trade secret protection. A trade secret is protected as long as it is kept secret. However, once a trade secret is lost, it is lost forever. As we have seen in a post-Wikileaks world, once confidential information is disclosed, it can be instantly distributed online for hundreds of millions to see, access and download.<sup>14</sup>

## **Problems**

An issue with new technology is that the law is constantly behind. “[Courts] try to keep up with technology and understand it, but things move so quickly.”<sup>15</sup> The use of cloud computing raises several problems for trade secrets. The heart of a trade secret’s status is its secrecy. Thus, placing confidential information in the hands of a third party cloud provider seems contrary to maintaining secrecy. Moreover, information placed into the cloud increases the risk that the information will be accidentally or intentionally disclosed to third parties.

---

<sup>13</sup> *Kewanee Oil Co. v. Bicron Corp.*, 94 S. Ct. 1879, 1883 (1974).

<sup>14</sup> WikiLeaks website publishes classified military documents from Iraq, [http://articles.cnn.com/2010-10-22/us/wikileaks.iraq\\_1\\_wikileaks-website-classified-documents-iraq-wiki-leaks-iraqis?\\_s=PM:US](http://articles.cnn.com/2010-10-22/us/wikileaks.iraq_1_wikileaks-website-classified-documents-iraq-wiki-leaks-iraqis?_s=PM:US).

<sup>15</sup> Judge Alex Kozinski, Ninth Circuit U.S. Court of Appeals, speaking at Golden Gate University’s Intellectual Property Distinguished Speaker Program, April 13, 2011.

One threshold issue is whether confidential information placed into the cloud diminishes its status as protectable information. In other words, can trade secrets lose their protection in the cloud? The answer may vary depending on the nature of the information and who places the information in the cloud. Courts have used six factors to determine whether a piece of information is secret. These comprise: (1) the extent to which the information is known outside the company, (2) the extent to which the information is known by employees and others inside the company, (3) the extent of measures taken by the company to protect the secrecy of its information, (4) the value of the information to the company and competitors, (5) the amount of time, effort, and money expended by the company in developing the information, and (6) the ease of difficulty with which the information can be properly acquired or duplicated by others.<sup>16</sup>

A New York district court found a company's customer list was not a trade secret because the information at issue had already been disclosed in the cloud and was publicly accessible. In *Sasqua Group v. Courtney*, 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010), an executive search consulting firm alleged that a former employee stole confidential customer information from a client database and later solicited those clients. The confidential database contained client contact information, individual profiles, resumes, descriptions of interactions with clients, and hiring preferences. The court focused on the sixth factor in the six-factor

---

<sup>16</sup> These factors are the "most-cited listing of the objective criteria for determining the existence of a trade secret." *M. Jager*, Trade Secrets Law § 5.05 (1995).

analysis; i.e. the ease of difficulty the information could be properly acquired by others. The defendant former employee demonstrated how easily she could find the same client database information by searching Google, LinkedIn, Bloomberg.com, and FX Week. The court found the client database did not constitute a trade secret because the information was easily accessible online to the public. In doing so, the court noted that the protection of certain information may no longer be viable in the 21st century in light of new technologies.<sup>17</sup>

A 2011 New Jersey district court case, however, found that trade secret information may not necessarily lose its trade secret status despite that information being posted on the internet. In *Syncsort Incorporated v. Innovative Routines, International, Inc.*, 2011 U.S. Dist. LEXIS 92321, (D.N.J. August 18, 2011), the plaintiff data transformation software company alleged that the defendant competitor had improperly developed software when the defendant allegedly improperly acquired and used the plaintiff's trade secrets, i.e. confidential command language. The defendant argued that parts of the plaintiff's command language were posted on the internet, and, thus no longer secret. Moreover, the defendant alleged that entire copies of the plaintiff's Reference Guides regarding the command language were temporarily posted on the Internet, once in Korea and once in Japan.

The court in *Syncsort* found that the internet postings did not defeat the command language's trade secret status because (1) the parts of command language posted were insufficient to fully

---

<sup>17</sup> *Sasqua Group v. Courtney*, 2010 WL 3613855, \*22 (E.D.N.Y. Aug. 2,

disclose the complete command language, and (2) the Reference Guide posts in Korea and Japan were obscure and transient such that it was not made generally known to other competitors in the industry. The takeaway from this case is that the “secrecy” of information may be determined based on the surrounding circumstances and nature of the online disclosure, instead of the mere fact that information was posted online.

Similarly, a current Northern District of California case *PhoneDog v. Kravitz*, No. C11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011), involves a dispute whether a Twitter account’s followers constitute trade secrets even when they are publically visible. The court denied the defendant’s motion to dismiss and ruled that PhoneDog, an “interactive mobile news and reviews web resource,” could proceed with its lawsuit against Noah Kravitz, a former employee, who it claims unlawfully continued using PhoneDog’s Twitter account after he quit. The court held that PhoneDog had described the subject matter of the trade secret with “sufficient particularity” and satisfied its pleading burden as to Kravitz’s alleged misappropriation by alleging that it had demanded that Kravitz relinquish use of the password and Twitter Account, but that he has refused to do so. And, with respect to Kravitz’s challenge to PhoneDog’s assertion that the password and the Account followers do, in fact, constitute trade secrets -- and whether Kravitz’s conduct constitutes misappropriation, the court ruled that the such determinations require the consideration of evidence outside the

---

2010).

scope of the pleading and should, therefore, be raised at summary judgment, rather than on a motion to dismiss. This case deserves watching.

Earlier this year, a Colorado district court ruled that a dance club owner could maintain his trade secrets misappropriation claim against a competing club owner for the alleged theft of his MySpace friends' profiles and contact information. *Christou v. Beatport, LLC*, No. 10-cv-02912-RBJ-KMT, 2012 WL 872574 (D. Colo. Mar. 14, 2012). The court rejected the defendant's argument that the MySpace friends were fair game because they were publically available on the internet.

Another issue arises when cloud providers use the hosted information for secondary purposes. For example, information containing customer lists or contact information are highly valuable for market studies and behavioral targeting. Providers can earn substantial revenues reselling this raw data to advertisers and other third parties.

Additionally, and perhaps more threatening to trade secrets, are cyber attacks. In October 2012, six major American banks were hit with a wave of computer attacks that caused Internet blackouts and online banking delays.<sup>18</sup> While customer account information was allegedly not taken, these acts show how easy it is to have successful cyberattacks. Moreover, a 2010 study from the Internet security company BitDefender revealed that 94% of a control group accepted "friend" requests from a complete

---

<sup>18</sup> [http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?hpw&\\_r=1&](http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?hpw&_r=1&)

stranger.<sup>19</sup> Twenty individuals in that study then conducted an online conversation with this friend, and fifteen of those individuals shared confidential information, including internal business strategies or information on unreleased products.

Hackers have recently targeted their attacks towards corporate trade secrets and proprietary information. McAfee reported on the Night Dragon cyber attacks that have targeted oil and gas industry trade secrets.<sup>20</sup> IBM's X-Force cyber security team also reported that cybercriminals now pinpoint valuable corporate data.<sup>21</sup> There is a thriving criminal market for converting stolen trade secrets into cash.<sup>22</sup> In fact, criminal gangs in China, Russia, and the Ukraine will steal information for companies looking to undercut their rivals.<sup>23</sup> Hackers are eagerly awaiting more corporations to embrace cloud computing and release prized data into the cloud.

The inherent risks in utilizing cloud computing were demonstrated last year with one of the largest security breaches in United States history – the March 2011 Epsilon security breach.<sup>24</sup> Epsilon is one of the largest permission based email marketing

---

<sup>19</sup> <http://www.hotforsecurity.com/blog/experiment-2-one-two-three-this-blonde-girl-looks-just-like-me-891.html>

<sup>20</sup> Global Energy Cyberattacks: "Night Dragon," <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>.

<sup>21</sup> Available at <http://www-03.ibm.com/security/landscape.html>.

<sup>22</sup> <http://www.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm>.

<sup>23</sup> <http://www.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm>.

<sup>24</sup> Epsilon data security breach expands, could be history's largest, <http://www.digitaltrends.com/computing/epsilon-data-security-breach-expands-could-be-historys-largest/>.

companies. It sends over 40 billion emails each year on behalf of over 2,500 clients. Its clients include US Bank, Capital One, Chase, Citi, JPMorgan, Best Buy, Hilton, Target, and Disney. On March 30, 2011, Epsilon detected an unauthorized entry into its customer databases. It discovered that hackers had obtained access to thousands of names and email addresses. As a result, these hackers now have the ability to send highly effective spear-phishing emails to their recently acquired targets.<sup>25</sup>

For instance, the following scenario could arise from the Epsilon or other cloud computing breaches: (1) hacker reviews improperly obtained customer information and discovers that the customer works at a large corporation or firm, (2) hacker crafts a well designed email posing as the company the client gave their email address (e.g. Best Buy, Target, Citi), (3) customer opens the email at work, clicks a provided link, and undetectable software is downloaded onto the customer's computer, and (4) undetectable software quietly sits inside the corporate network, searches for trade secrets or confidential information, and sends it back to the hacker. Security software company Symantec reports that in 2011 at least fifty companies in the defense and chemical industries were targeted by these spear fishing attacks, which were specifically aimed at prized research and development information.<sup>26</sup>

---

<sup>25</sup> Epsilon hacking shows new "spear-phishing" risks, <http://www.reuters.com/article/2011/04/04/us-hackers-epsilon-idUSTRE7336DZ20110404>.

<sup>26</sup> The Nitro Attacks: Stealing Secrets from the Chemical Industry, Eric Chien and Gavin O'Gorman,

Aside from the intentional theft by outside parties, trade secrets have always been susceptible to misappropriation by current or former employees. The typical case involves the disgruntled employee who discloses or uses trade secrets after termination. Yet, the use of cloud services such as social media increase the risks of both intentional and accidental disclosure by such employees.

A related issue involves the ownership of data. If a provider or employee modifies the data, do they have any ownership rights? Taking the case of a customer list, if an employee friends clients and adds them to a LinkedIn profile, does the contact belong to the employee or the employer. Consequently, if the employee leaves his or her employer, can the employee later contact previous clients? This issue was the underlying dispute in *TEK Systems v. Hammernik*, No 0:10-cv-0081, (D. MN. 2010).

In *TEK Systems*, the plaintiff, an IT staffing firm, alleged that a former employee violated a non-solicitation agreement when the employee contacted previous clients on LinkedIn. The non-solicitation agreement lacked any social media restrictions. The issue is whether the employee violated the agreement when she allegedly contacted the clients through her personal social media account during her employment, and then allegedly later contacted the clients after she left for a competitor. The parties eventually stipulated to the enforcement of the non-solicitation agreement and

---

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the\\_nitro\\_attacks.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf)

the return of TEK Systems' documents. Unfortunately, no ruling or precedential decision arose from this case.

The ownership of a social media account is also at issue in the previously discussed *PhoneDog v. Kravitz* case – whether the employer or employee owns the subject Twitter account. The court followed a similar approach in denying Kravitz's motion to dismiss PhoneDog's conversion claim. Kravitz challenged such claim on the ground that PhoneDog had not sufficiently alleged that it owns or has the right to immediately possess the Twitter Account. He also argued that PhoneDog failed to adequately allege that he had engaged in his alleged act of conversion "knowingly" or "intentionally." The court, however, found that these issues lie "at the core of [the] lawsuit" and that, accordingly, an evidentiary record outside the pleading had to be developed before the court could resolve such fact-specific issues.

One federal court in Philadelphia recently ruled that an employer can claim ownership of its executive's LinkedIn profile. In *Eagle v. Morgan*, No. 11-4303, 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011), the court held that an employer may claim ownership of its former executive's LinkedIn connections where the employer required the executive to open and maintain the account, the executive advertised her and her employer's credentials and services on the account, and the employer had significant involvement in the creation, maintenance, operation, and monitoring of the account. Similar to *Sasqua Group*, the court found that the contact lists in the LinkedIn account could not constitute trade secrets because they were publicly accessible

online. The takeaway in *Eagle*, however, is that employers should consider getting more involved in their employees' social-networking activities and utilize contracts to assign ownership in such accounts.<sup>27</sup>

The nature of trade secrets as digital information within the cloud raises potential litigation concerns. For example, data is often transitory, moving between various servers and facilities. Trade secrets may move from state to state, and even across international borders. Thus, difficulties may arise in establishing jurisdiction in instances of trade secret theft. Moreover, a cloud provider's obligation to comply with e-Discovery demands may compromise the integrity of trade secrets or confidential information if secrecy protections such as protective orders and confidentiality agreements are not employed.

Finally, problems may arise with data access continuity. What happens when the contract or subscription for cloud services terminates? The cloud provider may withhold data when a company fails to pay for services. Additionally, what happens when a small startup provider goes bankrupt or is purchased by another company? These and many of the problems discussed above may be addressed with effective and well drafted contracts as part of a well developed cloud computing strategy before placing your company's data in the cloud.

---

<sup>27</sup> The Court also recently dismissed Plaintiff Eagle's Computer Fraud and Abuse Act claim for failure to prove damages regarding the loss of her LinkedIn account. *Eagle v. Morgan*, 2012 WL 4739436 (W.D. Pa. Oct. 4, 2012).

## **Solutions**

The problems of storing data in the cloud are not insoluble. The first step is to conduct a trade secret audit or inventory before placing information in the cloud. Determine what information is sensitive and confidential. Highly valuable trade secrets can remain off the cloud and stored in house on secured networks or physical areas. Keeping information out of the cloud inherently reduces the risk it will not be disclosed on the cloud. When in doubt, don't make the information able on the cloud. To the extent that you determine that certain trade secret information can be placed in a secure cloud, keep track of such data, as well as the security measures in place to protect such data (encryption, confidentiality designations, written agreements, etc.) and who has access to such data. The single greatest security control you can deploy is to encrypt your data – if you do nothing else, at least encrypt your data.

Once you decide to utilize cloud computing, take all prudent and necessary measures to select the correct provider.<sup>28</sup> Perform diligent checks on all potential providers. Obtain references. Determine whether they have the capabilities to provide the type of services you desire, including the ability to meet any rapidly increasing demands. Conduct interviews with the providers. Find out their financial viability. Ask about the types of physical servers they use and why they chose that equipment. View their security and privacy policies and discover how many security breaches they have experienced. Determine whether your

data will be encrypted. Determine their backup and redundancy setups. Find out whether they offer 24/7 support and if they have any software that helps manage the provided services. Determine whether your cloud provider contracts its services with third parties. Evaluate choice of law, choice of forum, and indemnification provisions carefully. Security rather than price should be your top priority. Do not be afraid to demand better transparency from the cloud provider. Try to incentivize the cloud provider's conduct to keep your information absolutely secure. You may want to consider diversifying your portfolio of data stored on the cloud with multiple providers or backup all information stored in the cloud locally.

State law may require you to contract with the cloud provider to ensure reasonable security procedures and practices are in place. California requires businesses that possess personal information about California residents to implement and maintain reasonable security procedures and practices.<sup>29</sup> Businesses that disclose this personal information to third parties (e.g. cloud providers) must contract with the third party to implement and maintain reasonable security procedures and practices. Massachusetts also requires contracts to implement and maintain appropriate security measures when providing personal information to cloud providers.<sup>30</sup> Nevada requires businesses to

---

<sup>28</sup> Consider Cloud Security Alliance's Cloud Computing Security Guidelines, <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>

<sup>29</sup> Cal. Civ. Code § 1798.81.5.

<sup>30</sup> 201 C.M.R. 17.00 et seq.

use encryption on data storage devices that contain personally identifiable information.<sup>31</sup>

After the provider is chosen and a trade secret audit or inventory has been conducted, the best way to protect trade secrets and other information is through well drafted contracts and policies and periodic audits of the cloud provider. This includes contracts with both cloud providers and the company's internal employees who may access the information. First, define the ownership rights in the data. For example, you may want to explicitly state that the cloud provider and employees have no ownership rights in the data. The agreement can state that the provider and employees have limited access to the data only for certain reasons. Defining the limits of authorization can also help establish rights under the CFAA if the provider or employee violates the scope of their authorizations. Next, define the scope of the protected information. Specifically indicate which information is considered trade secret or confidential. The Economic Espionage Act's language may be preferred because it provides a broad trade secret definition. Also include language protecting confidential and proprietary data. Prohibit the unauthorized use or disclosure of company data, including trade secrets and confidential and proprietary information. Contracts can also provide for injunctive relief, liquidated damages, arbitration, and attorneys' fees.

Companies should also control access to their data. Agreements with cloud providers should restrict the use of data to

---

<sup>31</sup> Nev. Rev. Stat. 603A.010 et seq.

outside vendors or third parties. Provisions should also hold the provider and any subcontractors liable for security breaches. This is especially important in light of the 2011 Epsilon security breach. Companies should require heightened security standards by providers such as ISO standards. These standards represent an international consensus on good quality management practices. For example, they require quality audits, effective training, and corrective actions for problems. Companies should remain cautious, however, and not assume that compliance equals security. Compliance guidelines generally establish minimum standards, but are not a substitute for a complete security strategy.

Additionally, the Federal Trade Commission has provided 5 key principles for sound data security plans: (1) know the personal information you have, (2) scale down and keep only what you need, (3) protect the information you want to keep, (4) properly dispose of what you no longer need, and (5) create a plan to respond to security incidents.<sup>32</sup>

Contracts should include ongoing confidentiality obligations to protect trade secret information in case of termination. Additionally, contracts should require the return or deletion of any copies of the data (as appropriate) by the provider or employee after the termination of the agreement. Finally, there should be a provision prohibiting the withholding of data by the provider or employee in the case of a dispute.

As part of a comprehensive policy to address data protection in the cloud, companies should establish effective security and social

---

<sup>32</sup> <http://www.ftc.gov/bcp/edu/microsites/infosecurity/>.

media policies to prevent employees' disclose of information. Information security measures include password protection, email and electronic data policies, departmental trainings, and exit interviews to remind employees of confidentiality obligations.

Social media policies are even more critical today with explosion of social media in the workplace. Well drafted and communicated policies can effectively reduce the amount of sensitive information disclosed both accidentally and intentionally on the internet. Social media policies can restrict employees from posting confidential information on sites such as Facebook, Twitter, or LinkedIn. Employees should be educated about the implications of posting information to these sites through recurring training. For example, Facebook grants itself a license to any information posted on its site.<sup>33</sup> Twitter grants itself a license to make any posted content available to other companies.<sup>34</sup> Employers should provide constant reminders to employees not to disclose confidential data on such sites.

Social media ownership agreements and policies appear to have dramatically increased in importance for California employers after California's recent social media legislation. On September 27, 2012, California Governor Jerry Brown signed Assembly Bill 1844 into law, making California the third state in the country – Maryland and Illinois are the others – to regulate employers' ability to demand access to employees' or prospective hires' personal social media accounts.<sup>35</sup> Specifically, AB 1844

---

<sup>33</sup> <http://www.facebook.com/terms.php>.

<sup>34</sup> <http://twitter.com/tos>.

<sup>35</sup> AB 1844 goes into effect on January 1, 2013.

“prohibit[s] an employer from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media.” In other words, an employer may neither request nor require an employee or an applicant to divulge his or her personal social media account information.

While AB 1844 only applies to “personal” social media accounts, the lack of definition of the phrase “personal” and the overly expansive definition of “social media” is problematic, particularly since it is not always clear who owns company social media accounts. (See *PhoneDog*’s Twitter followers and *Eagle*’s LinkedIn contacts).

Employers should, however, be very cautious in the drafting of their social media policy. In fact, an overly broad policy may violate employee rights. Employers must align their policies with the National Labor Relations Act (NLRA) to avoid the ire of the National Labor Relations Board (NLRB). Section 7 of the NLRA protects both unionized and non-unionized employees’ right to engage in concerted activities in the United States. This NLRB has criticized several employers’ social media policies for being overly broad and violative of employee rights.

In fact, the NLRB recently held that Costco’s social media policy prohibiting employees from posting statements online that “damage Costco ... defame any individual or damage any person’s

reputation” violated the NLRA because it could reasonably tend to chill employees from exercising their Section 7 rights.<sup>36</sup>

In another recent case, the NLRB found that a BMW dealership’s discharge of a salesman for his Facebook postings did not violate the NLRA because the activity was not concerted or protected.<sup>37</sup> The salesman allegedly posted photos on Facebook of an embarrassing and potentially dangerous accident at an adjacent Land Rover dealership, along with sarcastic commentary such as “OOPS.” The board held that this was clearly not concerted or protected activity, and, thus his discharge did not violate the NLRA.

Several other social media-employment dispute cases caused the NLRB’s Acting General Counsel to release a report on January 24, 2012.<sup>38</sup> In its report, Acting General Counsel Lafe E. Solomon analyzed fourteen recent social media-employment dispute cases and reaffirmed explaining the NLRB’s position that social media policies that restrict employee’s abilities to discuss working conditions and wages are unlawful. In particular, Mr. Solomon found social media policies unlawful that (1) provide no clear guidance to employees as to what online communications and postings are appropriate, (2) do not provide specific examples of the types of confidential or sensitive information that are

---

<sup>36</sup> *Costco Wholesale Corp. and United Food Commercial Workers Union*, 358 NLRB No. 106 (Sept. 7, 2012).

<sup>37</sup> *Karl Knauz Motors Inc. d/b/a Knauz BMW and Robert Becker*, 358 NLRB No. 164 (Sept. 28, 2012).

<sup>38</sup> Report of the Acting General Counsel Concerning Social Media Cases, Lafe E. Solomon, January 24, 2012, [http://www.faegeb.com/webfiles/OM\\_12\\_31\\_Report\\_of\\_the\\_Acting\\_General\\_Counsel\\_Concerning\\_Social\\_Media\\_Cases.doc.pdf](http://www.faegeb.com/webfiles/OM_12_31_Report_of_the_Acting_General_Counsel_Concerning_Social_Media_Cases.doc.pdf)

prohibited from online disclosure, and (3) “would reasonably tend to chill employees in the exercise of their Section 7 rights.” The underlying concern is that overbroad social media policies may cause employees to believe that their rights under Section 7 – discuss their workplace environment and self-organize – are otherwise prohibited.

Employers should employ specifically tailored social media policies that protect trade secrets and confidential information. Indeed, the NLRB found an employer’s social media policy that restricted employees from using or disclosing confidential and or proprietary information as lawful and compliant with the NLRA. The NLRB however requires that these restrictions sufficiently describe and provide examples of what the employer considers proprietary, confidential, and/or trade secret information. Employers should distance the company from personal social media use by employees that attempts to associate the employee with the company. For example, employers should prohibit the use of company trademarks, graphics, or logos for personal use without company approval. Companies should also prohibit, or at least limit, the use of company provided email addresses for personal social media activity. Companies must be vigilant to ensure that their cloud computing policies and agreements, including social networking policies, remain current with changing technology to protect their most valuable assets.

### **Conclusion**

Cloud computing provides significant benefits for the development and growth of businesses. Companies that embrace

this technology and venture into the cloud must be careful and thoughtful. Companies should scrutinize what they put into the cloud and select reliable and security conscience cloud providers. Well drafted agreements and policies with both providers and employees can help reduce the risk of the disclosure of trade secrets in the cloud. A comprehensive cloud computing strategy can help companies realize the cost savings and financial opportunities in cloud computing, including social media, while ensuring that these benefits are not outweighed by the potential legal and business risks.



# Appendix J

**EXIT INTERVIEW CERTIFICATION**

This is to certify that I do not have in my possession, nor have I failed to return, any devices, designs, records, data, notes, reports, proposals, lists, emails, electronic data, correspondence, specifications, drawings, blueprints, sketches, laboratory notebooks, materials, equipment, other documents or property, or copies or reproductions of any aforementioned items belonging to \_\_\_\_\_, its subsidiaries, affiliates, successors or assigns (together the "Company").

I expressly represent that I have returned all Company property, including all confidential, proprietary, and/or trade secret information.

I have not made, forwarded or retained originals or copies of any documents, writings, emails, text messages, instant messages, any other electronic or voicemessages or information of any kind received at or sent from the Company by any means, including, but not limited to, any computer, wireless device, facsimile, or telephone.

I further certify that I have complied with all the terms of my employment agreement with Company dated as of \_\_\_\_\_, including, without limitation, the Company's Proprietary Information and Invention Assignment Agreement (the "PIIAA") signed by me, including, without limitation, the reporting of any inventions and original works of authorship (as defined therein), conceived or made by me (solely or jointly with others) covered by the PIIAA. I acknowledge and reaffirm my obligations to the Company as set forth in the PIIAA, an executed copy of which I acknowledge receiving herewith.

I further agree that, in compliance with the PIIAA, I will preserve as confidential all trade secrets, confidential knowledge, data or other proprietary information relating to products, processes, know-how, designs, formulas, developmental or experimental work, computer programs, data bases, other original works of authorship, customer lists, business plans, financial information or other subject matter pertaining to any confidential business of Company or any of its employees, clients, consultants or licensees.

I further certify that I have not engaged in any activity which is competitive with the Company or otherwise inconsistent with the written policies or agreements of the Company.

I further acknowledge that the Company is authorized to send a letter to my future employer explaining my continuing obligations to the Company.

On termination of my employment with Company, I will be employed by \_\_\_\_\_ in its \_\_\_\_\_ Division and will be working in connection with the following projects (generally describe based upon publically available information)\_\_\_\_\_.

Date: \_\_\_\_\_

\_\_\_\_\_  
(Employee's Signature)

# Appendix K

---

## D. Joshua Salinas

Los Angeles Office  
(310) 201-1514  
jsalinas@seyfarth.com



### *Areas of Practice*

Trade Secrets, Computer Fraud & Non-Competes

Intellectual Property

Patent, Internet & Privacy, Trademark, Copyright

Commercial Litigation

Alternative Dispute Resolution, Business Torts, Contract Disputes

### *Experience*

Mr. Salinas is an attorney in the Los Angeles office of Seyfarth Shaw LLP. As a member of the Commercial Litigation Department, Mr. Salinas represents clients in complex commercial disputes involving trade secrets and restrictive covenants, unfair competition, contract, and intellectual property claims in both state and federal court. His experience includes the prosecution and defense of trade secret misappropriation, unfair competition, and patent infringement claims.

Mr. Salinas has extensive experience in trial preparation, discovery, and law and motion. He also advises clients on non-competition, non-solicitation, and non-disclosure agreements, protecting and enforcing intellectual property rights, and litigation avoidance strategies.

Mr. Salinas is also an author of the Firm's trade secret blog, [www.tradesecretslaw.com](http://www.tradesecretslaw.com).

### *Education*

J.D., California Western School of Law (2011)

Honors Concentration in Intellectual Property, Telecommunications, and Technology Regulation

Academic Achievement Award (Highest Grade): Trial Advocacy, Trial Motions, and Negotiation

Pro Bono Honor Society

Philip C. Jessup International Moot Court Competition: Super Regional Champions, Final Round

Top Oralist

B.A., University of San Diego (2005)  
Minors in Biology and Chemistry

### ***Admissions***

California

### ***Courts***

U.S. District Court for the Central District of California

### ***Affiliations***

State Bar of California (Intellectual Property Section; Business Law Section; Trade Secret Subsection; Employment Law Section)

American Bar Association

Association of Business Trial Lawyers

ITechLaw Association

### ***Publications***

Co-Author, "New Law Protecting Personal Social Media Of California Employees and Students Adopted In California," *Seyfarth Shaw LLP - Management Alert* (October 1, 2012)

Co-Author, "California Court Rules That Non-Competition Agreement Contained In Employment Agreement Is Unenforceable Against Former Seller Even Though It Was Executed In Connection With The Sales Of A Business," *Seyfarth Shaw LLP - Management Alert* (August 29, 2012)

"Minnesota District Court Dismisses Computer Fraud and Abuse Act Claim Brought Against Former Employee Based Upon Narrow Interpretation Of Act," *Trade Secrets Law Blog* (March 21, 2010)

"Keep Your Pot of Gold Hidden, Ohio Court Rules Information Posted Online Not Trade Secret," *Trade Secrets Law Blog* (March 16, 2012)

"Oregon Federal Court Permits Declaratory Relief Suit To Proceed In Race To Judgment Non-Compete Dispute," *Trade Secrets Law Blog* (February 13, 2012)

"Top 10 2011 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law," *Trade Secrets Law Blog* (January 17, 2012)

"Does A Trade Secret Plaintiff Have To Disclose Its Trade Secrets Prior To The Commencement Of Discovery In California Federal Court?" *Trade Secrets Law Blog* (January 13, 2012)

"Department of Justice Takes Pro-Employer Stance On Amendments To Computer Fraud And Abuse Act: Employers Should Continue To Be Able To Hold Employees Liable For Violations Of Computer Usage Policies Under The Act," *Trade Secrets Law Blog* (November 22, 2011)

"Liability Under Computer Fraud and Abuse Act For Violating Computer Use Policies Gains Momentum In Ninth Circuit," *Trade Secrets Law Blog* (October 6, 2011)

"Employers' Obligation to Defend and Indemnify Rogue Employees In California?" *Trade Secrets Law Blog* (October 14, 2011)

"Case Study: Bose v. Interclick," *Law360* (September 29, 2011)

"New York Federal Court Dismisses Computer Fraud and Abuse Act Claims For Defendant's Alleged Use Of 'Supercookies' And 'History Sniffing'," *Trade Secrets Law Blog* (September 4, 2011)

"Private Information Stored On Electronic Devices Subject To Search By Law Enforcement If Arrested In California," *Trade Secrets Law Blog* (March 16, 2011)

"Computer Fraud and Abuse Act Remains Viable Claim For Employers To Assert Against Employees Who Steal Company Data," *Trade Secrets Law Blog* (March 2, 2011)

"District Court Holds That Computer Forensic Investigation Costs Satisfy "Loss" Requirement of Computer Fraud and Abuse Act," *Trade Secrets Law Blog* (February 9, 2011)

"Fitness Companies Spar Over Unauthorized Access Of Departing Employee's Personal E-mail Accounts," *Trade Secrets Law Blog* (January 25, 2011)

Terrence P. McGlynn, Daniel J. Salinas, Robert R. Dunn, Tana E. Wood, Deborah Lawrence, Deborah A. Clark (2007) *Phosphorus Limits Tropical Rain Forest Litter Fauna*, *Biotropica* 39:1, 50.

---

# Robert B. Milligan

Los Angeles Office  
(310) 201-1579  
rmilligan@seyfarth.com



## *Areas of Practice*

Trade Secrets, Computer Fraud & Non-Competes

Intellectual Property

Copyright; Internet & Privacy; Patent; Trademark

Commercial Class Action Defense

Commercial Litigation

Alternative Dispute Resolution; Business Torts; Contract Disputes; Franchise, Dealer & Distributor Disputes; Fraud Prevention & White Collar Criminal Defense; Insurance; Real Estate Litigation

Labor and Employment

California Labor Code Litigation; Single-Plaintiff Litigation; Wage & Hour Litigation; Work Place Counseling and Solutions; SOX Whistleblower Litigation

## *Experience*

Mr. Milligan is a partner in the Litigation and Labor & Employment Departments of Seyfarth Shaw LLP. His practice encompasses a wide variety of commercial litigation and employment matters, including general business and contract disputes, unfair competition, trade secret misappropriation and other intellectual property theft, franchise litigation, real estate litigation, insurance bad faith, invasion of privacy, consumer and employee class actions, wrongful termination, discrimination and harassment claims, wage and hour disputes, ADA and OSHA compliance, whistleblower and SOX cases, bankruptcy, and other business torts. He specializes in trade secret, non-compete, and data protection litigation and transactional work on a state, national, and international platform.

Mr. Milligan represents clients in state and federal courts in complex commercial litigation and employment litigation. His experience includes trials, binding arbitrations and administrative hearings, mediations, as well as appellate proceedings. Mr. Milligan also provides advice to clients concerning a variety of business and employment matters, including non-disclosure, non-compete, and invention assignment agreements, corporate investigations, trade secret and intellectual property audits,

commercial landlord/tenant disputes, ADA and OSHA compliance, and an assortment of franchise and bankruptcy issues.

He served as a judicial extern for the Superior Court of Yolo County, Civil Law Division and the Honorable Christopher M. Klein of the United States Bankruptcy Court, Eastern District of California.

Mr. Milligan was selected as a Southern California Super Lawyer Rising Star in Intellectual Property. He also served as a contributing editor of *Trade Secret Litigation and Protection in California* and is an author of chapters in *Continuing Education of the Bar's Trade Secrets Practice in California*. He is also the editor of Seyfarth's trade secret blog, [www.tradesecretslaw.com](http://www.tradesecretslaw.com), and was recognized by Legal 500 for the firm's trade secret practice.

Mr. Milligan serves as a member of the State Bar of California Intellectual Property Law Section Executive Committee and as Chair of the Intellectual Property Committee for the ITechLaw Association. He also serves as the Vice Chair of the ABA Intellectual Property Section's Trade Secrets and Interferences with Contracts Division.

## ***Education***

J.D., University of California, Davis (2001)

Dubenstein National Bankruptcy Moot Court Participant

Executive Editor, *University of California Davis Law Review*

Public Interest Scholar

B.A., Gonzaga University, *summa cum laude* (1997)

Alpha Sigma Nu

Phi Alpha Theta

Certificate of Achievement in Lean Six Sigma, Villanova University (2009)

## ***Admissions***

California

## ***Courts***

U.S. Court of Appeals for the Ninth Circuit

U.S. District Court for the Central, Eastern, Northern, and Southern Districts of California

## ***Affiliations***

American Bar Association (Trade Secret and Interference with Contracts Vice Chair)

Association of Business Trial Lawyers

Beverly Hills Bar Association

ITechLaw Association (IP Committee Chair)

Los Angeles County Bar Association (Litigation Inn of Court)

International Franchise Association

State Bar of California (Executive Committee Member of Intellectual Property Section)

Society of Competitive Intelligence Professionals

## ***Representative Cases***

### **Trade Secrets, Non-Competes and Intellectual Property**

*US Foods v. Shamrock Foods et al.* (Represent food distribution company in theft of trade secrets case; obtained temporary restraining order as well as preliminary and permanent injunction).

*Kaplan Higher Education v. Mitchell et al.* (Represent higher education company in employee raiding and theft of confidential information suit).

*eLoyalty v. Spanlink Communications* (Represent telecommunications company in multi-state litigation involving non-competition and trade secret claims).

*Pacific Dental Benefits v. Liberty Dental et. al.* (Represent health care provider in suit involving trade secret and breach of duty of loyalty claims).

*Staffmark v. Westaff* (Represent staffing company in connection with multi-state litigation concerning non-compete and trade secret claims).

*Sara Lee v. Albrecht* (Represent Sara Lee in connection with ex-employees violating confidentiality and non-solicitation agreements in Nevada and New Mexico).

*PKELLEY Enterprises v. Crate & Barrel, Inc.* (Defend client in case involving alleged copyright infringement).

*US Tower et al. v. Wifeye, Inc.* (Prosecute claims for trade secret theft involving security technology).

*Robert Half International Inc. v. Bateman* (Assisted client in obtaining permanent injunctive relief against former employee's misappropriation of trade secrets).

*Vitek v. Countrywide* (Defend client in case involving alleged misappropriation of trade secrets and employee raiding).

*Rewards Network v. Acacia Funding* (Assisted client in obtaining injunctive relief against former employee's misappropriation of trade secrets).

*Specialized Direct Response v. Customer Satisfaction Improvement Corp.* (Assisted client in obtaining injunctive relief against use of trade secrets and unfair competition).

*Independent Ink Inc. v. Illinois Tool Works* (Assisted client in obtaining dismissal of suit for false advertising under Lanham Act).

*Advantage Partners v. Salton Inc.* (Assisted with defense of patent infringement suit).

*Save On Service Marketing v. Specialized Direct Response* (Defend client in case involving alleged misappropriation of trade secrets and employee theft).

*Vans Inc. v. GM Footwear Corp.* (Assisted client in obtaining permanent injunction in trademark infringement matter).

### **Complex Litigation**

*Ohanesian v. Bosley, Inc. et al.* (2010-present)(Obtained dismissal with prejudice of suit brought against corporate entities and individual for alleged breach of fiduciary duty and other business torts).

*Black Donuts v. Big O Tires* (2009-present) (Represent franchisor in putative class action dispute with franchisees).

*Woodhouse v. Lincoln Benefit Life Company et al.* (2010-2011)(Represent client in multiple party case on claims for breach of contract and elder abuse).

*Aral v. Earthlink* (2008-2009) (Represent ISP in putative class action related to internet service).

*Roy v. Heald College* (2008) (Represent postsecondary institution in putative class action related to alleged tuition overcharges).

*Louie v. Countrywide* (2007-2008) (Represent tenant in ADA access case involving multiple parties and locations).

*CRTA v. Peace* (2004-2008) (Action to restore \$500 million in pension benefits to retired teachers trust fund).

*Guerra v. Allstate Life Insurance* (2006-2007) (Represent client on claims for bad faith, breach of contract, and fraud).

*Davis v. California Culinary Academy* (2006-2007) (Obtained summary judgment in landlord-tenant dispute; decision affirmed by California Court of Appeal).

*Garcia v. Protective Life Insurance Company* (2006) (Obtained favorable resolution for client on claims for bad faith and breach of contract).

*Roseville Plaza LLC v. Sizzler USA Real Property* (2005-2006) (Represent tenant in dispute with commercial landlord relating to option rights).

*ANJ Construction v. Allstate Insurance Company* (2005) (Obtained summary judgment for client on claims for professional negligence and fraud and request for punitive damages).

*Spencer v. Easterday/Amsan* (2004-2005) (Represent tenant in dispute with commercial landlord relating to lease default issues, and pursue counterclaims for various claims including fraud, unfair business practices, and breach of agreement).

*Universal Underwriters Insurance Company v. M.F. Salta Co.* (2003-2004) (Obtained summary judgment for client on claims for breach of contract and bad faith).

### **Labor and Employment**

*Maricic v. C.H. Robinson* (2011-2012) (Represent client in hostile work environment suit brought by former employee).

*Santos v. CH Robinson* (2010-2011) (Represent client in sexual harassment suit brought by former employee).

*Park v. Kaplan* (2009-2010) (Represent client in arbitration involving claims for false imprisonment, battery, assault, breach of contract, and false promise).

*Doe v. McClatchy* (2009) (Disability discrimination case brought by former employee).

*Doe v. Countrywide* (2008-2009) (Race and age discrimination case brought by contractor).

*Wong v. Countrywide* (2008-2010) (Obtained complete defense award in arbitration involving claims for race discrimination, false promise, and breach of contract).

*Doe v. Countrywide* (2007-2009) (SOX whistleblower case brought by former employee).

*Hall v. CH Robinson* (2009) (Represent client in suit involving claims of sexual harassment and violation of non-compete).

*Junkin v. Countrywide* (2006-2007) (Wrongful termination case brought by former employee).

*Burkhardt v. Countrywide* (2006-2007) (Age discrimination case brought by former employee).

*People of State of California v. Spherion* (2006-2007) (Represent client in case involving alleged violations of Business and Professions Code for alleged wage and hour violations).

*In the Matter of the Appeal of Staff Resources, Inc.* (2005-2007) (Represent client in appeal of alleged OSHA violations).

*Keifer v. Hamilton Engine Products* (2005-2006) (Assisted client in obtaining summary judgment in harassment case in federal court).

*Hill v. QB Rebuilders* (2004-2005) (Defend client in case involving alleged harassment and hostile work environment).

### **Bankruptcy/Creditors' Rights**

*Big O Tires v. Park* (2010-2011) (Obtained writ of possession and preliminary injunction in security interest action).

*Banco Popular v. Cardinal & Gold* (2008-2009) (Represent lender in judicial foreclosure action).

*Kendall v. HSN Interactive LLC* (2007) (Represent client in turnover action brought by Trustee).

*Gomes v. Staff Resources* (2006-2007) (Obtained favorable resolution of wage claim in bankruptcy case).

*In re Precision Farming* (2005-2007) (Obtained favorable resolution for client in case involving significant wage claims and preference exposure).

*Allstate Life Insurance Company v. McKee* (2005-2006) (Obtained judgment against debtor for fraudulent conveyance).

### ***Publications***

"New Law Protecting Personal Social Media Of California Employees and Students Adopted In California," *Seyfarth Shaw LLP - Management Alert* (October 1, 2012)

- "California Court Rules That Non-Competition Agreement Contained In Employment Agreement Is Unenforceable Against Former Seller Even Though It Was Executed In Connection With The Sales Of A Business," *Seyfarth Shaw LLP - Management Alert* (August 29, 2012)
- "New Hampshire Enacts New Law Requiring Disclosure of Non-Compete and Non-Piracy Agreements Prior to Job Offer And Change In Job Classification," *Seyfarth Shaw LLP - One Minute Memo* (June 20, 2012)
- "Data Breach! What Next? Privacy Tips for IP Professionals," *New Matter*, Vol. 36 No. 2 (July 2011)
- "Combating Employee Data Theft With CFAA," *Law360* (June 15, 2011)
- "Recent Court Decisions Further Limit Use of Competitive Contractual Restrictions With California Employees and Demonstrate Need For Employers To Develop Effective Trade Secret Protection Plans," *California Employer* (March 2011)
- Courts Split on Proof Requirements for Unauthorized Access in Computer Fraud and Abuse Act Cases, *Oxford Univ. Press's Journal of Intellectual Property Law & Practice* (February 2010)
- "Keeping On The Right Side of The Line: A Trade Secret Law Perspective," *SCIP* (December 2009)
- "Unhealthy Competition," *Daily Journal* (April 02, 2009)
- "Noncompetition Agreements Invalidated," *California Employment Law Special Report*, published by the Society for Human Resource Management (SHRM) (April 2009)
- "Is Your Company's Non-Competition Clause Enforceable?," *California Lawyer* (Vol. 29, No. 2) 36 (February 2009)
- "Your Company Cannot Afford Not to Adequately Protect Its Trade Secrets and Other Confidential Information," *Bloomberg Law Reports*, Vol. 2 No. 47 (November 2008)
- "Recent California Appellate Decision Highlights Additional Arrow in the Trade Secret Litigator's Quiver: Attacking the Independent Economic Value Element of a Trade Secret Misappropriation Claim," *New Matter*, Vol. 33 No. 3 (November 2008)
- "California Supreme Court Rejects the Ninth Circuit's Narrow Restraint Exception to California's Prohibition on Employee Noncompetition Agreements," *Bloomberg Law Reports*, Vol. 2, No. 34 (August 25, 2008)
- "California Court of Appeal Strikes Down the State's Latest Attempt to Divert Public Pension Funds to Address Fiscal Problems," *The NAPPA Report* (February 2008)

"Recent California State Court Decision Strikes Down Broad No-Hire Provision," *New Matter*, Vol. 32 No. 3 (November 2007)

"Ruling Nixes Broad 'No-Hire' Provisions," *Employment Law360* (August 2007)

"California's SB 20 –The Latest Attempt to Divert Public Pension Funds to Address Fiscal Problems," *The NAPPA Report* (November 2006)

"Protecting Your Company's Trade Secrets," *Sacramento Area Human Resource Association Newsletter* (August 2006)

"Putting an End to Judicial Lawmaking: Abolishing the Undue Hardship Exception for Student Loans in Bankruptcy," 34 *University of California - Davis Law Review* 221 (Fall 2000)

### ***Presentations***

"Online Copyright Infringement, File Sharing and ISPs - Where Are We Now?" ITechLaw Webinar (July 26, 2011)

"Hot Topics in California Trade Secret Law," State Bar of California Intellectual Property Section, Trade Secret Subcommittee (June 2011)

"Trade Secret Investigations - The Legal and Technical Perspective," LegalTech West (May 2011)

"The Anatomy of a Trade Secret Audit: Is the Data that Drives Your Company Adequately Protected?," Seyfarth Shaw LLP Webinar ( May 2011)

"Managing and Protecting Information (Including Trade Secrets) in the Cloud," 2011 ITechLaw World Technology Law Conference & Annual Meeting (May 2011)

"Corporate Website Hazards: What In-House Counsel Needs to Know," Los Angeles County Bar Association's Corporate Law Department Section Business Roundtable (February 2011)

"Trade Secret Protection in a Mobile Employment Environment," State Bar of California Annual Meeting (September 2010)

"Trade Secret Litigation and Protection in California," Seyfarth Shaw LLP Webinar (May 2010)

"Employees Run Amok: A Roundtable Program on Recent Developments in California Trade Secrets Law and Covenants Not to Compete," Los Angeles County Bar Association's Corporate Law Department Section (April 2010)

- 
- “Keeping on The Right Side of the Line: Best Practices for Acquiring Competitive Intelligence from A Legal Perspective,” Society of Competitive Intelligence Professionals (SCIP) 2010 International Conference and Exhibition (March 2010)
- “Litigation / Arbitration with Franchisees: Cost Containment: How, When & Why,” International Franchise Association’s 50th Annual Convention (Feb. 2010)
- “Dowell v. Biosense Webster, Inc.,” Intellectual Property Law Section of the State Bar of California, Trade Secret Subsection (Feb. 2010)
- “Protecting Trade Secrets in Times of Increased Staff Mobility,” National Business Institute, National Live Teleconference (July 2009)
- “Operating in a Challenging Economy - Creating Efficiencies, Process Improvements and Predictability in Commercial and Employment Litigation,” Association of Corporate Counsel (July 2009)
- “Psst! Can You Keep a Secret? Making Sure that Trade Secrets Stay Secret Under the UTSA,” Beverly Hills Bar Association Intellectual Property, Internet & New Media Section (July 2009)
- “Brescia v. Angelin: Trade Secret Identification Under C.C.P. § 2019.210,” California State Bar’s Trade Secret Standing Committee of the Intellectual Property Law Section (July 2009)
- “Best Practices for Gathering Intelligence and Sealing Leaks Without Exposing Yourself and Your Company to Liability,” Society of Competitive Intelligence Professionals Annual Convention (Chicago, Illinois) (April 23, 2009)
- “Non-Compete/Non-Solicitation Issues in the Franchise Context,” International Franchise Association Annual Convention (San Diego, California) (February 17, 2009)
- “The Impact of Edwards v. Arthur Andersen, How it Will Affect Lawyers and Their Clients,” Reedlogic Video Seminars
- “Strategies for Handling Trade Secret Disputes,” California State Bar Annual Meeting (September 2008)
- “Asset Marketing Systems, Inc. v. Gagnon: Ninth Circuit Recognizes Trade Secret Exception to Business and Professions Code Section 16600?,” California State Bar’s Trade Secret Standing Committee of the Intellectual Property Law Section (September 2008)
- “How Not to Inadvertently Waive the Attorney Client Privilege,” Association of Corporate Counsel (July 2008)
-

“Anti-Slapp Motions & Cease and Desist Letters,” California State Bar's Trade Secret Standing Committee of the Intellectual Property Section (May 2008)

“How to Make the Most of Mediation,” Association of Corporate Counsel (Summer 2007)

“Protecting Trade Secrets,” Sacramento Area Human Resource Association

“Sarbanes-Oxley for the Human Resources Function,” West Coast Labor and Employment Symposium

---

# Michael D. Wexler

Chicago Office  
(312) 460-5559  
mwexler@seyfarth.com



## *Areas of Practice*

Trade Secrets, Computer Fraud & Non-Competes

Commercial Litigation

Intellectual Property

White Collar Criminal Defense

## *Experience*

Mr. Wexler is a partner in the firm's Chicago office and Chair of the national Trade Secrets, Computer Fraud & Non-Competes Practice Group. His practice focuses on trial work and counseling in the areas of trade secrets and restrictive covenants, corporate espionage, unfair competition, complex commercial disputes, intellectual property infringement and white collar criminal defense in both federal and state courts. A former state prosecutor, Mr. Wexler's extensive investigatory experience and considerable jury trial practice enables him to advise clients with regard to potential disputes and represent clients through and including a determination of their rights at trial. Mr. Wexler has successfully obtained and defended temporary restraining orders and preliminary and permanent injunctions in several jurisdictions. He has represented clients in the insurance, securities, finance, banking, transportation, manufacturing, technology, pharmaceuticals, advertising, real estate, employment, medical equipment and computer industries throughout the United States. He is available to assist with patent litigation and other litigation involving complex technology. Mr. Wexler is also a member of the Firm's Administrative Committee and Lawyer Development Committee.

## *Education*

J.D., IIT Chicago-Kent College of Law, High Honors (1991)

Order of the Coif; Kent Legal Scholar; Member, *Chicago-Kent Law Review*; Member, National Moot Court Competition Teams; Legal Writing Teaching Assistant

B.A., University of Illinois-Champaign (1988)

---

## ***Admissions***

Illinois

## ***Courts***

U.S. Court of Appeals for the Seventh Circuit

U.S. District Court for the Northern District of Illinois (Trial Bar)

U.S. District Court for the Central and Southern Districts of Illinois

U.S. District Court for the Northern District of Indiana

U.S. District Court for the Eastern District of Wisconsin

## ***Affiliations***

American Bar Association

Chicago Bar Association

Illinois State Bar Association

ITechLaw Association

## ***Representative Cases***

*Pitney Bowes Inc. v. Walter Buyea*, No. CV-06-167-LRS (U.S. District Court, E.D. Washington) (successfully obtained standstill order, contempt finding for violation of standstill order and settlement in trade secret misappropriation, breach of contract and tortious interference matter in the postal technologies industry).

*Jeffrey Silver v. C.H. Robinson Worldwide and C.H. Robinson Company*, No. 06 C 2070 (U.S. District Court, N.D. Illinois) (successfully defended and settled dispute regarding protection of proprietary software in breach of contract claim and distribution of \$8 million worth of stock matter in logistics industry).

*Fujitsu Network Communications, Inc. v. Bud Doherty and Tellabs Operations, Inc.*, No. CL 2006 1357 (Circuit Court, Fairfax County, Virginia) (successfully defended breach of confidentiality claim through motion practice and resulting settlement in telecommunications industry).

*C.H. Robinson Worldwide, Inc. v. Command Transportation LLC, Paul Loeb and Eric Harrison*, No. 05 C 3401 (U.S. District Court, N.D. Illinois) (successfully brought misappropriation of trade secret,

breach of contract, copyright infringement and Computer Fraud and Abuse claim to protect \$140 million purchase of proprietary software and associated business resulting in settlement in the logistics industry).

*Universal Engraving Inc. v. ITW-Davis-Davis Engineering, Michael A. Garcia, et al.*, No. 05 CV 7467 (District Court, Johnson County, Kansas) (defeated application for emergency temporary restraining order at hearing resulting in settlement in the die engraving industry).

*National Association of Securities Dealers Arbitrations*, September 2006 and October 2006, (Chicago, Illinois) (breach of contract, violation of non-compete and misappropriation of trade secrets matters in the banking and investment industry).

*Owens Corning v. Michael J. Joyce*, No. 05 C 4894 (U.S. District Court, N.D. Illinois) (defeated application for emergency temporary restraining order to prevent defendant from working at new employer due to inevitable disclosure and breach of contract claim in building supplies industry).

*Carlisle Syntec Incorporated v. Ronald D. Head*, No. 05-CV-2592 (U.S. District Court, Middle District Pennsylvania) (obtained favorable settlement for defendant in breach of contract and inevitable disclosure matter seeking to bar defendant from working at new employer or soliciting customers of prior employer in building supplies industry).

*National Seating Company v. Richard David Turner*, No. 14955 (Chancery Court, Monroe County, Tennessee) (defeated critical aspects of application for temporary injunction order seeking to prevent defendant from working for new employer in any capacity in transportation seat industry resulting in settlement at full evidentiary hearing).

*Pharmaceutical Research Associates, Inc. v. Clareece West*, No. 05 CV 02831 (District Court, Johnson County, Kansas) (defeated critical aspects of preliminary injunction seeking to prevent defendant from working for new employer and from soliciting any client of plaintiff resulting in settlement in the pharmaceutical industry at full evidentiary hearing).

*Ingenix, Inc. v. April Gardner*, No. 05-80474-CIV (U.S. District Court, S.D. Florida) (obtained settlement to return and protect proprietary information of plaintiff in breach of contract and misappropriation of trade secrets matter in healthcare software and claim processing industry).

*Motorola, Inc. v. Mike S. Zafirovski*, No. 05 CH 17744 (Circuit Court of Cook County, Illinois) (successfully settled non-compete and breach of contract action on behalf of Motorola against former COO who accepted position as CEO with competitor in telecommunications industry).

*VHS Genesis Labs, Inc. v. Kimberly A. Graddy, FirstSource Laboratory Solutions, Inc., et al.*, No. 05-CV-00577-DFH-WTL (U.S. District Court, S.D. Indiana) (successfully settled during preliminary injunction evidentiary hearing breach of fiduciary duty, conspiracy, misappropriation of

trade secret and computer fraud and abuse case on behalf of plaintiff in laboratory testing and billing industry).

*Long USA, LLC and Dana Canada Corporation v. Aztec Industries, LLC, Gary Jablonski and Lance Jenkins v. Douglas Beck, William Brierley and Jeff Hogan*, No. 04-72195 (U.S. District Court, E.D. Michigan) (obtained settlement restricting activities of former employees and protecting proprietary information of plaintiff where defendants had set-up competing business while working for plaintiff in the transportation parts industry).

*GE Medical Systems Information Technologies, Inc. v. iMedica Corporation, et al.*, No. 304 CV 2514-D (U.S. District Court, N.D. Texas) (obtained settlement in breach of contract and misappropriation of trade secret matter to protect proprietary information regarding physician management software).

*BrainLAB, Inc. v. Jason M. Papes and Stryker Corporation*, No. 04 C 5986 (U.S. District Court, N.D. Illinois) (obtained favorable offer of judgment on behalf of defendants after successfully barring plaintiff from presenting any evidence of damages at trial in alleged employee raiding case in the medical equipment industry).

*Neubauer-Perkins, Inc. v. Quinn Boland, Connected II, Inc., Howmedica Osteonics Corp. and Stryker Corporation*, No. 04 CH 19637 (Circuit Court of Cook County, Illinois) (obtained favorable settlement for defendant in breach of contract action attempting to bar defendant from working for new employer or soliciting any client of former employer in the medical device industry).

*Rewards Network Establishment Services, Inc. v. Marc Borge and Acacia Funding, Inc.*, No. 04-2530 GEB JFM (U.S. District Court E.D. California) (successfully obtained TRO in Computer Fraud and Abuse Act, trade secret misappropriation, conversion, unfair competition and breach of contract matter in the restaurant dining credits and marketing industry).

*United HealthCare Services, Inc. v. Interlink Health Services, Inc. and Marnie Bute*, No. 04 CV 04360 (U.S. District Court, District of Minnesota, Minneapolis Division) (successfully obtained order preserving status quo in Computer Fraud and Abuse Act, trade secret misappropriation and breach of contract case in the healthcare industry).

*Spectera, Inc. v. Kenneth Holt*, No. CV 04-07258 (U.S. District Court C.D. California) (successfully obtained ex-parte TRO and preliminary injunction at hearing in Computer Fraud and Abuse Act, breach of fiduciary duty and trade secret misappropriation case in the vision benefit industry).

*Dana Corporation v. Hafke, Sutter, Charlotte Pipe & Foundry Company and Mosey Manufacturing Co.*, No. 04-CV-71292 (U.S. District Court E.D. Michigan) (successfully defeated the critical portions of multiple motions to dismiss in breach of contract, conspiracy, Computer Fraud and

Abuse Act, trade secret misappropriation and tortious interference case in the manufacturing of engine cylinder liners industry).

*Life Fitness v. Precor USA and Charles Fedorka*, No. 5:04CV91-V (U.S. District Court W.D. North Carolina) (successfully defeated preliminary injunction at hearing in fitness equipment industry).

*The Medstat Group, Inc. v. William Crown, Ingenix, Inc. and UnitedHealth Group, Inc.*, No. 04-250-CK (Circuit Court of Washtenaw County, Michigan) (successfully defeated critical aspects of preliminary injunction at evidentiary hearing in retrospective and prospective pharmaceutical studies industry).

*EMC Document Systems, Inc. v. Michael R. Dale, et al.*, No. 3:04 CV 082AS (U.S. District Court N.D. Indiana) (successfully defeated preliminary injunction at evidentiary hearing in mail inserting and document management industry).

*Hub Group Ohio, LLC v. Peter Deltufo*, No. CV 2004-02-0515 (Court of Common Pleas, Butler County, Ohio) (successfully obtained TRO and preliminary injunction at hearing regarding intermodal transport industry).

*Medstrat, Inc. v. John J. DiMercurio*, No. 2003 CH 001716 (Circuit Court of DuPage County, Illinois) (successfully defeated TRO and preliminary injunction at evidentiary hearing regarding medical diagnostic imaging).

*Baxter Healthcare Corp. v. Dasari and Bayer Corp.*, No. C 03-3392 (U.S. District Court N.D. California) (successfully obtained TRO in Computer Fraud and Abuse Act and trade secret misappropriation case regarding biopharmaceuticals).

*Philip Services v. Reno*, No. 03 CV 4002 (U.S. District Court S.D. Illinois) (successfully obtained preliminary and permanent injunction in non-compete matter regarding industrial cleaning industry).

*Hub Group Tennessee v. Herzog, et al.*, No. CH 03 0166 2 (Circuit Court of Shelby County, Tennessee) (successfully obtained TRO and temporary injunction in trade secret and non-compete matter regarding intermodal transport industry at evidentiary hearing).

*Beasley v. Hub City Texas*, No. 2002 62901 (District Court of Harris County, Texas) (successfully obtained TRO and temporary injunction at evidentiary hearing in sale of business, trade secret and non-compete matter regarding intermodal transport industry).

*Pitney Bowes Inc. v. Allen, et al.*, No. 02 C 4674 (U.S. District Court N.D. Illinois) (successfully obtained TRO in federal Computer Fraud and Abuse Act, trade secret, unfair competition and

---

non-compete matter; settled matter; obtained ex-parte seizure order by U.S. Marshal's Service for alleged violations of settlement and court order).

*United Behavioral Health, Inc. v. Jensen*, No. C 02-1760 CRB ARB (U.S. District Court N.D. California) (obtained ex-parte TRO and preliminary injunction for violation of federal Computer Fraud and Abuse Act in the healthcare industry).

*3Com v. Cambia, et al.*, No. 01 CH 8253 (Circuit Court of Cook County, Illinois) (successfully defeated trade secret misappropriation TRO at hearing regarding 3G wireless technology).

*Kusen v. Cambridge Homes, Inc.*, No. 3-00-0767 (Third Appellate District, Illinois) (unpublished) (successfully argued appeal affirming summary judgment in favor of real estate developer and against former salesperson regarding contractual and commission dispute).

*Follett Corp. v. Davis*, No. 99 C 6418 (U.S. District Court N.D. Illinois) (successfully obtained TRO in trademark infringement/cyberpiracy case).

*Shukur v. Baxter Healthcare*, No. 00 L 000806 (Circuit Court of Lake County, Illinois) (successfully argued motion to dismiss defamation case brought by former employee).

*Pozdol v. Pozdol*, No. 01 C 7139 (U.S. District Court N.D. of Illinois) (successfully obtained ex-parte TRO and permanent injunction in Lanham Act violation matter).

*Union League Club v. Flores*, No. 01 CH 1119 (Circuit Court of Cook County, Illinois) (successfully obtained ex-parte TRO and permanent injunction in workplace violence matter).

*Hawkeye Medical Supply (McKesson) v. Caligor et al*, No. 00 CV 1283 (U.S. District Court Central District of Illinois) (successfully obtained TRO in Lanham Act violation and trade secret misappropriation case at evidentiary hearing).

*Marvin Triplett v. Stephany Welzien*, No. 45C010008CP01021 (Circuit Court of Lake County, Indiana) (successfully obtained dismissal of action for payment of reward money by mother of deceased son).

*United Airlines v. Hansberry*, No. 99 CH 11341 (Circuit Court of Cook County, Illinois) (successfully obtained ex-parte TRO and permanent injunction against former employee in trespass and workplace violence case).

*People v. Manietta*, No. 99 CM 3617 (Circuit Court of Will County, Illinois) (obtained acquittal after trial of corporate supervisor for alleged battery against line worker).

*LensCrafters v. United HealthCare, et al.*, No. A9901609 (Circuit Court of Hamilton County, Ohio)  
(defeated preliminary injunction at evidentiary hearing in trade secret, restrictive covenant and breach of fiduciary duty matter regarding managed vision care industry).

*Niedermaier, Inc. v. Polyfoam Packers Corporation*, No. 94 L 12608 (Circuit Court of Cook County, Illinois) (obtained favorable defense verdict after bench trial regarding missing polystyrene molds).

### ***Presentations and Lectures***

“Employment Law Conference: Trade Secrets and Non-Competes,” Law Bulletin Seminars  
(November 8, 2007)

“Protecting Confidential Information,” Document Retention and Destruction in Illinois, Lorman  
Education Services (June 16 and June 23, 2005)

Moderator, “Successful Corporate Strategy for Protecting Trade Secrets and Confidential  
Information,” Advanced Approaches to Labor and Employment Law for In-House Counsel,  
Northstar Conferences LLC (May 4, 2005; March 3, 2004)

“Trade Secrets Litigation Trends and Dealmaking Tips,” Law Seminars International (June 2003)

“Strategies for Defendants in Trade Secret Litigation,” Law Seminars International (June 2003)

Guest Lecturer, “Demonstrative Exhibits and Examination,” Chicago-Kent College of Law Intellectual  
Property Law Trial Advocacy (Spring 2003)

“Records Management, Policies and Destruction and Electronic Discovery,” Price Waterhouse  
Coopers General Counsel Forum (May 2002)

Guest Lecturer, “Direct and Cross Examination,” Chicago-Kent College of Law Intellectual Property  
Law Trial Advocacy (Spring 2002)



Atlanta

Boston

Chicago

Houston

Los Angeles

New York

Sacramento

San Francisco

Washington, D.C.

London

[www.seyfarth.com](http://www.seyfarth.com)

**Breadth. Depth. Results.**

©2012 Seyfarth Shaw LLP. All rights reserved. "Seyfarth Shaw" refers to Seyfarth Shaw LLP (an Illinois limited liability partnership). Prior results do not guarantee a similar outcome. Our London office operates as Seyfarth Shaw (UK) LLP, an affiliate of Seyfarth Shaw LLP.  
#12-907 10/12