Employment Law Daily Wrap Up, STRATEGIC PERSPECTIVES—Protecting IP in the era of mobile workers, (Jun. 9, 2015)

Click to open document in a browser

By Pamela Wolf, J.D.

In the current environment of an increasingly mobile workforce, employers face real challenges to their ability to protect intellectual property. Greater employee turnover, increasing use of independent contractors, and the sheer volume and ease with which IP can be transferred all contribute to the problem, according to a panel of Polsinelli attorneys who discussed these and other challenges. Among the most important questions that employers must answer are what exactly qualifies as IP and who owns it? And, of course, employers must make sure they protect it.

Independent contractors. Independent contractors present a problem in that they are using their expertise not just for your company, but for their other clients as well, observed Polsinelli Shareholder Jim Swartz, who works in the firm's Atlanta office. Employers need to think about what steps they can take to "cabin" IP information that is accessible to independent contractors, as well as to clarify understanding about exactly who owns what, Swartz suggested.

Adam Weiss, a shareholder in Polsinelli's Chicago office, added that it's important for independent contractors to know that they also represent the company—customers, after all, really can't tell who is an independent contractor and who is an employee. With that in mind, employers should make sure that independent contractors understand what the company is about and what is the company's IP. Weiss suggested that companies use a clear written agreement that states who owns what: what the independent contractor has developed and what the company has asked the independent contractor to develop.

Social media questions. Social media has become an increasingly important means of communication for companies and their employees, which gives rise to the question of to whom the information on social media belongs, Polsinelli Shareholder Karen Glickstein pointed out. It's hard for an employer to protect a customer list when the same information is available on a LinkedIn page (perhaps via "connections"), she observed. Shareholder Steve Fox, who practices in the firm's Dallas office, said he doesn't see companies litigating over the secrecy of customer lists because of social media, but rather the *secrecy of the customer relationship*, such as how much business the company does with that customer.

Glickstein also cited a few court cases that exemplify some of the social media issues facing employers, such as whether an executive can take his Twitter handle and followers with him when he leaves (*Phone Dog v Kravitz*); who owns websites, blogs, and online content (*Artis Health v Nankivell*); who owns a mixed personal and professional social media account that may be considered an asset of the company because it's been used to promote it (*In re CTI, Inc*); and who owns an employee's LinkedIn account (*Eagle v EdComm, Inc*).

Most of these issues can be dealt with "on the front end," according to Swartz, by helping employees understand what the company defines ownership to mean and by using written agreements.

Courts are also beginning to see lawsuits raising issues of misrepresentation where social media indicates, incorrectly, that an employee is still affiliated with a company when that is not the case, according to Glickstein. With that in mind, Weiss suggested using exit agreements that incorporate an agreement that the company owns the marks and employees cannot use them when they leave the company. Companies can obtain the same agreement during the hiring process, Fox added.

Uniform Trade Secrets Act. Swartz turned his attention to the Uniform Trade Secrets Act, which he noted has been adopted in virtually every jurisdiction. Some states, he said, consider it the exclusive remedy for trade secret claims. The UTSA defines trade secret to include:

- Information (*e.g.*, patterns, compilations, programs, devices, methods, techniques, or processes) that …

- Derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons … and
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Most of the cases Swartz has seen recently have been in the area of *nontechnical* information, such as business plans and pricing information. Technical information, he pointed out, is often obviously a trade secret.

Protecting secrecy. What are the "reasonable efforts" to secure secrecy that employers must use? First of all, it's not "all conceivable efforts," according to Fox, butt it may include these:

- Placing the information in a vault accessible only to limited authorized employees;
- Requiring employees to sign agreements;
- Implementing sign-in and sign-out procedures;
- Stamping "proprietary" on materials; and
- Requiring passwords to access databases (and even better, limiting access to specific employees).

What about bidding information or plans that are not marked "Confidential?" Courts may not require a confidentiality agreement to find such information a protected trade secret, Fox said, *so long as* the company has explained in writing either that they are confidential or that they cannot be used outside the bidding process.

Swartz also raised the question of how companies can create an affirmative obligation of confidentiality in instances where the information is not technically a trade secret. He suggested using a tailored confidentiality agreement describing the information—hopefully, that would get beyond Trade Secrets Act preemption.

Glickstein recommended that companies update agreements to demonstrate that their agreements are serious, the information is protected, and to ensure employees understand that the company takes it seriously.

Threatened misappropriation. Injunctive relief for anticipated use of trade secrets is permitted under the UTSA, Glickstein pointed out. This applies to situations where a defendant has *access to trade secrets* and *joins a competitor* to perform duties *so similar* that the court believes those *duties cannot be performed without using the trade secret.*

Swartz noted that courts are adverse to granting injunctive relief that prevents former employees from working at a subsequent employer (not so in Texas, according to Fox). Courts are more willing, however, to grant injunctive relief that bars former employees from *using protected information*, Swartz said.

Third-party cloud services. Before permitting employees to use increasingly popular third-party cloud service providers, companies should make sure there is a reasonable amount of confidentiality maintained, according to Swartz. He suggested that companies should think through in advance how they want to utilize cloud storage. Companies should either have a policy on how to use cloud storage, or take it off the table, he said.

Protect competitors, too. It's also in companies' best interests to take steps to protect their competitors' confidential information when new employees come on board. This can be done during the recruitment and hiring process, according to Glickstein. Companies should find out the recruit's contractual obligations (such as in restrictive covenants) at that time, she said.

Fox added that companies should train employees involved in hiring to avoid soliciting other employers' confidential information and should send letters to job offerees instructing them not to bring confidential information from their former employers.

Comprehensive program. A comprehensive program to manage confidential information includes these elements, according to the Polsinelli attorneys:

- Confidential information/trade secrets inventories
- [Controlled] access to information
- Identifying corporate "custodians" of information
- Obvious labeling/marking of information
- Physical security

- IT security

Training. Current employees should also be educated about trade secrets and confidential information. Swartz recommended that companies have an ongoing training program on confidentiality. He said that in sensitive areas, sitting managers down once a year to talk about what they can and cannot do is really helpful.

Exit interviews. Post-employment confidentiality measures are important, too. Swartz suggested that in exit interviews, companies should do more than just require employees to sign documents; they should talk to exiting employees about confidential information and investigate proactively to find out what they had access to and where that information was stored.

Fox suggested that companies ask employees during the exit interview where they are going to be employed next and what they will be doing there.

Glickstein also cautioned companies to make sure they secure the exiting employee's computer drive—in the event of litigation, that will show the judge what the company has done to protect confidential and trade secret information. It's also important to preserve evidence and secure data. The risk of a breach should be assessed.

Source: Polsinelli's annual labor, employment, and benefits conference, titled, "Taking the Lead: Legal Strategies to Break Away from the Pack," was held on June 3 at the Chicago Botanic Garden in Glencoe, Illinois. Information about upcoming events is posted on the firm's website.

MainStory: Conferences Privacy ComputerFraudPrivacy StateLawClaims IndustryNewsTrends