TEXAS LAWYER
April 2, 2012
An ALM Publication
PRACTICE FOCUS
LABOR & EMPLOYMENT

How to Prevent Trade-Secret and Employee-Mobility Suits

BY LAURA M. MERRITT AND CHARLES T. GRAVES

Gone are the days when an engineer graduated from college, worked at a large company for 40 years, and retired with a pension and a gold watch. Due to increased corporate-structure shifts, a general working culture of free agency and rapid changes within industries, employees who reach retirement age with a dozen or more employers in their job histories are the norm.

In-house counsel must be involved in developing and implementing policies and procedures that help the human resources department and departmental supervisors operate effectively to avoid mobility suits from former employers and prevent misconduct that requires litigation by the company to protect its own information. Here are six ways the legal department can accomplish these goals.

1. Ensure that employees sign confidentiality and invention-assignment agreements on the first day of work, if not before. Even in companies with sophisticated human resources departments, in the hustle to get employees in the door, this agreement can be overlooked.

Such an agreement goes by different names. Essentially, it is that agreement in which the employee assigns intellectual property (using the magic wording blessed by the U.S. Court of Appeals for the Federal Circuit, such as "hereby assigns"), discloses any works of prior ownership, promises to keep confidential data confidential and return it when departing, and agrees not to bring third party data aboard.

2. Provide meaningful training. Even well-intentioned employees do not

always understand the confusing legal rules for trade secrecy, nonsolicitation and other restrictive covenants, invention assignments, work for hire and related doctrines. Adding an intellectual property and confidentiality training session to an annual conference or monthly lunch-and-learn opportunity is invaluable.

An employee rushing to meet deadlines can forget to take even simple steps, such as marking confidential information, maintaining the integrity of system passwords and utilizing common sense protections when working in public spaces. Frequent and direct reminders can prevent compromise of the company's private data. Training also can present an opportunity to remind employees about the "no reasonable expectation of privacy" language in the policies governing the company's electronic systems.

3. Gain control of remote-access and data-protection policies. Allowing unfettered, unmonitored access to all company systems can result in unintended information leakage, make it easy for employees to download key company documents and facilitate accidental exposure of the company's trade secrets via the mobile working environment.

It is often helpful to create written policies that restrict employee access to key company documents to a need-to-know basis. Creating electronic firewalls to restrict computer access is prudent, as is monitoring employee downloading and remote usage, particularly during sensitive periods such as the time between an employee's resignation announcement and departure date.

This not only helps control exposure but can provide helpful evidence in litigation to show that the company did not grant employees widespread access to its confidential information and trade secrets and took reasonable measures to protect that information.

4. Data protection and employee-mobility restrictions affect incoming and outgoing employees. From a defensive perspective, implementing and enforcing a search-and-purge requirement for incoming employees is perhaps the single most important mechanism to prevent an employee's former employer from suing the new hire and the company. Make it mandatory for each incoming employee to completely and carefully search all

personal computers, drives, handheld devices and other data repositories for anything belonging to a former employer, then either return or delete it before starting with the company.

Similarly, requiring upfront disclosure of restrictive covenants will help prevent a surprise restraining order from showing up on the general counsel's desk. In all but the most directly competitive, high-level employee situations, an in-house counsel generally can work out a compromise with the former employer to allow the employee to continue work without litigation.

When an employee is leaving the company, enforcing a search-and-purge requirement for departing employees will help protect company property and information. The employee should sign a certification stating that the employee has done so and either returned or deleted everything belonging to the company.

HR SHOULD PERFORM A MEANINGFUL EXIT INTERVIEW BEFORE THE EMPLOYEE'S LAST DAY OF WORK.

HR should perform a meaningful exit interview before the employee's last day of work. Topics for discussion: Has the employee searched her home computer and external drives for confidential information? Has she returned hard copies?

HR should obtain the employee's written representation that he understands and will comply with his obligations pursuant to the confidentiality agreement. It should provide the employee with a copy of the confidentiality agreement for his personal files and specifically remind him about the confidential-information protection and restrictive covenants to which he is subject.

Also, HR should ask for the employee's subsequent employer. If the employer refuses to disclose it, HR should know that this is a red flag, justifying follow-up from the legal department or outside counsel.

5. *Let laptops cool off before allowing the IT department to repurpose them.* A departing employee may leave forensic traces of illicit downloads, improper document access or even competitive activity on a work computer. If the company's standard operating policy is to permit the IT department to repurpose and wipe clean departing employees' devices, valuable forensic evidence can vanish before the legal need for it becomes apparent.

In the event of a high-level or potentially controversial departure, the legal department may want to consider a proactive forensic review even in the absence of a specific claim. If that's not possible, imaging the employee's hard drive can mitigate losses.

6. Don't rely only on unpredictable noncompetition covenants alone. Noncompetition, nonsolicitation, noninterference and other restrictive covenant litigation is highly volatile and constantly changing, and the law varies from state to state. Even the most well-drafted, recently updated, legally compliant and reasonable Texas noncompete agreement may not work if the employee moves to another state, the law changes or particular circumstances make it difficult for a judge to see how stopping the departing employee from taking the next job is a reasonable way to protect intellectual property.

Nevertheless, to the extent well-drafted restrictive covenants are enforceable, having them in place for key positions can be a helpful preventative strategy. Such agreements should be as individualized as possible and reasonable in scope, duration and geography.

Even if the company ultimately cannot enforce the agreement wholesale, it will be a jumping off point for a discussion with a departing employee's prospective employer. It may deter departing employees who are starting a business or joining a competitive business from doing so without seeking the company's blessing. IHT

Laura M. Merritt and Charles T. Graves are partners in Wilson Sonsini Goodrich & Rosati in Austin and San Francisco, respectively.