EMPLOYMENT & LABOR RELATIONS LAW
AMERICAN BAR ASSOCIATION SECTION OF LITIGATION

Winter 2014, Vol. 12 No. 2

Social Media: Protecting Trade Secrets and Proprietary Information

By Paul Cowie, Bram Hanono, and Dorna Moini

The ability of employees to steal trade secrets, reveal customer lists, and expose proprietary business information with the press of a button is frightening. In over 85 percent of trade-secret cases, the alleged misappropriator is someone the trade-secret owner knows, typically either an employee or a business partner. David S. Almeling et al., "A Statistical Analysis of Trade Secret Litigation in Federal Courts," 45 *Gonzaga L. Rev.* 291, 303 (2009). With the widespread use of mobile devices by employees, particularly because of bring-your-own-device (BYOD) policies and the increase in social media and cloud-computing platforms as a way to share and transfer data, the risks for employers are significantly increased. Some of the most common risks arising from the use of mobile devices and social media are employees taking or revealing customer lists, posting confidential information on social-media platforms, and moving data off the company's network. It's common for employees not to even realize what they have done. Courts are beginning to grapple with these types of cases, which provide lessons for employers. Not surprisingly, with innovations such as Card Munch, which allows a user to take a picture of a business card on a mobile device and automatically convert it to a LinkedIn contact, and other popular social-media applications such as Facebook and Twitter, trade-secret litigation is increasing exponentially. The number of cases filed in federal court is predicted to double by 2017. Almeling, *supra*, at 293. As a result, employers need to carefully craft policies and procedures to deter trade-secret misappropriation and, in the event litigation is unavoidable, position themselves to prevail. A review of recent cases highlights the potential costly impact of failing to implement these policies.

Trade-Secret Basics

The Uniform Trade Secrets Act (UTSA) defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process." Forty-seven states have adopted some version of the UTSA. To qualify as a trade secret under the UTSA, the information must derive economic value from not being generally known to the public, and the trade-secret owner must take reasonable steps to maintain secrecy of the information. The inquiry is fact-specific, taking into consideration factors such as the sensitivity of the information, the individuals who need access, and the internal procedures and practices taken to protect the information. Customer lists and business plans can be trade secrets.

Social-Media Contacts as Confidential Customer Lists

One of the biggest risks facing employers is that customer lists are increasingly at risk of losing their status as a trade secret because employees are both intentionally and sometimes unwittingly eviscerating the possibility that customer lists will qualify as a protected trade secret. Businesses,

typically those that employ a large sales force, often use social media as a vital tool to market and connect with customers, and they encourage their employees to do the same. These marketing techniques, while accepted as a common business practice, raise doubts about ownership of customer lists. In the first trial of its kind, the court in *Eagle v. Morgan* held that, absent a social-media policy, a LinkedIn profile—and all of its connections—belonged to the individual, not the employer. *Eagle v. Morgan*, No. 11-4303, 2013 U.S. Dist. LEXIS 34220 (E.D. Pa. Mar. 12, 2013). This case highlights the necessity to implement a comprehensive social-media policy covering ownership of social-media accounts. The issue, however, is compounded when considering the variety of social-media platforms that employees use across the workforce to communicate with clients and to solicit their business. When a top salesperson leaves for a competitor, does the social-media policy require him or her to delete the contacts he or she has made while employed?

As litigation increases and courts confront the question of whether various types of social-media information can be considered trade secrets and what employee actions may constitute misappropriation or breaches of confidentiality, a comprehensive policy is vital to prevailing in court.

Despite these challenges, the courts have indicated that businesses may have a viable trade-secrets claim with respect to customer lists on social-media accounts. *PhoneDog v. Kravitz*, No. C 11-03474, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011). In *PhoneDog v. Kravitz*, PhoneDog, an interactive mobile news-and-reviews web resource, sued its former employee, Noah Kravitz, alleging that Kravitz had improperly taken control of a Twitter account that PhoneDog provided him during his employment. Kravitz used the account to disseminate information and promote PhoneDog's services on behalf of PhoneDog. After his separation from the company, Kravitz changed the name of his Twitter handle from "@PhoneDog_Noah" to "@noahkravitz," but retained the 17,000 Twitter followers he had obtained during his employment with PhoneDog. PhoneDog sued, claiming that the Twitter followers constituted confidential, proprietary, and trade-secret information. At the initial pleading stage, the court found that PhoneDog had identified its alleged trade secrets—the account followers and Twitter password—with sufficient particularity so that the suit was viable. The case, however, settled shortly thereafter under terms that allowed Kravitz to maintain his Twitter account and followers. The court never decided whether the contacts actually constituted trade secrets. This case is instructive because it reiterates the need for employers to clearly identify their trade secrets, which can be accomplished with an appropriate social-media policy.

In another case, *Christou et al. v. Beatport, LLC*, the owner of several nightclubs, Regas Christou, sued his former employee for alleged trade-secret misappropriation. 849 F. Supp. 2d 1055 (D. Colo. 2012). While employed, the former employee had created an online marketplace for electronic dance music, called Beatport, with Christou's financial support. When the employment relationship ended, the employee founded his own competing club and threatened DJs that they would not be featured on Beatport if they performed at Christou's clubs. Denying the defendants' motion to dismiss the case, the court found that whether the plaintiffs' MySpace friends list was a trade secret was a question of fact and that Christou had alleged sufficient facts to maintain a trade-secret claim—at least at the pleading stage.

Similar cases are being litigated in European jurisdictions as well but with different results. For example, the High Court in London in *Whitmar Publications Ltd. v. Gamage* recently granted an injunction prohibiting the use of LinkedIn group contacts created in the course of an employee's employment. The employees had secretly collected the contacts while they were still employed and subsequently used them to set up a competing business. *Whitmar Publ'ns Ltd. v. Gamage*, [2013] EWHC 1881.

Status Updates and Tweets as Solicitations

Another scenario generating litigation arising from the use of social-media accounts is where employees, whether intentionally or inadvertently, solicit customers and/or former colleagues through status updates and tweets about a new job.

Invidia, a hair salon, faced this situation when its former employee resigned and information about her new job was posted on her Facebook page. *Invidia, LLC v. DiFonzo*, 30 Mass. L. Rep. 390 (Mass. Super. Ct. 2012). In *Invidia*, the hair-stylist employee had signed a non-solicitation agreement prohibiting her, for two years, from soliciting any of Invidia's clients or customers with the intention of providing the same or substantially similar services to those clients or customers. Four days after resigning from Invidia, DiFonzo's new employer posted a "public announcement" on her Facebook page, noting her new affiliation. In the comments below the post, an Invidia client, who was one of at least eight clients who had become Facebook friends with the hair stylist during her employment, posted "See you tomorrow!" and canceled her appointment at Invidia.

Despite the non-solicitation agreement, the court denied the employer's motion for preliminary injunction and held that staying Facebook friends with customers and posting about a new job did not constitute solicitation of the former employer's clients. The court held that as long as the client contacted the employee and not vice versa, there was no "solicitation."

By contrast, in *Corporate Technologies, Inc. v. Harnett*, the court concluded that an employee had unlawfully solicited his former employer's customers by sending an email blast announcing his new job. *Corporate Techs., Inc. v. Harnett*, No. 13-1706, 2013 U.S. App. LEXIS 19462 (1st Cir. 2013). Although the employee insisted that he had not solicited the employer's former customers because they had contacted him, the court was not convinced, holding that non-solicitation rights "cannot be thwarted by easy evasions, such as piquing customers' curiosity and inciting them to make the initial contact with the employee's new firm." These cases demonstrate the subtleties at play when determining whether there has been an improper solicitation and the need for employers to identify the type of conduct that is intended to be prohibited.

Inadvertent Disclosures

With the increasing use of social media in the workplace, employees may jeopardize confidential information in novel and unpredictable ways. For example, a seemingly innocent tweet or geo-location "check-in" could reveal a secret or a proprietary business plan. Many social-media sites do not even require the user to input his or her location at the end of a post; rather, the location is

automatically appended to the post. If the employer is negotiating a merger or acquisition, for example, an employee's frequent "check-ins" at the other company could reveal the identity of the target company. Similarly, if employees unexpectedly "friend" or "like" employees at the target company, that may also inadvertently reveal inside information. These types of disclosures are often unintentional, but without guidance from their employer, employees may not consider the consequences of such actions. Once again, a robust policy can provide direction and create values by putting employees on notice as to what the employer considers to be trade secrets and what steps should be taken to protect them.

BYOD vs. Employer-Issued Devices

Employers are increasingly moving from providing employees with company-owned devices to a BYOD system. But what are the consequences for trade-secret protection? Employer-issued devices provide potential benefits because of the ability for employers to mandate and control use of the device. They are company-owned property, can be limited to use for business purposes, and with the right policy can allow the employer to fully inspect and monitor the device. Employer-issued devices also diminish an employee's expectation of privacy. Additionally, the device and all data on the device must be returned at the end of employment.

With BYOD and the use of personal devices in general, it is much easier for employees to intentionally or unintentionally move trade secrets or other confidential information off company servers. First, the expectation of privacy and access to such personal devices is inevitably much more limited because it is the employee who owns the device, so employers cannot restrict the use of such devices to only business purposes. The result is that business and personal communications may become intertwined so that it becomes difficult to identify what belongs to the company and what belongs to the employee. At the most basic level, the employee's and the employer's contacts are likely to be commingled. How is a court to discern which contacts legitimately qualify as trade secrets? At the next level, what right can an employer maintain to inspect and monitor communications on such personal devices? The answer often relates back to the employee's reasonable expectation of privacy and whether the employer has instituted policies to protect specific business purposes.

For example, in *Stengart v. Loving Care Agency, Inc.*, the Appellate Division of the New Jersey Superior Court held that an employee had a reasonable expectation of privacy in communications with her lawyer via a personal email account, even though she used her employer's device. 408 N.J. Super. 54, 59 (N.J. Super. Ct. App. Div. 2009). In supporting its decision, the court relied on the sanctity of the attorney-client relationship but also cited the employer's policy, which stated that the employer reserved the right to review and access "all matters on the company's media systems and services at any time." The court found that "media systems and services" was too vague to inform the employee that she might be monitored. Of course, employers should also be aware of statutes such as the Electronic Communications Privacy Act of 1986 and the Stored Communications Act, which limit the employer's ability to access employee communications without consent.

Disposal of BYOD devices can also be problematic. For example, many employees sell their devices on eBay but forget to wipe them beforehand. If the employer has no policy or agreement

in place, the employer has limited ability to control what a former employee does with the device. Through mobile device management (MDM) software and/or a company buy-back policy, the employer can safeguard against these risks. MDM software helps employers manage mobile devices across the company's network. By controlling configuration settings, MDM can optimize the security of a BYOD program, by, for example, allowing the employer to remote-wipe a company email account upon separation of employment.

Thus, in conjunction with proper social-media policies, employers should institute BYOD policies that outline appropriate use regarding company documents and data. Companies can also consider a policy whereby cloud storage is prohibited for work-related documents. Alternatively, employers may consider creating a corporate-owned cloud account so that usage can be monitored. If an employer decides to use an outside cloud-storage service, it is important to ensure it offers full data encryption and allows employers to configure security settings and access controls. Services such as box.com, for example, encrypt data and documents upon transfer and have an intrusion-detection system that continuously monitors network traffic.

Crafting Policies and Agreements

All of these issues drive the need to implement robust policies regarding social media and mobile devices. There is ample room for development in establishing the rights and boundaries of both employers and employees as the use of mobile devices increases, social media changes, and litigation continues. Notably, many of the cases discussed above were decided at the preliminary stage, so it remains to be seen how courts will respond to these issues and what can be protected as trade-secret information.

To protect sensitive information and gain an advantage in the event of litigation, employers should create policies that address confidentiality and social-media ownership, and they should provide notice to employees regarding what constitute trade secrets and requirements regarding how to protect such information from disclosure. Employers should also implement targeted policies addressing the use of mobile devices, including the following:

- **Mobile-device management.** Employers should implement an MDM program on personal devices as a requirement for access to company documents. Most MDM programs also allow the employer to remote-wipe devices upon separation of employment. This can include Facebook and LinkedIn accounts explicitly belonging to the employer. An appropriate BYOD policy will address use during and after termination of employment and the protocols for appropriate use and data protection. It should also curtail privacy expectations and create consent to access and obtain information from the device. The challenge is effectively creating a policy that balances an employee's right to privacy and protection of personal data against the ability to protect company-owned material. The good news is that technology is continually developing to address these needs. *See, e.g.*, Press Release, Bradford Networks, Bradford Networks and MobileIron Partner for Secure and Compliant BYOD (Sept. 23, 2013).
- **Restricted access.** Restricted access should be part of an overarching objective applied to each of the policies described above because limiting access to

confidential documents is necessary to prove that the employer took reasonable measures in protecting the secrecy of its trade secrets. Access to documents should be on a "need to know" basis, and electronic files should have adequate password protections, especially in large corporations where hundreds of employees work on one network.

- **Termination of access.** Ensuring that former employees no longer have access to accounts, intranets, and other means of accessing confidential information is essential. A series of high-profile cases reiterates why it is important to implement standard protocols for terminating access. For example, in March 2013, a terminated Reuters journalist was indicted on felony charges of conspiring with a hacker group to deface the *Los Angeles Times* website, after he provided the Anonymous hacking group with log-in credentials for a Tribune Co. server.
- **Protection of privacy.** Finally, when crafting social-media policies, employers must respect employee privacy. Specifically, employers must comply with state laws addressing employer access to personal social-media accounts and decisions issued by the National Labor Relations Board (regarding policies that may be construed to chill or discourage employees from discussing work conditions under section 7 of the National Labor Relations Act). Indeed, pending legislation in some states may prohibit even asking whether the employee has a social-media account.

Conclusion

BYOD is here to stay and the use of social media and cloud-computing platforms will continue to increase and evolve as new social-media applications are created. Changes in the mobile landscape bring risk to employers and threaten their ability to protect trade secrets and other proprietary business information. Courts are just beginning to address these issues, and it remains to be seen what boundaries will be set regarding the protection of employer trade secrets and employees' rights to maintain social-media accounts before and after their employment. To protect trade secrets, deter misappropriation, and prevail should litigation become necessary, employers should implement robust policies regarding the use of social media and mobile devices.

Keywords: litigation, employment, labor relations, trade secret, social media, customer list, proprietary, employee, LinkedIn, Twitter, BYOD, non-solicitation, confidentiality agreement, mobile device management, privacy

Paul Cowie is a partner with Shepard Mullin in Palo Alto, California. Bram Hanono and Dorna Moini associates in the firm's San Francisco, California, office.