Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Social Media: A Danger To Company IP

Law360, New York (May 29, 2012, 1:06 PM ET) -- Social media and its impact on the workplace have long been objects of fascination in the media. Rarely does a month go by without news coverage of employees losing their jobs — or job applicants being turned away — for posting inappropriate online material on Facebook or elsewhere. No matter how often the scenario is played out, the questionable user behavior continues unabated.

This coverage has helped raise employers' awareness of the impact of online material harmful to their brand. And that awareness has in turn lead to a widespread effort to internally monitor such material, an effort that often becomes an important part of human resources and brand managers' responsibilities. Employers now recognize that an employee's derogatory tweet about his firm's product or service, if disseminated, can cause more damage to a brand than any number of negative reviews.

But while the impact of social media on human resources and brand management is well documented, its impact on intellectual property rights is the object of far less scrutiny. That is perplexing. Social media damage to corporate IP assets can hurt a company's value and bottom line far more than the over-sharing of holiday party snapshots ever could. Employers need to understand why this issue has become important, how social media can damage their IP, and what they can do to protect their assets.

Why Should This Be of Particular Concern to Employees at This Time?

The impact of social media on corporate activities is now magnified because social media is near-ubiquitous and the line between professional and personal social media communications is largely blurred.

That is in part the result of hardware developments. Gone are the days when an employee would use a Blackberry for professional communications, and a personal device (such as a laptop or smartphone) for personal communications. Nowadays, Bring Your Own Device (BYOD) is the norm. Employees generally expect to use their personal mobile device to access their work email and network. Traditional complaints from corporate IT departments about security concerns, or the need for device homogeneity among the workforce, have been largely set aside. Employees now conduct business and personal communications on the same devices.

But that blurring of lines is also the result of modern workplace practices. Many firms now allow their employees to use Facebook, Twitter or Pinterest in the workplace (and the firms that don't hopefully recognize that they still take place surreptitiously). An employee might write an email to a client one minute, broadcast a tweet the next, then generate a PowerPoint presentation for her boss before editing pictures on Instagram — all while sitting in her office. This has helped close, to employers' detriment, the privacy divide between what individuals are willing to share about themselves, and what their employers are prepared to share about their corporate activities.

These developments are plainly welcomed by employees, who can remain plugged in to their social networks at all times. However, they should be a source of headaches for companies concerned about protecting their IP assets — whether they exist in the form of patents, trade secrets or copyrights — as one social media slip-up can be enough to cause grave damage to those assets.

How Can Social Media Harm a Company's IP Assets?

Patents

The principal cause of harm to a company's patent IP as a result of social media abuse is the inadvertent, and premature, disclosure of a new invention.

An applicant will not be entitled to a patent on an invention if that invention was described in a printed publication more than one year prior to the date of the United States application,[1] and Internet publications (such as Facebook messages or tweets) will be deemed "printed publications."[2] Thus, if anyone prematurely discloses on Facebook information relating to an invention, that invention may well be deemed unpatentable, either during prosecution, or as a result of a later validity challenge in federal district court. The solution seems obvious: Make sure your research and development team is focused on patent development, and keep them away from all social media. But that is unrealistic.

First, teams of engineers often care primarily about the technology they are developing, and their technological contributions to the field. They focus far less on obtaining patent coverage on those contributions, for two reasons: (1) all rights to the resulting patents are generally assigned to their employers, leaving the employees with only an emotional stake in the patents, and (2) the engineers rarely have direct involvement in IP portfolio management. These engineers therefore do not have patent protection at the forefront of their mind when they use social media.

Second, collaborative creative teams are likely to rely on social media as a work tool for sharing ideas among team members. These may collaborate internally by communicating over email, Gchat, text messages, and occasional Facebook messages and tweets — a system that promotes the team's efficient progress toward its goal. But it is exactly this use of social media in the work context that is most likely to lead to inadvertent publication of protectable material. All it takes is an ill-conceived (and enabling) Facebook post proudly describing to friends the team's success in developing a new prototype, or a cellphone picture of said prototype shared on Twitter or Pinterest, to hamstring a company's efforts to patent the invention.

This lack of focus on the importance of IP, combined with the pervasiveness of a social media communication in the workplace, means that conditions are ripe for social media missteps. And those missteps can be costly. Hundreds of hours of engineer time, millions of dollars in R&D — it can all be rendered worthless by one ill-advised social media outburst.

The danger now is that employers may not recognize the risks involved, because social media disclosure issues are not yet common in the patent field. But these issues will become mainstream as increasingly tech-savvy counsel become accustomed to scouring the social media realm, through the process of discovery or otherwise, for invalidating disclosures.

Trade Secrets

Similarly vulnerable to social media disclosure are corporate trade secrets. The Uniform Trade Secrets Act defines a trade secret as information (1) that is valuable because it is not known or discoverable by other people who might benefit financially from it, and (2) that is the subject of reasonable efforts to keep it secret.

Trade secrets don't mix well with social media. Once the secret has been disclosed on a social media public platform, it is difficult to place it back under wraps. Consider the example of an employee at Coca-Cola Co. — a company whose trade secret recipe for its most famous product is said to be known by only a handful of people. After a week of late nights at the office, the employee finally logs on to Facebook or Twitter on Friday afternoon and posts: "Just finished purchasing orders for 50 tons of ingredient X. Am exhausted and ready for the weekend!" If the presence of ingredient X in the formula is not public knowledge, Coca-Cola may now have a problem.

While systems like Facebook or Twitter generally have defined procedures to address copyright violations (more on that below), the recourse available to a trade secret holder is less clear. Of course, Coca-Cola can request that the employee delete the message (which the employee may or may not agree to do), but by the time the company becomes aware of the post, the information may have been displayed for days, and worse, may have been reposted by any number of other users.

Even if the social medial platform agrees to cooperate and help track down and remove posts containing the sensitive information, the process can be fairly long, and not always efficient. By the time it is complete, the information may well have been in the public domain so long — and been exposed to many people — that it no longer qualifies as a trade secret.[3]

If, on the other hand, the platform refuses to cooperate, it is tempting to immediately turn to litigation. While that approach has merit, it should be adopted only after careful consideration. Indeed, a lawsuit could give the disclosed material far more publicity than it would otherwise have received — a counterproductive development. Conversely, however, litigation may be necessary to demonstrate that the employer is unafraid to take action to protect its IP, in that case and later ones.

Copyrights

Social media abuses can also lead to copyright violations, though those are generally easier to remedy than violations involving patents or trade secrets.

A copyright violation may occur, for example, when an employee publishes on Facebook, Twitter or Pinterest internal design documents to show off her latest projects. If the employee does not immediately remove the material upon request, it is imperative to trigger the website's Digital Millennium Copyright Act procedure. This generally involves sending the site a DMCA takedown notice, which should prompt the site to remove the content at issue. But the user at issue can file a counter-notice if he or she believes that the content was wrongly taken down, at which time the copyright holder may trigger litigation after 14 days if he wishes to pursue his claim.

As is the case with trade secrets, the copyright holder is working against the clock. The more time the protected material spends on display on the social media platform, the more likely it is to be widely disseminated. And once the material starts spreading to multiple users and locations, the process of curtailing the infringement can become exponentially more difficult.

What Can Employers Do to Protect Themselves?

Employers should implement social media policies that explicitly encompass intellectual property concerns. They should also monitor the social media activity of their employees, and aggressively enforce their IP rights whenever necessary.

Educating

The vast majority of employee social media abuses impacting IP rights are likely to be caused by ignorance of the issues, rather than malice. So the first step is to make sure that employee manuals and training courses highlight the dangers involved in mixing potential corporate IP and social media. Illustrations of the damage that an unintentional social media misstep can cause may be necessary to drive home the point that this online pastime can have a significant impact on the corporate bottom line, and indirectly, on the employee's continued employment.

Monitoring

To the extent possible, employers should monitor postings on social networks. Many already do so to keep track of defamatory material. Extending the review to encompass intellectual property violations should generally require little, if any, additional resources. But those monitoring efforts will have to remain fluid, for at least two reasons.

First, the social media landscape changes rapidly. The hot new social media arena one month may be a ghost town the next (see, e.g., Myspace.com). Employers will therefore have to remain informed of the latest developments in the social media field for their monitoring efforts to remain properly targeted.

Second, legislative efforts are under way to curtail employers' ability to fully monitor their employees' social media activity. By way of example, the Password Protection Act of 2012 was filed with the House and Senate on May 9, 2012. The act aims to prevent employers from requesting that job applicants share information from their personal social networking accounts. If that act is voted into law, the scope of available monitoring may change drastically.

Enforcing

Employers should be aware of the procedures to follow if and when their IP is threatened by social media behavior. In general, this means being familiar with the takedown provisions of Facebook, Twitter, Pinterest and others. In the case of employers likely to need to enforce their IP on a regular basis, it also means developing a standing relationship with both the relevant platforms and specialized outside counsel to ensure that the material at issue is taken down promptly and efficiently. When the time comes, employers must be prepared to act swiftly in order to halt the dissemination of harmful information, either directly, or through litigation counsel.

--By Ben Quarmby, MoloLamken LLP

Ben Quarmby is a partner in MoloLamken's New York office.

[1] 35 U.S.C. § 102(b).

[2] See MPEP § 2128; see also In re Wyer, 655 F.2d 221, 227 (C.C.P.A. 1981).

[3] Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("Information that is public knowledge or that is generally known in an industry cannot be a trade secret. If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished.").