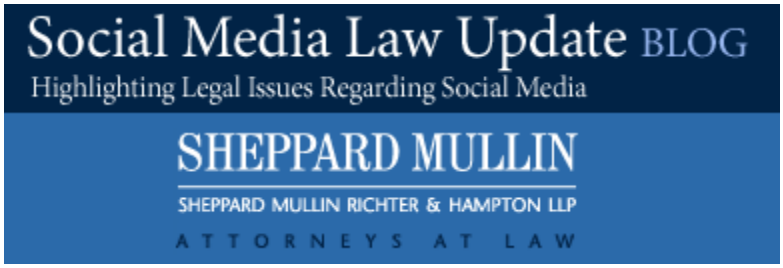

Social Media Law Update

April 6, 2011 by Sheppard Mullin

Protecting Trade Secrets In A Post-WikiLeaks World

By Michelle Sherman

It is not enough in a post-WikiLeaks world to hope that an admonition not to disclose sensitive company information in a social media policy will be enough. If company trade secrets are posted on the Internet they cannot be taken back, and if newsworthy, they will go viral. A perfect example of this is the prototype 4G iPhone that was mistakenly left in a Redwood City bar by an Apple software engineer celebrating his birthday. The iPhone ended up a few days later with Gizmodo, a tech website, that dismantled the smart phone, and shared its features in a blog article that quickly ended up with over 13 million views. In the case of WikiLeaks, it is reported that the 100,000s of pages of highly sensitive government documents were copied onto a Lady Gaga CD and leaked with disastrous results and world changing ramifications.

The story of the Apple iPhone and WikiLeaks highlight two different ends of the spectrum of confidential information being disclosed. First, there is the case of the accidental, unintentional disclosure. Second, there is the intentional taking of company trade secrets.

1. **Identify What The Business Considers To Be Trade Secrets Using The Broadest Available Definition, And Communicate With Specificity To Employees.**.

In the first case, a well drafted and communicated social media policy can reduce the risk of these disclosures. By well drafted, the policy should ideally identify the categories of information the company considers to be a trade secret. Speaking in generalities is not enough. The company should use the broadest definition of trade secrets, which can found in a criminal statute, the Economic Espionage Act ("EEA"), 18 U.S.C. § 1831 *et seq.*, to identify and list its trade secrets. Congress enacted the EEA in recognition of the importance of protecting intellectual property and trade secrets and to address the growing problem of the theft of trade secrets.

The EEA defines trade secrets as all types of information, however stored or maintained, which the owner has taken reasonable measures to keep secret and which have independent economic value. 18 U.S.C. § 1839. This definition is broader than other definitions of "trade secrets,"

including the Uniform Trade Secrets Act which has been adopted by many states.

Using the definition from the EEA, a business should clearly communicate in its confidentiality agreements with employees what the business means by do not disclose confidential, proprietary information. Because the different departments of the business - sales, manufacturing, finance, R&D - will be working with different kinds of proprietary information, the employee training should be done on a department by department basis so the trade secrets can be identified, and the ways in which they should be safeguarded can be discussed. This employee training should also include a discussion of the risks of social media and the Internet with respect to compromising the business' trade secrets.

The business should also assume that a competitor, who is thinking of hiring the employee, will ask the employee for a copy of any confidentiality agreement that may restrict what the employee can bring with him. The confidentiality agreement should clearly list the categories of trade secrets without disclosing the trade secret information itself. It is also worth including in the agreement that the business treats protection of its trade secrets as the highest priority, and that the company will pursue all civil and criminal (*e.g.* the EEA) legal remedies against the employee or any third party who induces or enables the disclosure of trade secrets. Let your competitors know that your business will not take the theft of its confidential and proprietary information lightly.

Sound draconian? Think again about WikiLeaks, and how the pages were picked up by the New York Times and other news organizations, and circulated over the Internet. Even if Bradley Manning, the computer operator in Iraq, who is charged with burning the classified files onto his Lady Gaga CD, had a change of heart and tried to get them back from Julian Assange, it would be too late. Daniel Ellsberg, who leaked the top secret report casting doubt on the Vietnam War in 1971 (Pentagon Papers), which he had through his job as an analyst at RAND Corporation, reportedly said that if he had it to do again today, he "would have gotten a scanner and put them on the Internet" and would not have waited for the press to analyze them before the Pentagon Papers were published.

2. **Know More About The Employees Who Will Have Access To Company Trade Secrets - Do Lawful Background Checks.**

Businesses may want to do background checks before an employee has access to trade secrets as part of their job responsibilities. Any background check should be done with the employee's written consent and in accordance with applicable laws including the Fair Credit Reporting Act, and, in California, the California Investigative Consumer Reporting Agencies Act. If there are red flags, and you will know them when you see them, then the business may want to think again about having the employee in a position where he has access to company trade secrets.

3. **Monitor Internet Mentions Of The Company And Quickly Demand The Removal Of Any Trade Secrets Posted On It.**

A business should monitor how it is being discussed on the Internet through one of several services (*e.g.* Google Alerts). If the business appears in the context of the disclosure of a trade secret, the business needs to act immediately to send a written demand letter to the website,

Internet service provider, or social networking site to remove the trade secret information immediately. If the demand letter clearly sets forth that the intellectual property rights of the business are being violated, most Internet sites will comply with the request and remove the material. The Internet service provider does not have a "safe harbor" from copyright infringement and intellectual property claims, and, therefore, needs to respond appropriately to requests to remove the content at issue. For example, YouTube's Terms of Service provide:

> "YouTube does not permit copyright infringing activities and infringement of intellectual property rights on the Service, and YouTube will remove all Content if properly notified that such Content infringes on another's intellectual property rights. YouTube reserves the right to remove Content without prior notice."

Section 230 of the Communications Decency Act makes it clear that immunity does not extend to any Federal criminal statute, or to any intellectual property law. 47 U.S.C. § 230(e). Consequently, it is unlikely that immunity extends to the disclosure of trade secrets since the EEA provides criminal penalties for the intentional disclosure of trade secrets (18 USC § 1832).

These recommendations serve two purposes. First, to reduce the risk of trade secrets being disclosed and shared all over the Internet. Second, to maintain the trade secret status of the company's information by demonstrating that the company is taking measures to keep it secret.

For further information, please contact Michelle Sherman at (213) 617-5405. (Follow me on Twitter!)