McAfee & Taft

TIP SHEET™

an informational newsletter on intellectual property matters

MARCH 2013

IN THIS ISSUE

Is your secret safe with me?

Trade secrets and the federal Freedom of Information Act

BY RACHEL BLUE
rachel.blue@mcafeetaft.com

Most states have adopted some version of the Uniform Trade Secrets Act, which is designed to prevent the disclosure of trade secrets. FOIA, or the Freedom of Information Act, allows individuals to access records collected by federal governmental agencies. USTA laws prevent the disclosure of information while FOIA promotes it. There are legitimate public policies behind both. (Some states have similar laws but focus here is on the federal level). We want to allow companies to safeguard confidential information they have developed in order to protect their competitive positions and encourage continued development of opportunities, but we also want some degree of transparency, so that, for instance, we can find out certain information that might be relevant to health and safety or environmental issues. What happens when those worlds collide?

Let's say that you run a manufacturing plant and have developed some trade secrets surrounding your processes. However, that plant is subject to regulation by the Environmental Protection Agency, and it's inspected. In the course of the inspection, the EPA representative requires that you provide information on a part of the process that you consider to be a trade secret. If you comply with the EPA demand and the information winds up in their reports or records (which may immediately or at some time in the future be subject to the Freedom of Information Act), can your competitor get the information by filing a FOIA request? Possibly. What if you refuse to turn the information over to the EPA, or what if it is another agency involved? Depending on the regulatory body you're dealing with, they may have the power to shut you down. In regulated industries, the landscape is typically that participation subjects you to compliance with certain rules and regulations. So it may be that, in this example, the EPA could take adverse action, possibly even close your plant.

FOIA requires that certain types of government records be published in the *Federal Register*. Other records can be made available for public inspection and copying, or are subject to being made available to the public in response to requests made in writing.

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

FOIA is a broad statute that covers many types of information, but not everything is subject to disclosure. Typically, Exemption 4 of the FOIA exempts from public disclosure two types of information: (1) trade secrets; and (2) information that is (a) commercial or financial, and (b) obtained from a person, and (c) privileged or confidential.

Congress intended this exemption to protect the interests of both the government and those who submit information. Its existence encourages submitters to voluntarily furnish useful and reliable commercial or financial information to the government without fear that they will suffer a competitive disadvantage from disclosure. With regard to the two categories of information, "commercial or financial" information is pretty easily understood. Although the precise definition can vary, trade secrets are generally defined as information that is not generally known or reasonably ascertainable, by which a business can obtain an economic advantage.

It's not difficult to see if a document is commercial or financial in nature, so the main issue is usually whether the information is privileged or confidential. This has come to be known as the "substantial competitive harm" test, and it has two prongs. Will the disclosure of the information:

1) Impair the government's ability to obtain necessary information in the future, or

2) Cause substantial harm to the competitive position of the person from whom the information was obtained?

If the answer to either is yes, the information is confidential and is exempt from disclosure through a FOIA request. The challenge is that the trade secret owner or the submitter is not the one who decides whether or not to release the information pursuant to a FOIA request; rather, the agency that collected the information decides if it should be exempt or not. So, you have a person working for a government agency who is unlikely to be unfamiliar with the development of the information, its marketplace worth, or the protective measures that surround it making the decision about whether or not it's a trade secret. Not great, right? Moreover, under FOIA, agencies must prove that any information they withhold from disclosure was properly withheld because it was subject to a FOIA exemption. The result is that agencies have no real incentive to withhold information unless it's ***absolutely clear*** that the information is really confidential. In other words, close calls are likely to be disclosed.

Is there anything at all you can do to keep information safe from competitors if you're required to submit it to a regulatory agency? First, as discussed further below, when confidential business information is disclosed, you should define it as such to the agency and request in writing that you be advised prior to any disclosure of the information under FOIA or otherwise. Second, there is a mechanism to minimize damage if the agency releases the information. If you submit the information and it's disclosed under FOIA, you can file a reverse FOIA administrative procedure action demanding a review of the agency's decision to disclose. Unfortunately, the review action won't put the trade secrets back in the bag, and the process stacks the cards in the agency's favor for the most part, so your chances at any real relief are pretty minimal.

It's better to try to prevent the disclosure to begin with. Of course, the first thing to do with an

CONTINUED ON NEXT PAGE

INTELLECTUAL PROPERTY PRACTICE GROUP

Mike LaBrie, ***Group Leader***
michael.labrie@mcafeetaft.com
(405) 552-2305

Sasha Beling
sasha.beling@mcafeetaft.com
(405) 270-6011

Rachel Blue
rachel.blue@mcafeetaft.com
(918) 574-3007

John Burkhardt
john.burkhardt@mcafeetaft.com
(918) 574-3001

Ryan Cross
ryan.cross@mcafeetaft.com
(405) 270-6026

Bob Dace
bob.dace@mcafeetaft.com
(405) 552-2268

Brad Donnell
brad.donnell@mcafeetaft.com
(405) 552-2308

Cliff Dougherty
cliff.dougherty@mcafeetaft.com
(405) 552-2302

Matt Gibson
matt.gibson@mcafeetaft.com
(405) 552-2348

Bill Hall
bill.hall@mcafeetaft.com
(405) 552-2218

Jessica John Bowman
jessica.johnbowman@mcafeetaft.com
(918) 574-3046

John Kenney
john.kenney@mcafeetaft.com
(405) 552-2244

Mike McClintock
michael.mcclintock@mcafeetaft.com
(405) 552-2213

Jim McMillin
james.mcmillin@mcafeetaft.com
(405) 552-2280

Zach Oubre
zach.oubre@mcafeetaft.com
(405) 270-6023

Andy Peterson
andy.peterson@mcafeetaft.com
(405) 552-2333

McAfee & Taft
ATTORNEYS & COUNSELORS

CONTINUED FROM PREVIOUS PAGE

INTELLECTUAL PROPERTY PRACTICE GROUP (CONT.)

Tony Rahhal
anthony.rahhal@mcafeetaft.com
(405) 552-2306

Reid Robison
reid.robison@mcafeetaft.com
(405) 552-2260

Jay Shanker
jay.shanker@mcafeetaft.com
(405) 552-2385

agency's request for confidential information is to confirm with your regulatory counsel that compliance is required under that particular agency's rules and regulations.

If you do have to submit the information, check with counsel or the agency representative to find out what particular procedures the agency might have to help protect the information from further disclosure, and comply with them. Most agencies do have some type of trade secret substantiation procedure in place. You should assume that if you don't follow the agency's specific procedure, they're likely to disclose your information under FOIA.

If the agency doesn't have well-defined substantiation procedures in place, follow these steps:

1. Create a paper trail with the agency to establish that you consider the information to be a trade secret. Transmittal e-mails or letters that set out your belief that the information is confidential could become part of the record that might either make it easy for the agency to refuse a FOIA request under Exemption 4, or establish that the disclosure was "arbitrary and capricious" if it's the subject of a reverse FOIA action.

2. Properly mark any submissions as confidential… but only if it really is confidential. Mismarking information as confidential when you haven't treated it that way will create credibility issues.

3. Unless the agency requires otherwise, submit the information in a format that is different from the one it's kept in during your ordinary course of business. In one case, the court drew a distinction between the paper information that a competitor received through a FOIA request and the same information (though in electronic format and thus more readily accessible) that the competitor stole from its rival.

4. Document, with your submission, who has access to it, what measures you typically take to keep it confidential in the ordinary course of business, and any warnings that typically accompany the information on those occasions where it must be disclosed. ■

Monitoring employees' use of company trademarks in social media

BY JESSICA JOHN BOWMAN
jessica.johnbowman@mcafeetaft.com

If you're an employer, chances are good that you employ some of the 1.06 billion individuals who regularly use Facebook®, as well as some of the millions who regularly post to other popular social media websites. And, whether you realize it or not, those employees may be using those social media outlets to identify with your company, and your company's trademarks.

When an employee uses a company's trademarks in a social media platform, it creates a host of concerns for the employer. For example, an employee's use of a mark may suggest a connection between the employer's mark and the employee's comments and other posts. Or, in more serious cases, an employee's improper use of a mark could cause serious damage to the strength, reputation and goodwill associated with the mark.

McAfee & Taft's Intellectual Property Practice Group represents and advises clients of all sizes, from individual clients and small companies to Fortune 500 corporations. Our clients have diverse intellectual property needs and concerns, and we work closely with them to identify and address each and every issue.

AREAS OF EXPERTISE

Advertising Law
Copyrights
Entertainment Law
Intellectual Property Litigation
Internet Law
Licensing
Patents
Software and Computer Law
Trade Secrets
Trademarks

CONTINUED FROM PREVIOUS PAGE

So what can an employer do to protect its trademarks? Quite a bit. Although it's impossible to monitor each and every social media website, the implementation of a social media policy that includes at least the following will go a long way in protecting your trademarks, and your company's reputation.

- The first and best way to defend your trademarks is through an employee training program. All employees should receive training on the proper and improper use of company trademarks. Provide a list of trademarks owned by the company and inform each employee that the trademarks belong to the company and should never be used without permission.

- Next, monitor your employees' use of social media websites on a consistent and regular basis. Inform your employees that you intend to monitor their use of social media websites and instruct any employee who makes unauthorized use of a company trademark to remove the mark immediately.

- Take advantage of protective measures offered by the social media providers. If an employee refuses to take down a post using a protected mark, send a request to the social media provider advising them that the offending post makes improper use of your company's property. You may also want to request that the provider remove any "community" or "unofficial" pages that have the potential to damage a protected mark.

- Finally, in many cases, the best defense will be a good offense. By establishing company accounts on key social media websites, and using them regularly, you can ensure that the majority of users who see your mark will see it in the manner and context you intended. Limit the number of employees authorized to make posts to this account and ensure that those employees receive additional training on the proper and improper use of trademarks. Consider providing a number of approved, appropriately noticed images for use in connection with those accounts. Remember, anything you post to your company's account can be liked, shared and re-tweeted countless times, so properly noticing your mark will help ensure continued protection of your mark when a post or image is re-broadcast by someone else.

Of course, your social media policy should take into account a number of individualized factors, such as the size of your company, the number of employees, and the ease with which your company can police the ever-expanding number of social media websites. But the steps listed above will form the building blocks of a policy that will help prevent the damaging use of protected marks, promote the proper use of those marks, and minimize the damage resulting from an employee's inappropriate use. ■

McAfee & Taft
ATTORNEYS & COUNSELORS

Keys to ensuring the secrecy of trade secrets

BY ZACH OUBRE
zach.oubre@mcafeetaft.com

Three can keep a secret if two are dead. – Benjamin Franklin

In the shrinking world of social media, privacy seems to be an all but forgotten concept. But in the world of business, trade secrets are critical to success. Trade secrets may be generally defined as information of economic value that is not generally known to others or easily ascertainable. Inherent in trade secret status is the protection and maintaining secrecy of proprietary information. So, in an age of Internet viruses, database breaches and tweeting employees, it is paramount that companies catalog and contractually protect their trade secrets, as well as limit trade secret exposure to key employees who are trained to identify and protect corporate secrets from accidental disclosure or theft.

A 2010 study of federal court cases done by the *Gonzaga Law Review* showed that 85% of trade secret cases allege a former employee or business partner as the misappropriator, making internal controls and contractual agreements the easiest (and perhaps the cheapest) safeguard against trade secret loss.

Recent judicial opinions show courts are reluctant to protect companies that fail to protect their secrets with written agreements. For example, the Seventh Circuit recently affirmed summary judgment in favor of a defendant alleged to have misappropriated the trade secrets of its competitor after negotiations between the competing entities for a proposed business venture failed. During venture talks, the plaintiff disclosed proprietary designs to the defendant but failed to have the defendant sign a confidentiality agreement. The appellate court found lack of a written agreement to be a failure to take "reasonable" measures to protect the alleged secrets, which is a requirement of most trade secret laws. Another employer lost its trade secret claim in a California district court case where it alleged a competitor misappropriated trade secrets by hiring the plaintiff's former employee. The district court found in favor of the defendant competitor, relying on the fact that the plaintiff employer failed to have its former employee enter into a confidentiality agreement regarding the alleged trade secrets.

Written agreements regarding corporate social media accounts are also critical. Recent district court cases involving disputes over social media illustrate the need for unambiguous agreements under which the employer owns and controls all social media used to market the business. For example, in a 2012 case out of Colorado, an employer sued a competitor after the competitor hired the plaintiff's former employee who took a MySpace® account with the names and contact information of the plaintiff's customers to the competitor. A written agreement clarifying the ownership, control and content of the corporate social media accounts would have likely avoided lengthy and expensive litigation and prevented the potential disclosure of the plaintiff's trade secrets.

So, although your company can't adhere to Benjamin Franklin's recommended tactic in maintaining secrecy, it isn't impossible to protect against trade secret misappropriation. The key: "secrets" must be kept a secret and businesses must take appropriate action to ensure secrecy. Identifying corporate trade secrets is a recommended first step. Drafting and updating confidentiality agreements and employee polices protecting and securing confidential business information are also recommended to aid in employee and judicial protection of your company's proprietary information. Businesses should also implement and execute social media policies delineating corporate ownership and content over social media accounts to prevent disputes over the company Facebook account and help prevent disclosure of proprietary information. ■

FTC amends Children's Online Privacy Protection Rule

BY SASHA BELING
sasha.beling@mcafeetaft.com

On December 19, 2012, the Federal Trade Commission amended the Children's Online Privacy Protection Rule to be consistent with the requirements of the Children's Online Privacy Protection Act. The amendments to the COPPA Rule will go into effect July 1, 2013. Under COPPA, child-directed website or service operators must first obtain parental consent before collecting personal information from children under 13. The goals of COPPA are to minimize the collection of personal information from children and to create a safer and secure online experience for children.

The amendments to the COPPA Rule address several loopholes that were exploited in the past. The amendments update and streamline current procedures, as well as modify and expand the definitions of key terms such as *operator, personal information*, and *website or online service directed to children.*

In the past, website operators exploited a loophole in COPPA by having third parties collect the personal information, thus avoiding the parental consent requirements. The amendment now applies responsibility of obtaining parental consent to website operators when a third party is performing the collection of the personal information, even if the third party lacks actual knowledge of the child-directed content.

The modified definitions of terms such as *operator* and *website or online service directed to children* will now cover operators of child-directed sites or services that integrate outside services such as plug-ins and add-on service providers. Under the new definitions, the plug-in operators and add-on service providers are deemed to be an *online service directed to children* and must comply with COPPA if they have actual knowledge that personal information is being collected directly from children users of another website or online service directed to children.

The definition of *personal information* is updated to reflect current technology by including geolocation information and persistent identifiers, such as cookies and IP addresses, that can be used to recognize a user over time and across different websites or online services.

Violations of the COPPA Rule can carry a fine of up to $11,000 per violation. If COPPA currently does not apply to you or your business, you should check your current practices to see how the amended COPPA Rule could affect you.

More information relating to COPPA and the COPPA Rule amendments can be found in the Children's Privacy section of the FTC website here: http://www.business.ftc.gov/privacy-and-security.

McAfee & Taft
ATTORNEYS & COUNSELORS

OKLAHOMA CITY
TWO LEADERSHIP SQUARE
TENTH FLOOR
211 N. ROBINSON
OKLAHOMA CITY, OK 73102
405.235.9621

TULSA
1717 S. BOULDER
SUITE 900
TULSA, OK 74119
918.587.0000

www.mcafeetaft.com