McAfee & Taft

TIP SHEET™

an informational newsletter on intellectual property matters NOVEMBER 2012

IN THIS ISSUE

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

Common sense trade secret protection

BY BILL HALL
bill.hall@mcafeetaft.com

Are your trade secrets at risk? ***Yes, every minute of every day.***

Can you minimize the risk? ***Yes, by creating a corporate culture where each employee recognizes the value of trade secrets to corporate health.***

The above sentences were the original sum total of my article. After all, these four sentences, in a nutshell, identify the problem and provide a preventive law solution. My editor advised me to provide more details. She's a hard task master. So to keep the peace, I offer the following for your consideration.

When I give presentations at intellectual property seminars, I lead with a section on trade secrets. Likewise, when asked to review a client's IP management, my initial inquiries concern management of trade secrets. Why? Because trade secrets are the least understood, yet most vulnerable, component of intellectual property. As a result, many companies fail to adequately protect their valuable trade secrets.

To understand the vulnerability of trade secrets, one need only consider the definition of a trade secret.

The **Economic Espionage Act** and the **Uniform Trade Secret Act** provide long legal definitions of the term "trade secret." However, for our purposes, I prefer the following definition:

A "trade secret" can be any technical, scientific, or business data **not generally known to the public**. The trade secret must provide an economic value to the owner and **must be protected by reasonable efforts to secure the trade secret**.

The vulnerability of trade secrets derives from the bolded portion of the definition. Trade secret owners must treat the information as a trade secret. Thus, a trade secret owner must be able to demonstrate reasonable due diligence to maintain the confidentiality of the trade secret.

Before discussing steps suitable to demonstrate the requisite due diligence, let's discuss how others failed to exercise due diligence. One of the most common examples concerns the improper handling of customer lists. Customer lists frequently exist in hard copy and electronic format. In one instance, a court concluded that the customer provided economic value to the business owner. However, because the owner did not secure the customer lists in locked filing cabinets, the customer lists did not carry appropriate markings of confidentiality, and the

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

INTELLECTUAL PROPERTY PRACTICE GROUP (CONT.)

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

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

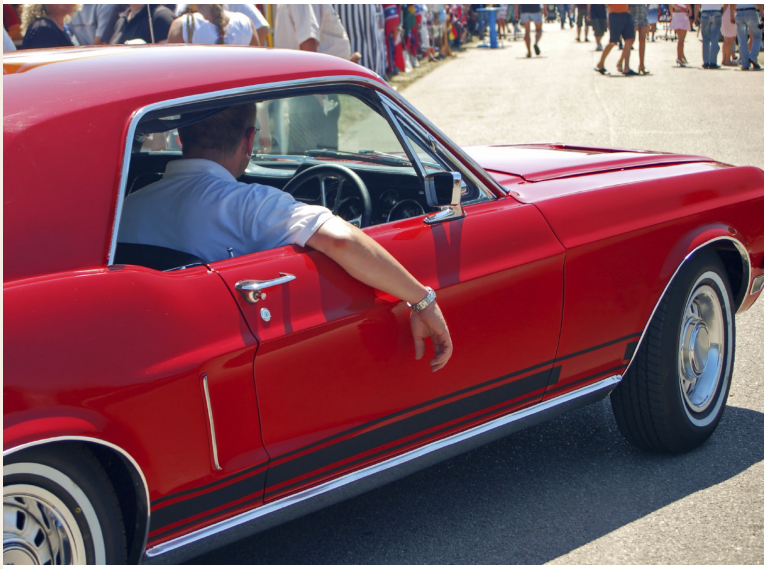
employees were not trained to treat the customer lists as confidential, the court refused to grant trade secret status to the customer lists.

Lack of employee training is the biggest obstacle to creating a culture where each employee values trade secrets. Employee training needs to address two major issues: the handling of trade secrets and the identification of company trade secrets. Before the employees are trained on how to safeguard trade secrets, they need a mechanism to identify corporate trade secrets.

I recall one instance when a client called to complain about some engineers who had published a trade secret in a peer review article. Even though the engineers did not follow proper protocols for publishing a paper, they did not intentionally publish the trade secret. They simply didn't know their paper inadvertently included important trade secret information. Knowing the corporate history, I explained to my client that the corporate culture did not provide an adequate basis for identifying technology that constituted trade secret information. In an engineering environment, engineers tend to believe that everything is obvious and well known to all in their field. I proposed two tasks to remedy the problem: (1) top-down reminders to all employees of the company's publication criteria; and, (2) a comprehensive review of the corporate technology.

I further recommended that the review establish levels of confidential information. For example, levels assigned to information might be: (a) public domain; (b) confidential; (c) sensitive confidential; and, (d) critical confidential. By establishing levels of confidential information, the company would be able to easily identify those employees having access to each level of confidential information, thereby establishing the necessary due diligence in safeguarding the confidential information. Employees should only have access to trade secrets on a "need-to-know" basis. The review required six months to complete; however, upon completion the client had a firm foundation for protecting its critical trade secret information.

Further, the review emphasized the importance of the trade secret technology to the entire company. As a result, the corporate culture toward trade secret information changed significantly. With the change in corporate culture, this client would not likely face the problem encountered by the Ford Motor Company in 1999.



In 1999 Ford was encountering difficulties in protecting its trade secrets. Someone in house was mailing internal documents to a small web-based journalist, Robert Lane. Mr. Lane, a Ford enthusiast and an employee at a PEP BOYS® store, ran the website blueovalnews.com. Through a contact with a local car club, Mr. Lane became aware of a Ford technical meeting being held at a nearby Holiday Inn. Putting on his journalist hat, Mr. Lane attended this confidential meeting **unchallenged**. He subsequently published the agenda from the meeting on his webpage. Ford naturally brought suit seeking an injunction against publishing the material from the meeting and other material provided to Mr. Lane. "Injunction denied," said the court. Ford obviously had an internal problem; however, beyond the improperly disclosed documents one has to question the wisdom of holding a technical

McAfee & Taft
ATTORNEYS & COUNSELORS

CONTINUED ON NEXT PAGE

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

meeting at a Holiday Inn. The meeting clearly lacked any security as Mr. Lane was able to walk in unchallenged, obtain a copy of the agenda, and leave with two coffee mugs and four posters. By the way, at the time of the meeting, Mr. Lane owned two F-150's and four Mustangs, including a 1969 model that he drove to the meeting.

I use this story during seminars and have been known to have a "stranger" drop in just to see if anyone in the seminar will challenge an unknown "guest." Usually, everyone in the audience is appalled when I throw the stranger out of the meeting … that is, until they hear the Ford story.

One client took this scenario to heart and decided to change the corporate culture using a game. Employees were divided into teams. The goal: steal or otherwise gain access to confidential information through the other teams. For example, if an employee left a computer workstation unattended and not password protected, an opposing team that accessed that station would be awarded points. More points were awarded based on the level of access gained. If a laptop was not secured to the desk, bonus points were gained by absconding with the laptop. By the end of the three-month game, protection of trade secret information was a cultural trait.

The benefits of culturally protecting trade secrets will extend beyond the office walls. As employees gain awareness, they will be less likely to accidentally reveal critical trade secrets when attending conferences and conventions, flying on airplanes, etc. Conferences are prime risk areas. Part of the employee training should include awareness factors. For example:

1. Are you familiar with everyone in the audience?
2. Does the audience have a need to know the information (or are you bragging)?
3. Where are you? Is the audience constantly changing?
4. Will the disclosure lead to or include corporate trade secrets?

Finally, a word on contracts (and another story): confidentiality agreements are dangerous. Boilerplate confidentiality agreements are *really* dangerous.

Confidentially agreements are necessary tools for many research companies. However, please be aware that confidentiality agreements have a narrow purpose. Many years ago as a new attorney, I received a request from a client for a confidentiality agreement that would allow them to assess a contractor's capabilities. Six months later, I asked the client how the review went, only to learn that they had engaged the contractor three months prior. When I asked who prepared the services agreement, the client informed me they were using the one I had provided. For the last 20 years, I consistently remind each and every person requesting a confidentiality agreement that these agreements are ONLY for the exchange of INFORMATION. If money or services will be changing hands, they need a different agreement.

In summary, to establish a corporate culture with a focus on protecting trade secrets, companies should identify and classify their trade secret data, establish access to the trade secrets only on a need-to-know basis, secure the data in locked cabinets and secure electronic systems, ensure that all employee agreements contain an obligation to safeguard corporate confidential information, escort all visitors to corporate facilities, and conduct employee exit interviews.

It's 1:30 in the morning. ***Do you know who has access to your trade secrets?*** ■

McAfee & Taft
ATTORNEYS & COUNSELORS

Canada's Anti-Spam Legislation to impact electronic marketing and communications

BY SASHA BELING
sasha.beling@mcafeetaft.com

Until recently, Canada was the only G8 country without specific anti-spam legislation. Canada's new anti-spam legislation Bill C-28, commonly referred to as **Canada's Anti-Spam Legislation (CASL)**, is set to go into effect sometime in 2013. The CASL will significantly impact businesses' electronic marketing and communications practices.

Unlike Canada, the United States already has laws in place that address unsolicited commercial messages via email and telephone:

- **Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)**
- **Telephone Consumer Protection Act (TCPA)**

Currently pending before Congress is H.R. 6377, the Mobile Device Protection Act (MDPA), which requires prior consent from a user prior to the time when monitoring software installed on their mobile device first begins collecting and transmitting information.

In the U.S., CAN-SPAM establishes requirements regarding unsolicited commercial electronic communications. In Canada, CASL applies broadly to all communications either sent by Canadian individuals or companies, or to Canadian recipients, or messages simply routed through Canadian servers. In general, CASL has more stringent requirements for compliance than CAN-SPAM. For example, CASL requires documented prior consent (opt-in) before sending commercial messages, whereas CAN-SPAM does not have an opt-in requirement. In addition, CASL is technology neutral, meaning that it applies to all forms of electronic communications, including emails, texts, images, voice or sound, or even technologies not yet developed. In addition to more stringent requirements, CASL also imposes more severe penalties for noncompliance. In contrast to CAN-SPAM's $16,000 penalty per violation, CASL could impose penalties of up to $1 million per violation for individuals and up to $10 million per violation for businesses.

The CASL also addresses privacy issues, specifically requiring that users give consent to the installation of programs and are informed that a program has monitoring capabilities before that program's installation.

The CASL is enforced by three organizations: the Competition Bureau, the **Canadian Radio-television and Telecommunications Commission (CRTC)**, and the Office of the Privacy Commissioner. The CRTC is encouraging businesses to begin preparing for CASL's enactment and has recently released informational bulletins to help businesses better understand the legislation and facilitate compliance with CASL.

For an illustrative example, the table on the following page shows how the CASL compares with existing U.S. laws, CAN-SPAM and TCPA, and proposed H.R. 6377 MDPA.

Businesses should begin preparing for the enactment of CASL by obtaining documented consent of future communications recipients and establishing communication practices in compliance with CASL. If outside marketing companies are used, take steps to ensure the outside marketing company is familiar with, and in compliance with, the CASL. While these options are not guaranteed to prevent all violations, having such procedures in place can reduce the potential for problems resulting in added costs. ■

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

COMPARISON OF CASL WITH EXISTING U.S. LAWS

	Canada	United States		
	CASL **C-28** **Expected enforcement in 2013**	**CAN-SPAM** **15 U.S.C. §7701**	**TCPA** **47 U.S.C. §227**	**MDPA** **H.R. 6377** (pending legislation)
Protection from	Unsolicited commercial electronic messages; installation of computer programs without express consent	Unsolicited commercial electronic mail via the Internet	Telephone solicitations and use of automated telephone equipment	Monitoring software on a consumer's device and collection of information
Communications covered	Electronic messages sent by any means of telecommunication, including text, sound, voice, or image (email, instant messaging, social media messages, text etc.)	Emails, including social media messages	Automatic dialing, artificial or prerecorded voice messages, text messages, and fax machines	Communicating the usage of a mobile device, location of a user, or information collected to another device or system without prior consent
Prior consent required	Yes	No	Yes	Yes – prior to the time when the monitoring software first begins collecting and transmitting information
Provide opt-out	Yes	Yes	Yes	Yes
Extraterritorial	Yes – covers any messages sent, received, or routed through a Canadian device	Yes	Yes – covers calls and faxes originating from outside the U.S.	Not explicitly stated in the current legislation
Penalties	■ Up to $1 million per violation for individuals ■ Up to $10 million per violation for businesses	Up to $16,000 per violation	The higher of ■ Up to $1,500 per violation, or ■ Actual monetary loss	■ Injunction, or ■ The greater of » Actual monetary loss, or » $1,000 per violation, or ■ Both
Grants private right of action	Yes	Yes – only by Internet access service providers	Yes	Yes

Concerns over copyright infringement drive Google to change search algorithms

BY ZACH OUBRE
zach.oubre@mcafeetaft.com

Business on the Internet recently got a lot more interesting.

On Friday, August 10, 2012, Google announced a major change to its search algorithms that would alter the ranking of websites based on the number of copyright infringement removal notices a website receives. So, if your site has a high number of infringement removal notices, Google will rank it lower on its list of search results. Google's announcement **can be found here**.

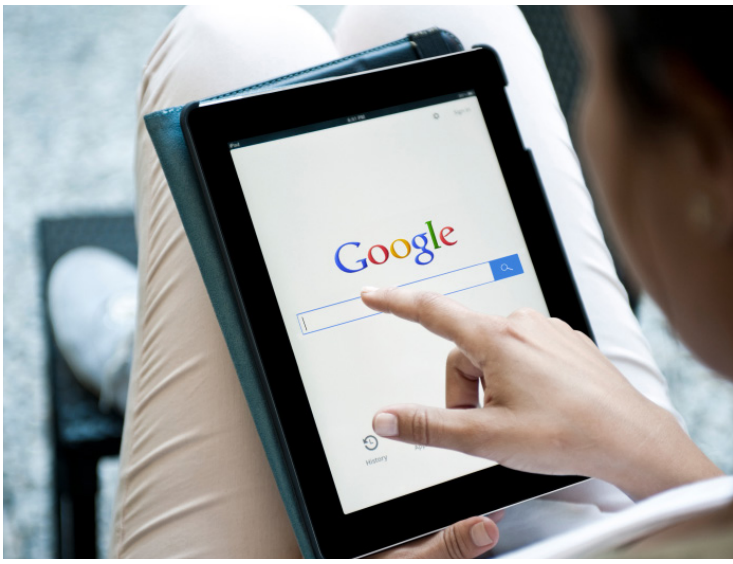
The idea is simple. When most of us search Google, we go to a site listed on the first page of our search results. So, the people and businesses that breach copyright laws in order to add content to a site presumably do so to get more Google "hits" and attract more

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

Internet traffic. Google's algorithm change seeks to eliminate the infringers' incentive by pushing them to the bottom of a Google user's search results.

The change could dramatically affect who sees what on the Internet since Google users have been increasingly more diligent about monitoring copyright use online. According to Google, the search engine now receives more than 1 million removal notices each month and removes 97% of the content specified in take-down requests. Between July and August of this year, Google processed 4.3 million removal notices – which are more than Google received in all of 2009.



There is, however, one interesting catch. Google's new policy alters search algorithms based on "valid copyright takedown notice," which does not require proof of actual copyright infringement. "Valid" only refers to a complaint being validly formatted – i.e., correctly submitted. Google doesn't check whether copyrights have been harmed by a particular site. According to Amit Singhal, Vice President of Google Software Engineering,

> *"Only copyright holders know if something is authorized, and only courts can decide if a copyright has been infringed; Google cannot determine whether a particular webpage does or does not violate copyright law."*

So, the chief concern among Google's critics is the "false positive problem," entities filing take-down notices without a legally valid complaint of infringement. According to the consumer group Public Knowledge, "[s]ites may not know about, or have the ability to easily challenge, notices sent to Google. And Google has set up a system that may be abused by bad faith actors who want to suppress their rivals and competitors."

To protect against false positives, Google provides site owners an opportunity to send a counter-notice to report a false removal notice in order to reinstate the link. This may force companies doing business online to get dramatically less traffic on their sites if they lose their place in the Google search index or, at least cost businesses time and money in making a counter-claim to correct Google's response to a false complaint.

This unfortunate result of Google's policy change is even reiterated on Google's help page, which previously stated: "[t]here's almost nothing a competitor can do to harm your ranking or have your site removed from our index," but has since been changed to say: "Google works hard to prevent other webmasters from being able to harm your ranking or have your site removed from our index."

So, baseless copyright complaints submitted in a valid Google format could be the new tool of competitors or even disgruntled former employees who happen to be Internet savvy. For those businesses that routinely search Google for their content on other people's sites – make sure your website comes up as well. ■

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