YOU AUTO KNOW©

February 2012

Robert A. Poklar, Esq.
Weston Hurd LLP
The Tower at Erieview
1301 East 9th Street
Suite 1900
Cleveland, Ohio 44114-1862
p: 216.687.3243
f: 216.621.8369
rpoklar@westonhurd.com
www.westonhurd.com

SOCIAL MEDIA

Scenario:

As you walk through your dealership, you see several employees on their smartphones, or iPads, checking email, texting and/or tweeting. You don't know whether the activity is for business-related purposes or personal purposes. You are becoming concerned, not only about the lost productivity, but what exactly your employees are saying about the dealership, the business, the product, your customers or other employees. What are the dealership's responsibilities and duties?

First, there are numerous Internet-based communication channels, more commonly known as social media. For example, Facebook, MySpace, Twitter, LinkedIn, Flickr, YouTube, Teeton AT, just to name a few. Further, it is the most rapidly growing means of communication in the world. It must be clearly understood that this is a very unsettled area of employment law. However, it is universally agreed that there should be a section in your Employee Handbook specifically dealing with social media communications and their content. As stated, the case law is not developed in this area and the over-reaching attempt at enforcement by an employer can lead to adverse actions by an employee.

Generally, courts have found there is no reasonable expectation of privacy by an employee using a company-owned computer or email system as long as the company has a policy regarding social and electronic media. In fact, there are some cases which state that an employee's personal emails stored on a company computer were not protected since there was not a reasonable expectation of privacy. However, the written policy must be concisely written in order that it does not appear to be an over-reaching attempt to seek personal and confidential information about an employee or to prohibit protected activities. In any litigation, the plaintiff or defense counsel is going to attempt to discover social networking information. This will involve attempting to obtain current and archived materials.

Generally, an attempt to obtain information from the network sites themselves cannot be subpoenaed. There are several Federal Acts such as the Stored Communications Act which prohibit an entity from releasing private information. However, as always, there are ways to get around this prohibition.

There are several cases that have been decided for the employer and/or for the employee regarding postings on social media sites. In some instances, employees have been dismissed for activity that has been posted on their MySpace site for overly criticizing a company's safety standards and insulting customers. However, the employer has to be careful it does not risk obtaining undesired or unwanted information regarding a protected class of employee, based upon race, religion, ADA, or sexual orientation. Although the

rights of both employer and employee are in a state of flux, it must be noted that the use of a company-owned computer can expose the employer to liability if the computer is used for derogatory or harassing remarks directed from one employee or another employee. There is also the danger of viewing pornographic images being discovered by an employee. This could form the basis of a sexual harassment claim.

The question the employer has to ask is whether employees have a reasonable expectation of privacy in their social networking activities. Again, the case law is not developed. An employee could attempt to sue for invasion of privacy or violations of the Stored Communications Act, wrongful termination, violation of the Federal Wire Tap Act, NLRB violations, Genetic Information Non Discrimination Act, Fair Credit Reporting Act, to name a few examples. Further, the employer may run afoul of the Patriot Act when, in some instances, the employer is obligated to provide certain information to the government.

It must be noted that generally, as long as a company has a tightly written policy, an employee does not have a reasonable expectation of privacy while on company business. The policy must specify prohibited activities, specify the right for inspection for cause, must specify that the employee does not have an expectation of privacy concerning the company or its customers and the policy will not interfere with Federally protected rights. Further, there is the issue of when an employee is not physically at work. In this day and age of instant communication, is the employee subject to the policies and procedures of the business if he or she is using company-owned electronic devices or phones after hours? The same question applies if the employee is using his or her own smartphone and/or computer after hours.

A couple of months ago, this author wrote a *You Auto Know*© regarding an employee's use of texting to contact customers during a sale and/or service of a vehicle. Be advised that any such communication is discoverable in a lawsuit and at times communications which, at the time would seem harmless, could prove to be detrimental to the dealership.

The bottom line is you need to review your Employee Handbook and have a written policy regarding electronic media and social networking. If you do not already have such a policy, it is strongly recommended that you contact your legal counsel in order to discuss the benefits of such a policy.

CONTACT INFORMATION
Robert A. Poklar, Esq.
Weston Hurd LLP
The Tower at Erieview
1301 East 9th Street, Suite 1900
Cleveland, Ohio 44114-1862
p: 216.687.3243; f: 216.621.8369
rpoklar@westonhurd.com
www.westonhurd.com

As always, these are highlights of the law and are not to be construed as containing the entire law. This is not to be construed or relied upon as a legal opinion. If you are presented with this problem, contact your legal counsel for advice.