

EMPLOYMENT LAW ALERT

June 2012

Ruskin Moscou Faltischek's Employment Law Capabilities

- Sexual Harassment Prevention
- Discrimination Avoidance
- Restrictive Covenants (non-compete, non-solicitation) and Unfair Competition
- Protection of Trade Secrets, Proprietary Information and Business Opportunities
- Employment At Will, Breach of Contract and Termination for Cause
- Employee Policy Manuals
- Family and Medical Leave
- Wage and Hour Requirements
- Employee vs. Independent Contractor
- Executive Employment Agreements and Severance Packages
- Comprehensive Litigation Services

For further information, please contact these Employment Law Group members:

Jeffrey M. Schlossberg
Chair
(516) 663-6554
jschlossberg@rmfpc.com

Douglas J. Good
(516) 663-6630
dgood@rmfpc.com

Joseph R. Harbeson
(516) 663-6545
jharbeson@rmfpc.com

Kimberly Malerba
(516) 663-6679
kmalerba@rmfpc.com

Do You Have a BYOD Policy? It's Not What You Think. . .

By: Jeffrey M. Schlossberg



What may have once been the "me" generation has now transformed into the "i-generation" (iPhone, iPad, iCloud). As a result, the time has come for employers to consider BYOD - Bring Your Own Device - policies for the workplace. The implications of failing to stay ahead of the i-curve can be significant.

For a variety of reasons, employers have permitted employees to use devices for work that the employees have personally purchased. In some cases, it is a conscious decision by the company to save thousands of dollars by not having to purchase such equipment for its employees. In other cases, no thought whatsoever has gone into the transition of company-purchased equipment to employee-owned devices.

Regardless of the reason, the impact on a company is the same. Here are a few scenarios that can arise:

- 1) How does a company ensure data security? Company owned equipment can be programmed to restrict access as needed. Can you restrict a phone you do not own?
- 2) How do you track time if someone is working on their own iPad? If an employee was working on a company laptop, you could track the time. Can you do so on someone's iPad?
- 3) How does a company handle a workplace harassment investigation where the evidence is contained on an employee's personal iPhone?
- 4) How does a company retrieve work-related information when an employee leaves the company's employ?

With these (and other) issues already affecting important aspects of the business, what is a company to do?

Previous Alerts

[May 2012](#)
[April 2012](#)
[March 2012](#)
[February 2012](#)
[January 2012](#)
[December 2011](#)

Follow us on 

**HAVE A
GREAT SUMMER!
SEE YOU IN
SEPTEMBER!**

Initially, a company has to make an informed decision of whether or not it wants to permit employee-owned devices to be used or if it prefers to limit work-related matters to be conducted on company-owned and distributed equipment.

If a company is going to permit employee-owned devices to be used for work, policies must be implemented. Some of the most important issues that should be addressed in such a BYOD policy are:

- 1) Including a statement that the company owns certain information even if contained on an employee-owned device.
- 2) Indicating that the company can determine which devices may be used.
- 3) Providing a mechanism whereby the company can gain access to information when necessary.
- 4) Requiring employees to provide employers with passwords.
- 5) Identifying whose responsibility it is to repair the employee-owned device.
- 6) Determining how the company will track non-exempt employee work time.
- 7) Addressing what will happen to information upon employment termination.

Of course, these are just a few of the issues that require attention. In future editions of the Alert we expect to provide more insight into the continuing development of BYOD issues and other cutting edge topics affecting the workplace.

Update: Time Again to Tweak Your Social Media Policy

As a result of a third report issued by the National Labor Relations Board's General Counsel addressing social media in the workplace, it is time for a short quiz on social media policies:

1) Can an employer direct employees not to "release confidential company information"?

No. This provision was held unlawful as it could be unreasonably interpreted as prohibiting employees from discussing and disclosing information regarding their own conditions of employment as well as the conditions of employment of other employees; actions protected by the NLRA.

Solution - clarify the policy so it does not preclude sharing of employee salary information.

2) Can a social media policy prohibit "offensive, demeaning, abusive or inappropriate remarks"?

No. This was found unlawful as would preclude a broad spectrum of communications that would include protected criticisms of the employer.

Solution - prohibit comments that are defamatory, vulgar, obscene, threatening.

3) Can you tell employees to "Make sure that any photos, music, video or other content is legally sharable and you have the owner's permission"?

If you've read this far, you probably guessed the answer is "no." You are correct. The policy was found to prevent employees from legally using the employer's logo in protected activity.

Solution - instruct employees that use of logos must be consistent with copyright laws.

~~~~~

If we can be of assistance on these or any other employment law issues, please do not hesitate to contact us.



**Smart Counsel. Straight Talk.**

East Tower, 15th Floor  
1425 RXR Plaza, Uniondale, NY 11556-1425  
516.663.6600  
[www.rmfp.com](http://www.rmfp.com)



Attorney Advertising

**Employment Law Alert** is a publication for distribution without charge to our clients and friends. It is not intended to provide legal advice, which can be given only after consideration of the facts of a specific situation.