

EMPLOYMENT NEWS ALERT

2nd Quarter 2010

Brian E. Curtis, Esq.

∓NETWorkplaceø

The Rise of Social Networking on the Job

A Series on How Employers Should Manage Social Networking Sites in the Workplace

In the first installment of this four-part series to be published over the course of this year, we raised the employerø concern over an employeeø use, and potential abuse, of social networking sites at work and provided options on how employers could work to try to limit the risks inherent in these concerns. See our 1st Quarter ENA published on February 1, 2010.

In this second installment, we will focus on an area of the law that is developing into what may be the most challenging issue to employers in New Jersey and nationwide í the employeeø constitutionally-protected right of privacy when using social networking sites while on the job. As you know, an employeeø privacy is a hot-button topic here in New Jersey, in view of our state Supreme Courtø recent decision in *Stengart v. Loving Care Agency, Inc.*, 2010 N.J. LEXIS 241 (March 30, 2010), finding that an employee who used her companyø computer for personal email had a reasonable expectation of privacy in those emails. We touched on this ∓privacyø issue in our April *NewsFlash*, and, recognizing its growing significance to social network sites, have expanded our information for you here in this series.

The Right of Privacy in Social Networking

As recently reported in April by EPIC ó Electronic Privacy Information Center ó the ∓powers that beø at Facebook have announced significant changes to the privacy settings on its website affecting the ability of its millions of users to protect the information posted on their Facebook pages. GCs and HR professionals, at first look, may say õso what?ö, but to do so would be to put your Companyø interests in jeopardy. Remember, most of the ∓millions of usersø on Facebook are also your employees and many of them are members of multiple social networking sites. Like it or not, many of them surf these sites while at work. When your employeeø privacy protections are reduced, ultimately so is your Companyø ability to protect its confidential proprietary information.

The most pressing concerns of the recent announcement of changes to Facebook usersø privacy settings is that these changes will not only allow for Facebook to more readily integrate with many other web sites, but they will also make it more difficult to limit the disclosure of a Facebook userø personal information. Referred to as "instant personalization", these changes will give Facebook's business partners access to incredible amounts of personal data about Facebookø users, unless these users opt-out of the new feature. Some of the personal data includes details such as a userø friends, their ∓friends of friendsø, their interests, their likes and dislikes, etc., and could conceivably result in the disclosure of personal information about other persons and organizations to whom the user is connected on Facebook. These disclosures can be made without consent! EPIC has also reported that as part of these changes, Facebook has removed an important privacy safeguard which will now allow third parties like Facebookø business partners to maintain an individual userø data *indefinitely*.

From the HR perspective, Facebookø privacy policy changes are alarming. Even Congress has taken notice. US Senator Charles Schumer (D-NY) has reached out to Facebook CEO Mark Zuckerberg to express concern. In fact, EPIC has also reported that Senator Schumer has asked the FTC to set down guidelines for social networking sites.

What Can Your HR Managers Do Right Now?

We previously explored in Issue 1 what options might be available to your Company to address an employee's use of Facebook, LinkedIn, Twitter, and other social networking while on the job, the most important of which is to

Educate your employees! Most simply do not realize that their online activities can cause real security and privacy concerns for the Company. Tell them not to give out personal details online. Tell them how their actions can affect the Company and each of their co-workers in order to give your employees a sense of responsibility for the private information they disclose and for what they post online.

On a final note, though EPIC is an organization which focuses on protecting individual privacy rights and would typically be a source of consternation for business interests, it would be wise for GCs and HR managers across New Jersey to make themselves aware of EPIC's mission in order to know the pulse of this ever-evolving area of the law and its impact on appropriate workplace policies.

We have the tools and the expertise to help your HR departments draft and implement policies that will ensure your Company is protected while at the same time staying competitive in the marketplace and maintaining an efficient and productive workplace. **CALL US NOW! WE CAN HELP!**

If you would like additional information on the topics detailed in this issue, or any prior issues, of [Employment News Alert](#), or otherwise need assistance and advice on any employment matter, please call or email as follows:

Brian E. Curtis, Esq.

(732) 277-8261

becurtis@strykertams.com

The materials and information disclosed in this issue, and all issues, of [Employment News Alert](#) is for informational purposes only. It is not for the purpose of providing legal advice and does not create an attorney-client relationship between the firm of Stryker, Tams & Dill and the reader, or between Brian E. Curtis, Esq. and the reader.

*Revised June 1, 2010
Excerpts reprinted with permission
Employment News Alert © 2004 Brian E. Curtis, Esq.*