BCLP. Client Intelligent

RetailLawBCLP

MONITORING EMPLOYEES' EMAIL AND INTERNET USE RAISES LEGAL CONSIDERATIONS

Mar 03, 2017

Retailers should be aware that federal laws prohibit the interception of another's electronic communications, but these same laws have multiple exceptions that generally allow employers to monitor employees' email and internet use on employer-owned equipment or networks.

As a result, under federal law, when retail employees use an organization's telephone or computer system, monitoring their communications is broadly permissible, though there may be exceptions once the personal nature of a communication is determined. For example, under the National Labor Relations Act, employers cannot electronically spy on certain types of concerted activity by employees about the terms and conditions of employment.

Although monitoring is broadly permitted under federal law, some states, including Connecticut and Delaware, require that employers notify employees that they may be monitored. Even in states that do not require notice, employers often choose to provide notice since employees who know they are being monitored are less likely to misuse corporate systems. It is good practice for a retailer to have employees sign a consent or acknowledgment that monitoring may occur and to inform them that personal calls may not be made from particular telephones.

Employers may also monitor what an employee posts to social media. However, under some state laws employers cannot request that an employee provide his or her username and password to a social-media account in order for the employer to see content that was not published publicly. In 2016, sixteen states introduced or passed legislation prohibiting employers from requesting such information. This would include, for example, posts that were made available only to an employee's friends, or personal network. In addition, some state laws prohibit employers from requiring that their employees accept a friend request that would permit the employer to view friends-only social media posts.

Finally, some states prohibit monitoring of telephone calls on an employer's telephone network without the consent of one or both parties to the communication.

What to consider when crafting employee monitoring policies:

1. Does your organization publish an acceptable use policy?
2. Does the acceptable use policy explain what employees may and may not do over the internet while at work?
3. Does the acceptable use policy explain the disciplinary consequences of violating the policy?
4. Do you have the ability to block or otherwise restrict access to internet sites that are barred under the acceptable use policy?
5. Does your employee handbook make employees aware of monitoring?
6. Does the state in which the employee works require single or dual consent for monitoring telephone conversations, and have your employees consented?
7. If your organization monitors phone calls, do you have a policy to cease monitoring when a call is clearly personal in nature, and do you follow it?
8. Have you considered whether an employee might be able to argue that they have an expectation of privacy to their work emails or to their work phone calls?
9. Are you monitoring emails to or from password-protected personal accounts?
10. Are your employees using their own computer equipment to send emails or view the internet?

For more information, contact the author, David Zetoony, at 303-417-8530/202-508-6030 or david.zetoony@bryancave.com, or any member of the Retail team.

MEET THE TEAM

Merrit M. Jones

San Francisco

merrit.jones@bclplaw.com
+1 415 675 3435