Employment Law Q&A: May I monitor an employee's emails and internet usage?

Ryan Neumeyer, Karina R. Conley | Thursday, April 26, 2018

Q. May I monitor emails that an employee sent on the employee's work computer or review other information accessed on my (the employer's) network?

A. Like many other legal questions, the answer is: "It depends."

Generally, it is permissible for you as an employer to monitor your own computer systems including, but not limited to, employees' work email communications and internet usage.

The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act (ECPA) controls an employer's liability for intercepting emails. Under the ECPA, if an employer has a policy in effect stating that it can monitor its email system, employers may monitor emails sent by employees on their work devices. As such, you should ensure that you have a policy in your handbook or otherwise stating that employee emails and internet usage may be monitored and that employees should have no expectation to privacy in their email communications or computer usage while at work or when using work systems.

It is, however, a more delicate situation when an employee accesses personal emails or social media through their employer's network, which may then allow the employer the ability to access to such information. The Stored Communications Act (SCA), codified at 18 U.S.C. Chapter 121 §§ 2701–2712, governs stored communications, including an employee's search history, emails, passwords and other

information stored on an employer's network. But the SCA prohibits an employer from reviewing private communications stored somewhere other than the employer's system, including personal and secure websites, private social media pages, and personal emails provided by the third party internet or email providers (i.e., Gmail, Yahoo, etc.)

Several cases have dealt with these issues in the past several years:

- In *Holmes v. Petrovich Dev. Co., LLC*, 191 Cal. App.4th 1047 (2011), a California appeals court held that an employee's email communications with her attorney sent over the company server were not protected by California's attorney-client privilege, and the employee had no reasonable expectation to privacy where: (1) the company had previously notified the employee pursuant to a company policy that any communications transmitted through its network may be monitored; and (2) the employee acknowledged receipt of the policy.
- However, in *Stengart v. Loving Care Agency, Inc.* 201 N.J. 300 (2010), a New Jersey court held that an employer's policy did not sufficiently preserve its ability to monitor an employee's personal email account where it did not expressly notify the employee of this possibility.
- In *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 763 (N.D. Ohio 2013), a terminated employee turned in her cell phone without deleting her personal email account. Thereafter, a Verzion employee accessed and read approximately 48,000 of the employee's emails over an 18-month period. The emails contained communications about employee's family, career, financials, health, and other personal matters. In some instances, the Verizon employee opened emails that the former employee had not even opened yet. In a suit filed by the former employee, the employer argued that it had consent because the employee did not delete her password prior to turning in her cell phone. The U.S. District Court for the Northern District of Ohio, however, held that Verizon and its employee did not have authorization to search the terminated employee's personal emails simply because it had a policy that stated that it could monitor all email and internet use. The court also opined that Verizon could potentially be liable under the SCA for the action of its employee opening emails that the former employee had not yet opened.
- In *Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026, (N.D. Cal. 2014), the U.S. District Court for the Northern District of California held that a terminated employee had no claim under SCA or Wiretap Act where through no fault of the former employer, text messages the employee sent and received on his new iPhone appeared on his old company phone, which he had turned in to his former employer without deleting it from his personal Apple account. The employee later deleted the Sunbelt number from his Apple account, but alleged through his counterclaims that Sunbelt had been monitoring his private messages in the meantime. The court ruled that it was not a wiretap violation because Sunbelt did not intentionally intercept any communications. Further, the simple act of reading messages that came up on the devices did not violate the SCA because Sunbelt did not break into the Apple network or the former employee's service provider's network to access the information, which would have been required for a violation.

3 tips for monitoring your employee's computer and internet use

These cases demonstrate the following three tips for employers regarding monitoring employee's computer and internet use:

1. Have a policy notifying employees that their use of the company's systems may be monitored and that employees should not have an expectation of privacy on employer's systems.
2. Make sure employee's acknowledge receipt of such a policy.
3. Do not access password protected sites, such as internet based personal email and social media sites without explicit written approval and authorization from the employee to do so.

Ryan Neumeyer

Team member bio

Karina R. Conley

Team member bio