Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How To Keep An Eye On Workers But Keep Out Of Trouble

By **Bill Donahue**

Law360, New York (March 18, 2013, 3:04 PM ET) -- After the controversy that erupted last week over news that Harvard University was surreptitiously peeking into the work email accounts of its administrators, Law360 asked attorneys how employers can avoid getting into hot water when they need to access an employee's electronic information.

The situation that confronted Harvard could happen anywhere: employees appeared to be releasing confidential emails to the media, and the bosses wanted to investigate. But the backlash, too, was pretty predictable. Digital information is stored and transmitted today in largely the same manner at home and at the office, and it's easy for the feeling of privacy inherent in the former to creep slowly into the latter.

As Harvard's staffers found out, employers don't see it that way. Whether it's to protect intellectual property and trade secrets, heighten data security, respond to allegations against an employee that could create liability for the company, or simply to ensure productivity, organizations feel a need to be able to monitor and access company-owned computers, email accounts and networks.

"An employer does not want to have its hands tied by not being able to review that kind of information when an adverse situation arises," said James P. Walsh Jr., an employment partner at Morgan Lewis & Bockius LLP.

But going about the process the wrong way can cause problems. Though the Harvard situation likely isn't actionable, it was a media headache, and other types of employee tracking can lead to invasion of privacy claims and federal law violations. Here are some tips to more easily — and legally — balance the growing tension between respecting the digital privacy of employees and making sure clients have the ability to get the information they need.

Have it in writing: Nothing is private.

Though some countries have statutory protections for the privacy of employees, the U.S. starts with a fundamentally different baseline — whether the employee should have reasonably expected that their communications or materials were going to stay private.

If an employee can prove that they had a reasonable expectation of privacy, companies that monitor or track information can face claims for common law invasion of privacy, violations of the federal communications privacy laws or, for public employees, violations of the Fourth Amendment.

The best way to make sure workers don't believe they're in private while on work computers or websites is to establish a cleanly drafted, understandable policy that expressly says otherwise, according to Robert Brownstone of Fenwick & West LLP.

"An employer should go very far in a written policy to stake out its rights," Brownstone said, noting that it should explicitly encompass access to all aspects of storage and transmission, on both hardware and the company network. "That way, there is no expectation of privacy. Period. To me, that should be highlighted and the main point of any technology use policy."

Get the policy in front of employees, not buried away.

Equally important, though, is that employees actually have access to the rules so they can understand what they're signing away by working at the company. If an employer has a strong policy but hides it away in a dense manual, employees could possibly claim that they didn't know it existed.

One easy way to counter this preemptively is to require each employee to acknowledge a pop-up screen on their computer when they log on, explaining that any information they create or transmit on company machines or networks isn't private, said Justine Phillips of McKenna Long & Aldridge LLP.

"When employees claim their rights to privacy were violated, they'll say, 'You have a 70-page handbook, am I supposed to read every page of that?'" Phillips said. "It's a lot easier from the other side to just say, 'How about the message you get when you log onto your computer every morning?'"

Other forms of posting and regular reacknowledgments of the written policy by employee signature can also help make sure workers can't feign ignorance about their privacy rights on work email and work computers.

"The best thing an employer can do is chip away, regularly, at the expectation of privacy," Phillips said.

Only create rules that will be consistently enforced.

In addition to having a strong policy in place, courts dealing with workplace technology privacy issues want to see that any intrusive policies were fairly and regularly enforced on all employees, Brownstone said.

For companies that give themselves broad rights to monitor and police employee communications but then rarely or selectively enforce them, they run the risk of the policies being deemed arbitrary, discriminatory or unenforceable.

"If you have this really strict writing but everyone knows you're not following it and have orally told people you're not following it, it's really pretty useless and you're actually worse off for it," Brownstone said.

If a more laid-back employer is afraid of seeming like Big Brother, it's better to write a more tailored technology policy than to simply ignore the one they have, he said.

"They would be better off to couch it differently," Brownstone said. "The compliance gap between writing and what you do is a real problem."

Have a good reason to snoop, and know when to stop.

When the Harvard story broke, the school's administration said it needed to check the emails to prevent further releases of highly confidential information about students. Like Harvard, all employers should have a legitimate business reason to protect when they exercise their right to access employee files, according to Phillips.

"Don't satisfy your curiosity. Curiosity killed the cat," she joked. "Don't try to peek into someone's emails or communications and look into something purely because you're curious about it."

Real concern over the leak of sensitive information, a credible threat of violence or harassment, and any number of other reasons can prompt an investigation, but extending the probe past the reasons you started can be troublesome, Morgan Lewis' Walsh said.

"While an employer may have a legitimate reason at the outset to commence investigation, they do have to be cognizant that the original cause may not justify looking into every nook and cranny," Walsh said.

Know the foul lines.

So, what should an employer be careful of, even with a well-enforced, perfectly drafted technology policy?

Companies should generally steer clear of trying to gain access to password-protected personal email accounts and personal social media websites. Each move, including trying to coerce an employee to hand over a password, carries some risk of violating the federal Stored Communications Act, certain state laws and a common law right to privacy.

Employers also want to be wary of areas of unsettled law, including the monitoring of employee-owned devices, the protections afforded to concerted labor activity over personal social media, and employer access to temporary files left on work computers from personal email accounts.

Indeed, the law for monitoring and tracking employees electronic information is changing with the technology that stores and transmits it, but employers should still stick to common sense when setting policy and conducting investigations into its workforce, Walsh said.

"There are still basic tenets," the Morgan Lewis attorney said. "Clearly communicate your policies with your employees. Be reasonable. Don't overextend."

--Editing by John Quinn and Katherine Rautenberg.

All Content © 2003-2013, Portfolio Media, Inc.