JOURNAL REPORTS: LEADERSHIP

Should Companies Monitor Their Employees' Social Media?

May 11, 2014 5:05 p.m. ET

John Weber

Social networks offer a window into how people live their lives.

But should employers be looking into that window?

Journal Report

Insights from **The Experts**

Read more at **WSJ.com/LeadershipReport**

More in Big Issues: Technology

Has Twitter Peaked?

Can Massive Open Online Courses Replace Traditional Classroom-Based Education?

Is Now the Time to Buy a 4K TV Set?

Should Broadband Internet Access Be Regulated as a Public Utility?

It's becoming an increasingly important question. The number of people fired over social-media posts is rising, and many employers look closely at a job candidate's online presence before making a decision.

For an idea of how prevalent those practices have become, consider a 2013 survey from CareerBuilder, which helps corporations target and attract workers. According to the survey, 39% of employers dig into candidates on social sites, while 43% said they had found something that made them deep-six a candidate—such as posting inappropriate

Are Consumers Better Off Putting Everything In the Cloud?

WSJ Radio

Nancy Flynn, Executive Director of The ePolicy Institute, and Lewis Maltby, President of the National Workrights Institute, join WSJ's Mathew Passy to debate whether employers should be monitoring social media accounts

00:00 | 35:39

photos or information, or bad-mouthing a former boss.

On the flip side, 19% said they found information that sold them on a candidate, such as communication skills or a professional image.

Some advocates say employers should be doing even more than they are now to monitor social media—they should keep an eye on workers' tweets and updates around the clock. Privacy proponents and worker advocates say it's unnecessary. Most of what people post has nothing to do with work, they say, and shouldn't be monitored unless there's a clear reason to suspect wrongdoing.

Arguing the case for strong monitoring by employers is Nancy Flynn, the founder and executive director of the ePolicy Institute. Lewis Maltby, president of the National Workrights Institute, argues it's counterproductive and unnecessary.

Nancy Flynn *ePolicy Institute*

Yes: Keeping an Eye on Employees Helps Companies Protect Themselves

By Nancy Flynn

Management has a right and responsibility to monitor how employees are using social media at all times. If companies don't pay attention, they may end up facing any number of serious problems.

It's all too easy for disgruntled or tone-deaf employees to go onto social media and criticize customers, harass subordinates and otherwise misbehave. Sometimes that can bring workplace tensions and complaints, sometimes it can damage a company's reputation in the marketplace, and sometimes it can lead all the way to lawsuits or regulatory action. (And, like email, social-networking records can be subpoenaed and used as evidence.)

Not Harmless

Some critics say that this is an exaggeration—that most of what people post on social networks is private and perfectly harmless, and has no bearing on their work. These critics also argue that companies often do these searches out of prudery or as ideological witch hunts.

The Company Will Be Watching You

A 2012 report by Gartner Inc. on the use of digital surveillance in the workplace forecast that by 2015, 60% of corporations will have formal programs for monitoring employee activity on social media, up from less than 10% in 2012. Among the report's suggestions on how to stay within legal and ethical bounds, it recommends companies establish formal monitoring and surveillance policies that include the following:

- A statement of objectives
- Assignment of responsibility and accountability for surveillance activities
- Detailed descriptions of surveillance activities supported
- Assignment of security classifications to the data collected
- Statement of requirement for oversight and auditing of the program
- Reference to a defined author-
- References to enabling and limiting regulations, legislation and policies
- Contact point for complaints about unauthorized or overly intrusive surveillance

Source: Gartner Inc. ization and approval process The Wall Street Journal

In fact, a significant chunk of employees acknowledge posting information that they shouldn't. Consider the results of the "2009 Electronic Business Communication Policies and Procedures Survey" from American Management Association and my organization, the ePolicy Institute. In the survey, 14% of employees admitted to emailing confidential company information to third parties; 6% sent customers' credit-card data and Social Security numbers; and another 6% transmitted patients' electronic protected health information.

Some of the examples I've come across show just how serious those types of employee missteps can be. Hospital employees have come under criticism or have been fired for discussing patients on Facebook—which violated not only hospital policy but also the federal Health Insurance Portability and Accountability Act. A city official accidentally put some city employees' private information on a public website, then linked to the site from Twitter, which exposed the workers to potential identity theft and left the city vulnerable to regulatory action, negative publicity and lawsuits.

In many other cases, employees have griped about their company online, or posted joke videos that put it in a bad light and took a considerable amount of damage control to undo.

Strict monitoring allows employers to spot potential problems early, get the information offline as quickly as possible and discipline the employees involved. Along with keeping an eye on what happens on internal computer networks and public social media, companies should ask for access to employees' Facebook accounts and other private social media.

Looking at Candidates

Beyond that, some critics say it's unfair for companies to use social media as a factor in screening potential hires. It could lead to discrimination, they say, and it may screen out otherwise strong candidates who have done some things the company doesn't like but aren't related to work.

Of course, it is important that companies don't use social media to discriminate based on things like age, ethnic background or religious beliefs. Employers should make sure that they have legitimate business reasons for rejecting applicants.

But, contrary to what critics argue, when companies conduct social-media checks on prospective hires, they typically *are* searching for legitimate evidence to withdraw or rethink a job offer, such as references to drugs or other illegal activities, comments that are discriminatory or harassing, or signs that an applicant has been dishonest about work history or abilities.

They aren't just snooping around for, say, embarrassing photos that offend HR's sensibilities. To suggest that HR professionals monitor social media to root out private activity that they personally disapprove of is to make light of real dangers and potentially costly and protracted legal and regulatory risks.

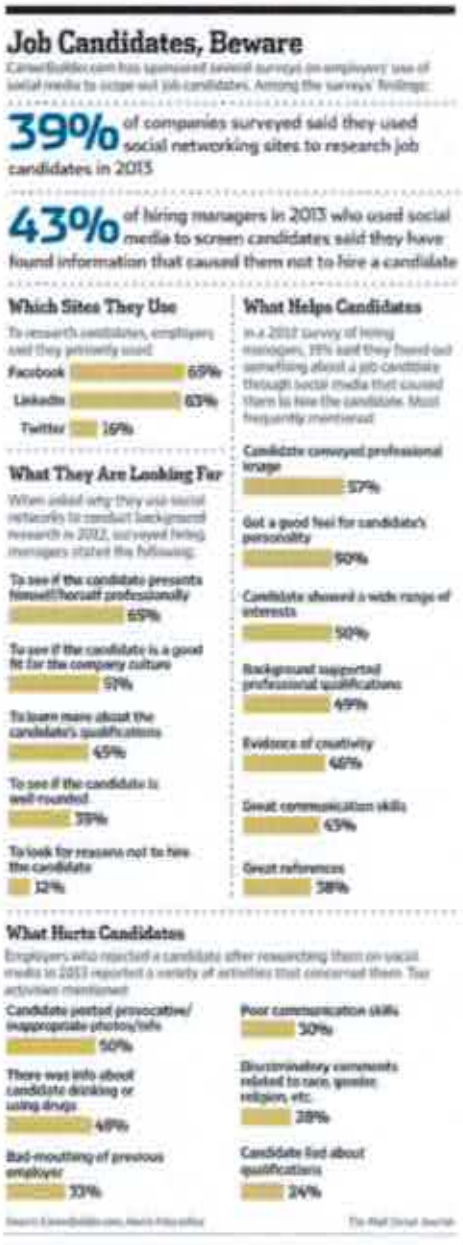
Ms. Flynn is the founder and executive director of The ePolicy Institute, a training and consulting firm that helps employers limit email and Internet risks. She can be reached at reports@wsj.com .

No: It Too Often Becomes a Fishing Expedition Unrelated to Work Issues

By Lewis Maltby

Employers don't need to practice wall-to-wall monitoring of

Lewis Maltby *Beth Van Hoeven*



employees' social media to protect their legitimate interests.

Yes, employers have a legal *right* to monitor employees' conduct on their work computers. But the only time employers have a legal *duty* to monitor employee communications is when the employer has reason to believe that the employee is engaged in illegal conduct.

Many successful companies do exactly that—monitor only when there is a solid reason to suspect employee wrongdoing. These policies have been in place for years and work well.

The fact is, the vast majority of what employees do on the Internet has nothing to do with work, takes place during their private lives and is done on their personal computers. Once again, employers should get involved with employees' private lives only when there is reason to be concerned.

Human Elements

It's simply too easy to turn social-media searches into fishing expeditions. Employers are human and cannot avoid being offended by employees' private behavior that goes against their values. Experience shows that employers fire employees for reasons having nothing to do with work. People have lost jobs because of their political opinions and religious beliefs. A photo in a bikini has cost many women their job. One man was fired because his employer didn't like his short stories (too much sex and violence).

What's more, companies frequently reject qualified applicants because they don't like what they find out about them online. The majority of employers in a recent survey (77%) said they now conduct Internet searches of prospective employees, and over a third (35%) have rejected job applicants because of information they found. I have spoken to otherwise fair employers who refuse to hire anyone who has party pictures on their Facebook page.

Refusing to hire people because of private behavior unrelated to work is not only unfair, but hurts the employer. In a competitive economy, companies need to hire the most qualified applicants. When HR professionals reject the top candidate because they disapprove of the person's private life, the employer loses, too.

There's more subtle damage as well. HR professionals are already hard pressed to investigate applicants thoroughly. Often there isn't enough time to speak with every prior employer, or to verify the

applicant's academic record. Taking time away from these crucial activities to go on Internet fishing expeditions diminishes the quality of the hiring process.

Internet searches also put employers at risk of liability. An employer who learns that an applicant is gay, Moslem, disabled, or over 40 years old, and then hires someone else may face discrimination charges. Once the employer has such information, it may be difficult to prove that it wasn't used in making the hiring decision. Even if the employer ultimately prevails, valuable time and money are lost. It's much safer not to acquire the information.

Use With Care

Of course, there are situations in which an applicant's Internet activity is of legitimate concern to an employer. A police department should think twice about hiring an officer that belongs to racist groups. Someone who visits child-pornography sites shouldn't be hired to work with children. A applicant with a drinking problem could be the wrong choice to drive a truck.

In cases like these, employers should hire a third party to conduct the search. Employers should determine what type of information is relevant to the job and instruct search firms to report only this type of information.

You can't blame employers for wanting to know more about applicants before making a commitment. There are circumstances where the Internet may contain relevant information. But sending HR professionals indiscriminately trawling through social media is unfair and causes more problems than it solves.

Mr. Maltby is president of the National Workrights Institute, a nonprofit research and advocacy organization focused on human-rights issues in the workplace. He can be reached at reports@wsj.com .