July 16, 2015

Five Technology, Media, and Telecommunications Developments Important to Employers

---

For the latest employment, labor and workforce management news and insights in the technology, media, and telecommunications industry, subscribe to our Technology Employment Law blog.

The laws that govern the workplace affect companies in the technology, media, and telecommunications industry in myriad ways. From the rise in workplace discrimination claims unique to this industry and the increase in union organizing activities affecting high-tech and new media companies, to Federal Trade Commission ("FTC") regulation of social media policies, compliance in the workplace is a challenge. Further, as new technologies are introduced into the workplace, additional hurdles arise, including data privacy and security obligations as well as policies on working with robots and robotic systems that are compliant with Occupational Safety and Health Administration ("OSHA") recommendations. This issue of Epstein Becker Green's *Take 5* addresses all of these evolving issues confronting employers:

1. **BYOD Programs: Privacy and Security Issues and Minimizing the Risk**
2. **High Tech and New Media: Organized Labor's New Frontier**
3. **A Growing Role for the FTC in Regulating Workforce Management**
4. **Avoiding Age Discrimination Complaints in an Industry Noted for a Lack of Age Diversity**
5. **Robotics in the Workplace: How to Keep Employees Safe and Limit Exposure to OSHA Citations**

1. **BYOD Programs: Privacy and Security Issues and Minimizing the Risk**
   By Brandon C. Ge

As mobile devices become more prevalent, employers are increasingly turning to bring-your-own-device ("BYOD") programs that allow employees to use their personal devices for work purposes. More people are beginning to own multiple mobile devices, such as smartphones and tablets, and wish to use these devices for work purposes. Even without an employer-sanctioned BYOD program, many employees choose to use their personal devices for business purposes, allowing them to work from nearly anywhere.

A BYOD program can provide several benefits. Employees—who often develop preferences toward particular devices or brands—can use whatever devices they prefer. Instead of having to acclimate to company-issued devices, employees can use devices with which they are already familiar. Many people also find it inconvenient to carry company-issued devices in addition to their personal devices when traveling. With the growing emphasis on lighter and thinner mobile devices, many employees are reluctant to neutralize these weight savings by carrying extra devices. Companies may also find that they save money by not having to issue devices and manage data and voice plans. These savings can instead be used to provide support and maintenance.

While BYOD programs have potential benefits for both companies and employees, many companies struggle to design programs that maintain these benefits while protecting the privacy and security of sensitive data. Depending on the organization, such data may include individuals' personal, financial, and health data, as well as important business-related data, such as human resources information, confidential information related to legal matters, and trade secrets. Therefore, employers need to consider various measures to minimize the risk involved in a BYOD program.

Concerns for Employers

By allowing employees to use their own devices for work purposes, employers lose some degree of control compared to a company-owned device. Although criminal cyberattacks frequently make headlines, employee negligence and lost or stolen devices continue to be a primary cause of data breaches. People tend to carry their personal devices everywhere, so when they are allowed to create, store, and transmit work-related information on these devices, there is a heightened risk of exposing sensitive company data to unauthorized individuals when these devices are lost or stolen.

There are also risks that do not involve loss or theft of devices. For example, if employees download malicious software, third parties may gain access to sensitive data. As another example, employees, especially those who own multiple devices, often store or back up their data in the cloud for convenient access across devices. In this instance, if the cloud service provider experiences a security breach, the company's information may be at risk.

Employers also need to keep in mind that people frequently allow friends and family to use their personal devices. Compounding the risk is that when devices are shared with trusted friends and family members, the devices are often handed off already unlocked, potentially allowing unrestricted access to company information and networks. Friends and family members may also lack the employee's security training and may inadvertently install malicious software that puts company data at risk.

Companies must consider business purposes, such as preserving reputation, as well as the numerous potential legal obligations surrounding data privacy and security. For example, federal and state breach notification laws would apply to the unauthorized use or disclosure of certain types of data. The information may be subject to many confidentiality laws, such as the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule. Businesses need to consider the various security laws that may apply, such as the HIPAA Security Rule and the Gramm Leach Bliley Act. There may be contractual obligations or trade secret laws to keep in mind. Employment laws may also enter the picture. For example, if nonexempt employees are allowed remote access via their BYOD devices, they might perform more "off the clock" work, which could give rise to wage and hour claims.

Moreover, employees may have privacy concerns. While some enjoy the freedom to use personal devices for both work and personal reasons, others may be hesitant to blur the lines between their work and personal lives. Some employees may be concerned about the privacy of their personal data, such as photos, text messages, personal email, and web browsing histories.

Implementing a Successful BYOD Program

One of the first steps in implementing a BYOD program is determining which employees should be permitted to participate. Not everyone in an organization needs mobile access to work e-mail and files. Certain positions in the organization may also involve greater risk that outweighs the benefits of participation. Employers should carefully analyze the various job functions within the organization and determine whether participation in the BYOD program is appropriate for each.

To address the concerns associated with a BYOD program, employers should have a carefully crafted BYOD policy and make sure that employees read, understand, and consent to its terms and conditions. The terms and conditions should describe the ways in which the employer will access and use employees' devices. For example, employers should retain the right to access devices for business purposes, if necessary. The policy should also describe employees' responsibilities, which may include reporting lost or stolen devices within a certain timeframe and refraining from using unapproved devices or installing unapproved applications.

Businesses should adopt procedures that address termination of employment, including procedures for deleting company data stored on terminated employees' devices.

Processes should be implemented to ensure that terminated employees no longer have access to company networks.

Companies should also implement various technical safeguards, such as encryption and passcode protection. Using a mobile device management ("MDM") solution can help with configuring and enforcing these safeguards. MDM software can allow employers to require encryption and strong passwords, disable cloud services, lock devices after a period of inactivity, remotely wipe lost or stolen devices, and prevent the installation of unapproved applications on employees' devices. MDM solutions can also help companies track which devices are participating in the BYOD program.

Training is vital to a successful BYOD program. Training should include regular reminders of good security practices, such as using strong passcodes, physically securing devices against loss or theft, and refraining from giving others access to devices that are used for work. BYOD programs shift much of the control over security to employees, so it is vital that employees are properly trained and receive periodic training refreshers.

2. High Tech and New Media: Organized Labor's New Frontier

By Steven M. Swirsky

When one thinks of industries where union activity remains strong and additional organizing is likely, one may think of health care, education, retail, heavy manufacturing, and other "old school" fields, but not high tech and "new media." Recent developments, however, including targeted campaigns focusing on employers in the Silicon Valley, its East Coast cohort Silicon Alley, and online, demonstrate that these assumptions may not be correct. High tech and new media are in the sights of not only some of America's most actively organizing unions but also a coalition of interest and advocacy groups that are partnering with a coalition of unions with the common goal of increasing union representation at high-tech companies and the various contractors, subcontractors, and vendors that clean their facilities, feed their employees, and drive them to and from their facilities.

Taken together with the recent rule changes adopted by the National Labor Relations Board ("NLRB" or "Board") to allow for much faster union representation elections in smaller units defined by unions, and the Board's continuing emphasis on the application of the National Labor Relations Act to employees who are not represented by unions and who work in non-union workplaces, employers in the high-tech and new media fields should be aware of how these forces can impact their businesses and the ability to maintain dynamic workplaces.

Silicon Valley Rising: An Industry-Targeted Movement

When 1930s legendary bank robber Willie Sutton was asked why he robbed banks, he replied that was where the money was. Today's labor unions, with their emphasis on income inequality and the gap between the 1 percent and the 99 percent have realized

that Silicon Valley and technology companies are where the money is today and that there are many more employees in these industries who are not receiving the high salaries, stock options, and perks that many think of when they think of Silicon Valley.

A well-financed effort by a coalition of unions—including the Teamsters, the Service Employees International Union (SEIU), the Communication Workers of America (CWA), UNITE-HERE, the South Bay Labor Council, the NAACP, and other community organizations—have banded together to establish "Silicon Valley Rising" to organize employees of high-tech employers and the various vendors and service providers that they rely upon.

Silicon Valley Rising' describes its goal as addressing what it sees as a two-tiered economic system in which, in its view, direct employees of the companies in the technology and media industry are paid well and receive good benefits, while those who support the industry as employees of contractors and suppliers are not. Silicon Valley Rising's focus includes the vendors and contractors that Silicon Valley employers rely upon for transportation, maintenance, food service, and the like.

One of Silicon Valley Rising's first successes came earlier this year, when it was certified as the bargaining representative of the company that Facebook relies upon to provide shuttle bus services between its various facilities at its headquarters. Soon after it won a representation election, Teamsters Local 853 negotiated a first contract with Loop Transportation that significantly increased wages and benefits and changed work rules and the like. In its campaign, Local 853 made clear that it saw the party that ultimately controlled the purse strings as being Facebook and media reports demonstrated the fact that Facebook was dragged into the matter and was ultimately responsible.

SiliconBeat (the "tech blog" of the *San Jose Mercury News),* the *Los Angeles Times, USA Today,* and other publications are all reporting that while apparently not a direct party to the negotiations between Loop and the union, Facebook has now "approved" the collective bargaining agreement, which it had to do before the contract could go into effect. In fact, Loop and Local 853 announced in their joint press release, "The contract, which workers overwhelmingly voted to ratify, went to Facebook for its agreement as Loop's paying client before implementation." Such economic realities are the type of consideration that the NLRB's General Counsel has been urging the Board to look at in deciding whether a joint-employer relationship exists.

High-tech and new media companies often rely upon third-party vendors to provide a range of non-core support services so that their own employees can focus on their primary activities. But if, as expected, the NLRB rewrites its definition and standards for determining who is a joint employer, the risks are increasing that high-tech and new media companies, like other employers, will face the prospect of having to stand alongside their vendors as employers of the vendors' personnel, including bargaining with their unions when they are represented.

3. A Growing Role for the FTC in Regulating Workforce Management

By Daniel J. Green

The FTC may be joining other federal agencies—such as the U.S. Department of Labor, the Equal Employment Opportunity Commission ("EEOC"), and the NLRB—in regulating the employment relationship, especially in the technology industry. On May 29, 2015, the FTC indicated that it would begin scrutinizing employer social media policies. Pursuant to the FTC's new guidance, an employer should ensure that its social media policy requires employees to disclose their connection to the employer prior to endorsing any of the employer's products on social media. Without such a policy, the employer may be held liable for false advertising because of the employees' failure to make an adequate disclosure.

FTC regulations[1] require a person who endorses a product to disclose any material connections with the seller of that product that affect the endorser's credibility. For example, video game reviewers must disclose that they are paid for their reviews by the games' manufacturer. The regulations also provide that the recipient of an endorsement "should advise" the endorser that "the connection should be disclosed, and it should have procedures in place to try and monitor his postings for compliance."

Under the new guidance, employees must disclose their employment relationship when endorsing their employer's product. Employers are not expected "to monitor every social media posting" by their employees. An employer's social media policies, however, should advise employees of their disclosure obligations. Further, employers "should establish a formal program to remind employees periodically of [the employers'] policy." And if an employer learns that an employee has posted a review without an adequate disclosure in violation of company policy, the employee should be instructed to remove the review or correct it to contain a disclosure.

This guidance comes in the context of increasing FTC scrutiny of the technology industry. The FTC's guidance was issued in response to changing technology and provided specific guidance to bloggers, video game reviewers, and Internet-based businesses. The FTC has also been active in seeking to regulate crowdfunding and the sharing economy. These categories of products often blur the lines among customers, suppliers, and employees. Many sharing-economy companies specialize in creating a marketplace for labor, including car rides, pet sitting, and miscellaneous household chores. The FTC is looking to promulgate regulations that place the burden on sharing-economy businesses to protect other market participants. The agency will be accepting comments on this issue until August 4, 2015. This rapidly developing area of the law will likely spawn new regulations governing the independent contractor relationship and may even result in a new category of worker, other than employees or independent contractors, governed by a different set of regulations.

---

[1] 16 C.F.R. § 255.5.

Finally, although employers are aware that non-compete and non-solicitation agreements should be carefully drafted so as not to run afoul of the antitrust laws, the FTC may begin scrutinizing the anticompetitive effect of settlement agreements resolving these cases. The agency has been aggressively scrutinizing "pay for delay" settlement agreements in which plaintiff brand-name pharmaceutical companies pay defendant generic pharmaceutical manufacturers not to enter the market (whereas, in most settlements, the defendant pays the plaintiff). Last year, we discussed how agreements among employers not to compete for employee talent can violate antitrust law. Settlement agreements in which either party receives concessions that it could not have received had it prevailed in the lawsuit may soon be subjected to similar scrutiny. For example, settlements in which both plaintiff and defendant agree not to hire or solicit each other's employees for a period of time may soon be subject to FTC investigation.

All employers, but especially those in the technology industry, should keep abreast of new legal developments, which may come from unexpected directions. An informed employer will be better positioned to adapt to, and even shape, developments without paying to litigate the test case.

4. **Avoiding Age Discrimination Complaints in an Industry Noted for a Lack of Age Diversity**
   By Lori A. Medley

Current gender and sex discrimination lawsuits filed against various Silicon Valley companies and the reported lack of gender diversity in the technology industry have recently garnered a great deal of attention. In addition, a series of age discrimination suits over the years and increased attention in the media on the industry's recruitment practices reveal that the technology industry is also vulnerable to complaints of age discrimination.

The technology industry is often described as youth-oriented and is noted for having extreme age imbalances among employees. According to a 2013 survey conducted by Payscale.com, an online salary, benefits, and compensation information company, the median ages of employees at the technology industries' top companies fall within the range of late 20s to late 30s. Given the reported lack of age diversity, this environment makes the industry vulnerable to lawsuits from individuals who are 40 or older and protected by the Age Discrimination in Employment Act of 1967 ("ADEA") and/or state and local anti-discrimination laws. Indeed, over the years, there have been several age discrimination cases brought by individuals in their 50s and 60s against the technology industry that have attracted media attention. The cases typically involve allegations of age discrimination in the workplace that the former employees alleged led to their terminations.

The technology industry has also faced criticism that its recruitment efforts imply a discriminatory preference for younger employees. Specifically, the industry has been noted for placing advertisements for positions that appear to suggest that people within a certain age range should apply for the position. The EEOC has taken notice of this

practice and, at least in instances in which the job notices specify that the position is for "new graduates" or individuals of specific graduating classes, has viewed these job notices as illegal because they deter older applicants from applying. Generally, under the ADEA, job advertisements cannot specify age preferences unless there is a bona fide occupational qualification for the age restrictions. Employers should also take note that with the EEOC's focus on addressing systemic discrimination, in which the EEOC is investigating alleged discriminatory patterns or practices or discriminatory policies that have a "broad impact on an industry, profession, company or geographic area," employers in the technology sector could be at risk for an EEOC enforcement initiative. In addition, the increased attention on the technology industry's hiring and recruiting practices could lead to a rise in age-based failure-to-hire litigations. Indeed, this past spring, a job applicant in his 60s filed an age discrimination putative class action lawsuit alleging that a technology company failed to hire him because of his age.

Given the increased focus on diversity issues facing the technology sector, technology industry employers can take the following steps to help minimize the risk of incurring an age-biased claim:

- Carefully review all advertisements or notices for job positions to ensure that they do not, either explicitly or implicitly, suggest that only individuals of a certain age range should apply. Avoid using phrases such as "new or recent graduates" or stating in the qualifications that individuals who graduated from specific class years (such as 2007 to the present) should apply. Instead, terms such as "entry-level position" and "no experience required" would be acceptable.

- Remove all questions or inquiries from employment applications that seek to elicit information about an applicant's age unless the applicant's age is a bona fide occupational qualification that is reasonably necessary to the normal operation of the business.

- Avoid asking questions or requesting information during the interview process that could establish an individual's age, such as date of birth, year of high school graduation, etc. Even if this information does not play a deciding role in whether to hire an applicant, the hiring process could be deemed tainted. The better practice is to wait until after the individual has been hired and the person's age or date of birth is needed for payroll and/or insurance purposes to collect such information.

- Make sure that company policies and procedures are up to date and address all forms of discrimination.

- Establish and promote a corporate culture that does not tolerate discrimination in any form.

5. Robotics in the Workplace: How to Keep Employees Safe and Limit Exposure to OSHA Citations

By Valerie N. Butera, with Theresa E. Thompson (Summer Associate)

Today's workplace is rapidly changing and so is its workforce. An increasing number of jobs once performed by humans are now performed by robots, and this has not escaped OSHA's attention. In fact, an OSHA test case is currently underway regarding the protection of employees when working with robots.

The first instance of a robot-related fatality in the United States occurred July 21, 1984, in a die-cast factory. Over the subsequent 15 years, OSHA and the National Institute for Occupational Safety and Health ("NIOSH") published guidance regarding robotics safety. In light of this test case and the increasingly broad range of hazards that OSHA targets, it is likely that OSHA and NIOSH will soon update guidelines for the safety of employees who work with or around robots. Despite the age of some of the existing OSHA and NIOSH recommendations regarding safe work with robots, they provide a helpful framework for employers to rely on in their efforts to keep employees safe and avoid costly OSHA citations. Most incidents of injury occur during activities such as maintenance, programming, and adjustments of robots. To avoid such incidents, employers should consider the following fundamental areas for safety improvements.

Designing Robotic Workstations

When designing robotic workstations, there are a number of factors to consider, such as how much space the robot will need to function. This will likely be more than a human being would need to conduct the same task. Employers need to be sure that adequate clearance distances are established.

One of the most important features of a robotic workstation is a safety fence, at least six feet in height, with an electrical interlocking gate. It should not be possible to access the robotic workstation when the gate is closed. This will prevent unauthorized entry into the range of the robot's moving parts. When the gate is opened, the operation of the robot should stop. Deliberate manual action should be required to restart the robot's automatic operation. In addition, employers should:

- avoid free-standing steel posts—these create "pinch points" where an unsuspecting worker can become trapped between the post and the robot's arm;

- consider limit switches and fixed stops located near an axis of rotation or translation;

- provide barriers between the robotic equipment and the object if freestanding objects in the robot's proximity cannot be avoided; and

- be aware that safety rails, chains, ropes, and floor markings, although useful as a cautionary reminder, do not provide adequate perimeter guarding.

Another important feature of a safe robotic workstation is a presence sensing device. Presence sensing devices include light curtain installations, pressure floor mats, and ultrasonic sensors on the robot's arm. When a presence is sensed by the device, the robot is triggered to either operate at a greatly reduced speed or halt motion entirely. The ideal design includes more than one presence sensing device.

Furthermore, employers should do the following:

- Contemplate all aspects of robotic controls. Controls from which the robot can be operated should never be located within the area where the robot is working and should always be guarded against accidental operation.

- Include as much remote technology as possible so that most troubleshooting can occur outside the robot's workstation. The control panel should feature single function controls, allowing an operator to control single pieces of equipment in the workstation safely, and user-prompt displays to minimize human errors.

- Make sure that there are numerous emergency stops located in easily accessible and convenient locations, as well as a portable programming control device that contains an emergency stop.

- Consider whether an emergency stop should cut off power or trigger a braking system to avoid additional hazards like the sudden dropping of a robot's arm or flinging of a work piece.

Training for Employees and Supervisors

Extensive safety training should be provided for all employees who are expected to have any possible contact with the robot system. Workers must be familiar with all working aspects of the robot, including the full range of motion, known hazards, programming information, locations of emergency stop buttons and power sources, and the importance of safety barriers. Training should also include procedures for freeing a colleague who becomes caught. It is important to emphasize that just because a robot is stopped does not mean it will remain stopped, and just because a robot is a repeating a motion does not mean it will continue to repeat only that motion.

Newly trained employees should be closely supervised until they adjust to the robot. Training requirements do not, however, only apply to newly hired, inexperienced employees. Experienced robot programmers and operators should also receive refresher training courses that allow them to stay up to date with technological advancements and remind them of the concern for safety. Supervisors should receive the same robotics training as other employees and operate under the assumption that no one is permitted to enter the robotic workstation without first reducing the speed of the robot or halting its movement.

Establishing Policies and Procedures Regarding Robotics Safety

Employers should create written safety rules for working around robotics. These rules and procedures should be strictly enforced and violations should result in disciplinary action. Policies should require employee training, detail energy control procedures, and mandate periodic inspections. It may be advisable to establish different personnel for robotics safety to avoid conflicts of interest and assure proper supervision of robotic workstations.

Unauthorized personnel should never enter the robot workstation or access the robotic controls. Operators should never be in the area where the robot is working while the robot is operational. Lockout procedures and control panel protection should be employed. Further, a buddy system should be created, mandating the presence of another worker with access to an emergency stop any time that an employee enters the robotic workstation.

Conducting a Systematic Safety Analysis

If an employer has robotics in the workplace, it is important to conduct a systematic safety analysis to assess existing hazards and how they should be addressed. Two popular strategies for such an analysis are the Job Safety Analysis and the Fault Tree Analysis. The Job Safety Analysis involves identifying hazards faced by employees in each step that they take to complete a task and developing solutions for each hazard. When conducting this type of analysis, employers should keep in mind the variability in the way that tasks may be performed.

Alternatively, a Fault Tree Analysis begins by defining the unwanted injury event and then graphically constructing the sequence of events and conditions that could lead to that event. Failure rates and human reliability values can allow probabilities of sequences to be completed. For this analysis, knowledge of the events that could lead to an injury is essential.

Whichever type of analysis an employer conducts, it is important to ensure that selected devices and procedures are appropriate for actual and anticipated tasks and hazards, considering the robot's use, programming, and maintenance operations. Employers should evaluate maintenance policies and records to determine the degree of potential hazard exposures inside robotic workstations and ensure that robots meet current industry standards.

By taking these safety measures, employers that use robotics in the workplace can significantly reduce the risk of employee injuries and demonstrate their commitment to safety in this brave new world.

* * *

For additional information about the issues discussed above, please contact the Epstein Becker Green attorney who regularly handles your legal matters or an author of this *Take 5:*

Brandon C. Ge
Washington, DC
202/861-1841
bge@ebglaw.com

Steven M. Swirsky
New York
212-351-4640
sswirsky@ebglaw.com

Daniel J. Green
New York
212-351-3752
djgreen@ebglaw.com

Lori A. Medley
New York
212-351-4926
lmedley@ebglaw.com

Valerie Butera
Washington, DC
202-861-5325
vbutera@ebglaw.com

About Epstein Becker Green

Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in offices throughout the U.S. and supporting clients in the U.S. and abroad, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.