July 2016

Five Trending Challenges Facing Employers in the Technology, Media, and Telecommunications Industry

---

Employers in the technology, media, and telecommunications industry continue to face numerous workplace management and compliance challenges under changing laws. From evolving mandates regarding benefits and momentum toward portable benefits, to diversity initiatives and even the use of technology and wearables in the workplace, employers must navigate a myriad of laws in order to maintain compliant workplaces. Further, accumulations of massive amounts of data in the workplace continue to present storage and data privacy and security concerns. In addition, evolving standards concerning joint-employer status pose strategic challenges in the labor-organizing arena. This issue of Epstein Becker Green's *Take 5* addresses all of these evolving issues confronting 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.

1. **Moving Toward a System of Portable Benefits in the Gig Economy**
2. **Wearables in the Workplace: Promise and Pitfalls**
3. **The EEOC Advocates for a More Diverse Technology Industry**
4. **Data: It Is Lurking Everywhere, Especially in the Shadows**
5. **Does the NLRB's New Joint-Employer Standard Mean That a Corporate Social Responsibility Policy Can Turn a Customer into a Joint Employer?**

1. Moving Toward a System of Portable Benefits in the Gig Economy

By Michelle Capezza

As the employer-employee relationship and the meaning of a "workplace" continue to evolve in the "gig" (or "sharing" or "on-demand") economy, a model of portable employee benefits, which are managed by mobile workers themselves, is gaining appeal. This employee benefits approach is not currently intended to replace employer-provided benefits for all workers but rather to fill a gap for those who may work independently as contractors or as temporary employees, do not have access to workplace benefits, or move from employer to employer quite frequently. Development of such a model, however, calls into question the future of the employer-provided system of employee benefits, which has been under attack in recent years.

As a result of the demise of the employer-provided pension plan and the rise of participant-directed savings plans, workers have already felt the movement away from the paternalistic approach to retirement benefits. This development has not been without controversy, as exemplified by the debates regarding participant savings rates, education regarding investments and fee transparency, and the U.S. Department of Labor's ("DOL's") fiduciary rule regarding investment advice.

Also, on the health care front, the Affordable Care Act has provided a platform for workers to obtain their own individual health insurance in the Marketplace, either through choice or necessity, and the tax benefits of employer-provided health benefits are being threatened in tax reform initiatives. With the implementation of consumer-driven designs, employees are also managing their health spending and insurance choices.

These changes in benefits design and access to employer-provided programs, as well as the rise of the mobile workforce, have provided a foundation for further movement toward portable benefits. This movement continues to manifest itself in several ways, including through:

- ***President Obama's call for portable benefits programs.*** In his fiscal year 2017 budget, President Obama called for the development of programs to provide grants to states and nonprofits to design ways to provide retirement and other employee benefits that can be portable and accommodate contributions from multiple employers. In addition, he called for legislation regarding open multiple employer plans ("MEPs") among unaffiliated employers to allow for pooled plans and continued contributions when employees move between employers participating in the same MEP. He also proposed requirements to allow part-time workers to participate in plans and measures for easier rollovers to plans. These initiatives would build upon earlier proposals for automatic payroll individual retirement accounts ("IRAs") and other tax credit initiatives to small businesses.

- ***Automatic payroll IRA programs and other alternatives***. For employers that do not sponsor any retirement savings plans, there is increased momentum for automatic payroll IRAs. To date, at least five states (California, Connecticut, Illinois, Maryland, and Oregon) have enacted legislation that will require certain employers that do not sponsor a retirement plan to enroll employees automatically in a state-run IRA program. New Jersey and Washington have approved retirement marketplaces for eligible employers to shop for retirement savings programs, and many more states are considering alternatives, including state-run IRAs and MEPs. These initiatives follow guidance from the DOL facilitating such efforts (including parameters for state-run IRAs to avoid being subject to ERISA) and complement the U.S. Department of the Treasury's guidance regarding *myRA* accounts, as well as President Obama's agenda. Other legislative proposals include mandates for contributions to plans run by third parties or the federal government. Laws in this area will continue to evolve.

- ***Portability policy advocates.*** In "Common Ground for Independent Workers," an array of businesses, labor organizations, venture capitalists, and other stakeholders in the gig economy have called for policies to ensure a social safety net for all workers. This past May, Uber was among the first employers in the gig economy to come to agreement with the Independent Driver's Guild, which is working on ways to offer its members a range of portable benefits. Retirement Clearinghouse ("RC") has advocated for auto-portability plans that move retirement savings assets automatically with workers as they switch jobs. RC has requested an advisory opinion from the DOL to permit negative consent, which would allow plan account balances to roll automatically into a new employer's plan.

What Employers Should Do Now

In the race for talent, it is important for employers to consider their own philosophy concerning employee benefits and the types of programs that they desire to offer their workers, whether full time, part time, contingent, or otherwise. It is also necessary to assess compliance with any programs that may be mandated by changing laws. In this evolving landscape, an employer should:

- examine its organization's workforce and determine which benefits programs are desirable to attract, motivate, and retain these workers in a competitive marketplace;

- identify any gaps in benefits offerings and consider how to fill those gaps;

- monitor legislation affecting employee benefits and applicable compliance requirements; and

- determine whether its organization is subject to laws that will require it to comply with certain government-mandated programs when no applicable benefit program is otherwise offered by the employer, and decide whether it is instead desirable to establish, or expand coverage under, an employer-sponsored plan.

2. Wearables in the Workplace: Promise and Pitfalls

By Ian Carleton Schaefer and Bonnie I. Scott

In recent years, the use of wearable devices, such as smartwatches and Fitbits, has gained popularity not only with the general public and consumers but also among employers as a way to encourage workers to maintain healthier habits and, in turn, help reduce health care costs. Increasingly, companies are distributing wearable devices to employees as part of workplace wellness programs. According to one estimate, nearly half of employers that have a workplace wellness program use fitness trackers.[1] This trend shows little sign of abating. The data collected from these trackers—on such things as quality of sleep and activity level, for example—can be shared with health insurance companies, which may allow employers to negotiate lower insurance policy rates for their employees. Companies that have encouraged wearable fitness trackers have also realized other benefits, including decreased absenteeism and increased worker productivity.

Beyond wellness applications, employers around the globe are also using wearables to increase worker safety. One company in Australia, for example, has had its truck drivers wear "SmartCaps"[2] in an effort to reduce fatigue-related accidents. These hats resemble baseball caps but include built-in sensors that can detect driver alertness and provide a warning to drivers when their fatigue level begins to rise.

To be sure, the benefits of wearable devices, as well as the value of the data generated by them, cannot be ignored. Yet, despite the potential benefits of introducing wearables into the workplace, employers should be mindful of the potential legal pitfalls. Monitoring employees, whether during work or non-work hours, can expose employers to legal risks even if the monitoring is intended to promote employee wellness, improve business operations, or keep employees safe.

What Are the Legal Risks?

Several legal risks arise from the various health-related data that can be collected from these workplace wearables and used by employers. One key threat is that cybercriminals could hack into the servers of companies that sell fitness tracking

---

[1] Patience Haggin, *As Wearables in Workplace Spread, So Do Legal Concerns*, The Wall Street Journal, March 13, 2016, http://www.wsj.com/articles/as-wearables-in-workplace-spread-so-do-legal-concerns-1457921550.

[2] RioTinto, *Hi-Tech Cap Helps Coal & Allied Truck Drivers Work Smarter to Manage Fatigue* (May 2013), http://www.riotinto.com/media/media-releases-237_8713.aspx.

wearables (and manage the associated mobile health apps) and access employees' personal data. It is also possible that these companies could sell employees' personal data to advertising companies or other third parties without employee knowledge.

In addition to data privacy and security concerns, antidiscrimination laws also represent an important risk for employers. For example, under the Americans with Disabilities Act ("ADA"), employers are prohibited from conducting a "medical examination" of employees unless the examination is "job-related and consistent with business necessity."[3] A medical examination includes a procedure or test that seeks information about an employee's physical or mental impairments or health. Because wearables today can measure various health metrics, such as heart rate and blood pressure, an employer's rollout of wearables could unintentionally result in prohibited medical examinations under the ADA. While employers are permitted to conduct voluntary medical examinations as part of voluntary workplace wellness programs, provided that certain conditions are met, this is still an area in which employers should be cautious. Further, to the extent that wearables collect information about employees' family medical history or other genetic information, employers may face liability under the Genetic Information Nondiscrimination Act ("GINA"). Under GINA, it is illegal for employers to use genetic information in making employment decisions. Finally, employee monitoring, particularly with respect to GPS location, can also potentially run afoul of protections afforded by the National Labor Relations Act ("NLRA").

How Can Employers Mitigate the Risks of Using Wearables in the Workplace?

While the law in this area is in its nascent stage, before rolling out a wearables program, either as part of an overall wellness plan or independently, employers in all industries should do the following:

- Although wearable technology is rapidly advancing and adopting novel methods of employee tracking and monitoring may be alluring, exercise particular caution when adopting novel tracking methods, regardless of how strong the underlying business, health, and/or safety justification may be.

- Consider working with a third-party vendor to administer the workplace wellness program so that you receive information derived from employee wearables on an aggregate basis that does not individually identify data for any specific employee.

- Ensure that there is a policy in place detailing how the technology will be used and the scope of information that will be collected. Also, consider obtaining employee consent related to data collection.

---

[3] U.S. Equal Employment Opportunity Commission, *Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act (ADA)* (2000), https://www.eeoc.gov/policy/docs/guidance-inquiries.html.

- As the legal landscape surrounding workplace wearables evolves, closely track and monitor developments in applicable state and federal laws (including the ADA, GINA, and NLRA, among others) and revise your policies accordingly.

3. The EEOC Advocates for a More Diverse Technology Industry

By Nancy L. Gunzenhauser

Throughout 2016, the Equal Employment Opportunity Commission ("EEOC" or "Commission") has been examining initiatives to identify and attempt to rectify a perceived lack of diversity in the workplace. The EEOC has, in particular, identified the technology industry as an area where significant strides can be made to create a more diverse workforce.

Following a May 18, 2016, public meeting on diversity in the technology industry, the EEOC issued a "Diversity in High Tech" report ("Report") summarizing research on the lack of diversity in the "high-tech sector," defined as industries that employ a high concentration of employees in the STEM (science, technology, engineering, and mathematics) occupations and the production of goods and services advancing the use of electronic and computer-based production methods. The Report highlighted several demographic trends within the industry, generally showing that the high-tech sector is still predominantly white, male, and under 40 years old. Citing the high-tech sector as "a major source of economic growth fueling the U.S. economy," the Report also identified demographic differences among the types of positions within the industry, noting that African Americans and Hispanics were disproportionately underrepresented in leadership positions in technology jobs.

According to the Report, the lack of diversity in the labor force within the high-tech sector can be attributed to the demographics of graduates with STEM degrees. Nearly 70 percent of graduates in engineering, mathematics, and computer science are men. While the Obama administration has included STEM education as a priority, the current graduates in STEM fields are significantly less diverse than in the general labor market.

Further, more than half of the women working at STEM companies in the high-tech sector eventually leave or do not advance within the STEM industry. The Report attributed women's exit from the high-tech sector to an "inhospitable" work culture, isolation, work styles incompatible with the "firefighting" style generally rewarded, long hours and travel, and a glass-ceiling effect.

While the high-tech sector originated in Silicon Valley, the scope of this industry has grown across the United States. To see whether the diversity statistics differed at the epicenter of high tech, the Report further analyzed the labor force within Silicon Valley. The labor force generally in Silicon Valley is split evenly between men and women; however, within the tech industry, it becomes a 70-30 split in favor of men. While Asian Americans fared better within Silicon Valley than across the national survey for

professional jobs, white men "dominated" leadership positions across the nation and even more significantly in Silicon Valley.

While the Report is valuable in highlighting changes that are necessary to create a more diverse workforce within the technology industry, the EEOC's public meeting made clear that the Commission expects technology companies to address what it perceives to be the implicit and unconscious biases leading to the current demographics. In many technology start-ups, hiring practices and human resources policies are generally among the last concerns in growing companies; thus, companies recruit via word of mouth or weed out certain categories of candidates, such as older workers, leading to a more homogenous workforce. The findings stated in the Report and at the public meeting should encourage emerging companies to consider employee issues at the forefront, rather than as a secondary concern.

In Silicon Valley, where the lack of diversity is amplified within the high-tech sector, changes in California law may encourage employers to recruit from a more diverse pool of candidates. At the end of June, the California Legislature passed an amendment to the Equal Pay Act that, if signed by the governor, would provide a cause of action for a differential in pay on the basis of race or ethnicity unless the employer can show that the difference is based on a bona fide factor other than race or ethnicity. (The California Equal Pay Act was also recently amended to protect women more strongly against pay differentials.)

In addition to the Report, recently proposed EEOC guidance on national origin discrimination and the EEOC's updated proposed rule to include salary bands on the annual EEO-1 report demonstrate the Commission's commitment to encouraging a more diverse and inclusive workforce. The EEOC's in-depth look at the high-tech sector should induce technology employers to review hiring practices and audit the diversity within their workforce, as the EEOC's enforcement of systemic discrimination has increased significantly over the past 10 years.

4. Data: It Is Lurking Everywhere, Especially in the Shadows

By Adam S. Forman and Matthew Savage Aibel

For years, companies have been struggling to understand the multitude of locations where their data resides. From traditional employment files with embedded Social Security numbers, to new-aged hiring software with videos of job applicants, and enterprise software used to facilitate employee communications, controlling employee, customer, and corporate data is, to say the least, a logistical challenge. One of the newest entries into the mix is the increased use of ShadowIT and cloud-based storage systems.

ShadowIT involves workers' use of unsanctioned products and applications to perform the work of the business enterprise. In other words, ShadowIT occurs when employees use their personal emails and applications, such as a cloud-based storage system,

instead of company-approved solutions. According to a recent survey, about one-third of IT use is considered ShadowIT. Whether responding to a subpoena in a wage and hour dispute, attempting to safeguard previous corporate secrets, or analyzing the extent of a data breach, a company's failure to understand the scope and location of ShadowIT data could be problematic. Companies should have policies in place regarding employees' (and other workers') use of unapproved applications, but there should also be an understanding that a policy is not a panacea.

For data storage, recent studies show that most organizations are using over 1,000 cloud-based services. Indeed, one such study found that an average organization had 1,154 cloud services in use. This large number demonstrates that companies must manage the sheer volume of data in the cloud or potentially be exposed to liability.

Companies must also think about physical storage when a laptop or a phone is stolen and suddenly control over data on that item is lost. One leaked file in California, for example, could require a company to send out a data breach notification to millions of customers in California (an issue magnified under varying state laws as well in the current landscape). No overall system is perfect for this task, and the idea that company data can be completely controlled may be an illusory one, but there are important issues for companies to consider and sensible steps that they should take to safeguard data, including the following:

- **Survey ShadowIT Usage**. Companies should consider conducting anonymous data audit surveys of employees to find out what other applications or products employees are using to perform their jobs. The company can then review its IT department to determine if it lacks the functionality for a certain program or if the problem of unsanctioned product use is simply a result of a lack of employee education as to the sanctioned products available to employees.

- **Manage ShadowIT Usage**. Employees using ShadowIT or unsanctioned products create control risks for companies, and employers may consider disciplining employees for not following corporate policies on approved applications. On the other hand, having draconian disciplinary measures in an effort to maintain control over data will not necessarily stop ShadowIT use but may force it deeper undercover. Discipline could also have an adverse impact on employee engagement and retention.

- **Consider "Amnesty."** Companies should consider whether it makes sense to implement a time-limited policy, whereby employees can bring their unapproved software or application to the IT department to see if the program can be moved onto an approved list from the corporation, without the threat of discipline or sanction.

- **Review Vendor Contracts.** Companies should review their contracts with vendors for approved cloud-based products and software. This may include

auditing other cloud-based companies where data is stored to ensure that the company is adhering to best practices of network security. The contracts should contain data breach notification clauses, as well as indemnification agreements, when possible.

- **Train Workforce.** Frequently, employees are the "weak link" in data control efforts, as they are often the cause of a data breach into a company's secure network. Training employees about how to spot scam phishing emails and protect intellectual property can go a long way toward mitigating that risk.

Technology is constantly evolving such that there will always be a new product or service that could potentially be a benefit to employee productivity. A ShadowIT survey, while helpful, is only a look back in time. Companies need a way to address ShadowIT use as it evolves going forward. A company prohibition on ShadowIT without some method for employees to submit new products for consideration without fear of reprisal keeps the company in the dark about its data. Companies must also be mindful of the other cloud-based providers' security protocols and the likelihood that a third party could accidently let sensitive data out into the public domain.

5. Does the NLRB's New Joint-Employer Standard Mean That a Corporate Social Responsibility Policy Can Turn a Customer into a Joint Employer?

By Steven M. Swirsky and Daniel J. Green

In August 2015, the National Labor Relations Board ("Board") issued its decision in *Browning-Ferris Industries of California, Inc.*, 362 NLRB No. 186 (2015), adopting a new standard for determining whether a company is a joint employer and therefore subject to all of an employer's legal obligations under the NLRA with respect to the employees of another employer that provides it with services, leased or temporary labor, or the like. Since then, there have been many dire predictions as to how this new test would result in finding businesses to be joint employers of the employees of those they do business with, whether suppliers of temporary labor, franchisees, or a wide range of other circumstances. The latest permutation involves claims that a business that maintains a corporate social responsibility ("CSR") policy intended to ensure that its suppliers and business affiliates comply with applicable laws and treat their employees fairly is, by virtue of such a policy, a joint employer of the supplier's employees.

Under the new test that the Board adopted in *Browning-Ferris Industries* ("BFI"), what matters is whether the purported joint employer *possesses* the authority to control the terms and conditions of employment, either directly or indirectly, of another employer's employees. In other words, the actual or potential ability to exercise control, regardless of whether the company has, in fact, exercised such authority, is now the focus of the Board's inquiry. As the Board puts it, "reserved authority to control terms and conditions of employment, even if not exercised, is clearly relevant to the joint-employment inquiry."

Not surprisingly, the Board's decision in BFI has been appealed. An amicus brief supporting a challenge to the BFI decision recently filed on behalf of Microsoft illustrates that the Board's new standard, if left undisturbed, is likely to have the unintended consequence of discouraging responsible companies from encouraging their suppliers to provide their employees with benefits in excess of the bare minimums required by law.

In BFI, the Board held that the NLRA imposes joint-employer obligations if (1) a common law employment relationship exists between the putative joint employer and another entity's employees and (2) "the putative joint employer possesses sufficient control over the employees' essential terms and conditions of employment to permit meaningful collective bargaining."

As this amicus brief points out, one potential consequence of the new joint-employer rule is to discourage companies from maintaining CSR policies to ensure that those companies they do business with, in the United States, follow responsible policies when it comes to the treatment of their own employees. Typically, CSR policies provide for a minimum set of standards that would-be suppliers and service providers are expected to follow. For example, in March 2015, Microsoft announced that it would do business with only those large suppliers that provided employees with at least 15 days of paid leave annually. Both President Obama and Secretary of Labor Perez praised Microsoft's CSR policy and expressed the hope that other companies would follow suit.

After BFI was decided, however, a union representing the employees of one of its suppliers claimed that Microsoft was a joint employer of the supplier's workers and therefore subject to the supplier's obligations under the NLRA *vis–à–vis* the supplier's workforce. When Microsoft disagreed and declined to participate in bargaining between the supplier and its employees' union, the union filed an unfair labor practice charge against Microsoft claiming that the company was a joint employer of the supplier's workers and accusing it of unlawfully refusing to bargain.

The amicus brief highlights the importance of the first element of the BFI test (i.e., only common law employers can be liable as joint employers) in constructing a workable definition of "joint employer." Basing the existence of joint employer status simply on whether a company has "sufficient control . . . to permit meaningful collective bargaining" overlooks the fact that a wide variety of economic actors have substantial control over the terms and conditions of workers employed by others. A company is unlikely to adopt a CSR policy if it lacks the size and market power to encourage vendors to comply with that policy. Thus, CSR policies do not demonstrate control over labor relations but, rather, should be more properly thought of as eligibility criteria for suppliers to provide services and do business. As Microsoft points out in its brief, "such oversight and standard-setting is commonplace in a supplier contracting relationship and is not the type of control that can support a finding of joint employment."

Thus far, unions have had some success in organizing the employees of vendors, such as shuttle bus companies that provide services to technology companies. They have

also had limited success organizing workers directly employed by technology companies. This presents a strategic challenge for unions as the direct employers of the employees they represent are often in commoditized businesses with comparatively low margins, unable to offer the pay and benefits provided to technology company employees. Unions therefore have a strong financial interest in blurring the distinction between customers and employers, in an effort to forge a strategy to force technology companies to the bargaining table and extract expensive concessions.

* * * *

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

Michelle Capezza
New York
212-351-4774
mcapezza@ebglaw.com

Ian Carleton Schaefer
New York
212-351-4787
ischaefer@ebglaw.com

Adam S. Forman
Detroit (Metro) / Chicago
248-351-6287 / 312-499-1468
aforman@ebglaw.com

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

Bonnie I. Scott
Washington, D.C.
202-861-1869
bscott@ebglaw.com

Matthew Savage Aibel
New York
212-351-4814
maibel@ebglaw.com

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

Nancy L. Gunzenhauser
New York
212-351-3758
ngunzenhauser@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