EMPLOYMENT, LABOR & WORKFORCE MANAGEMENT

EPSTEIN BECKER GREEN

VIEWS YOU CAN USE TAKE 5

TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS

May 2018

Five Workplace Challenges for Employers in Changing Times

As Gordon Gekko famously pronounced in the 1980s classic movie *Wall Street,* “The most valuable commodity … is information.” Those words have never rung truer than in today’s world and in today’s workplaces. And as the old adage goes, with great power comes great responsibility.

Modern employers have access to an unprecedented amount of data impacting their workforce, from data concerning the trends and patterns in employee behaviors and data concerning people analytics used in hiring, compensation, and employee benefits, to data that analyzes and dissects the composition of the employee workforce itself. For employers, this presents numerous challenges and opportunities, particularly in an employment age focused on the increased demand by employees, regulators, shareholders, and the general public for transparency.

For the latest employment, labor, and workforce management news and insights in the technology, media, and telecommunications industry, please visit and subscribe to Epstein Becker Green’s Technology Employment Law Blog.

These two competing phenomena—the availability of big data and the need to use big data responsibly—present nuanced and unique challenges for all employers.

What follows in this edition of Epstein Becker Green’s *Take 5* is our analysis and advice on striking the appropriate balance—to leverage the power of information while mitigating organizational and reputational risk:

1. **Big Data Analytics in Hiring**
2. **Diversity in Tech: What Employers Can Do Now**
3. **Pay Equity Audits: Holding a Mirror to Current Compensation Practices**
4. **The Time to Develop a Benefit Plan Cybersecurity Policy Is Now!**
5. **Are Genetic Screening Benefits Truly Beneficial?**

1. Big Data Analytics in Hiring

By Adam S. Forman, Nathaniel M. Glasser, and Matthew S. Aibel

While the phrase has different meanings depending on the context, “big data” typically refers to data that is so large in volume that computers, rather than traditional methods of analysis, are necessary to understand it. “Big data analytics,” a phrase often used synonymously for the actual data and its computerized analysis, encompasses data’s volume, collection speed, type collected, and how best to decipher it. Marketing departments have long used big data analytics to target potential customers with pinpoint accuracy. Human resources (“HR”) departments increasingly consider whether and how to incorporate big data tools into their hiring processes.

The promise offered by big data analytics, and certainly the vision sold by many of the vendors that specialize in selling big data tools for application in the HR context, includes better outreach to potential applicants, increased efficiency in the hiring process, fewer people hours spent combing through resumes, and the selection of more qualified and better-matched candidates. The market includes a variety of analytical tools for these purposes, such as algorithms that scan resumes to match candidates to jobs by simulating human hiring tendencies, measure candidates on personality traits deemed critical for success in the job, and assess the cognitive abilities of each candidate against those of high-performing incumbents. Vendors market their big data tools as predictive algorithms that will allow their clients to hire the right people by using data that maps the applicant’s profile onto the company’s available openings. Ultimately, by hiring the “right” people, companies will improve productivity, increase retention, and spend fewer resources on employee selection.

Many of these big data tools use artificial intelligence (“AI”) or machine learning to help select attributes and candidates for hiring. Machine learning takes the baseline algorithms that make selection decisions and improves upon them by learning from “mistakes.” For example, a job role might change organically such that an old job description might not adequately assess the skills needed by an applicant, but an AI algorithm trained to mine the data of current employees in the role might find character traits that help “define” the skills needed to succeed in the role. By taking these character attributes of current employees into account as a machine learns, hiring decisions potentially improve as the selection algorithm changes.

Before blindly adopting big data analytics, however, employers must be aware of the potential risks. For example, an employer cannot easily “look under the hood” to see precisely how the selection algorithm is operating, partially because vendors consider the algorithm to be proprietary and confidential, and partially because the vendors themselves do not know exactly how the algorithm has changed as a result of machine learning. Without the ability to assess what the selection algorithm is doing, employers may have difficulty determining which factors, if any, are a potential source of bias. Additionally, in the event of litigation involving an AI algorithm’s selection criteria, the employer may be unable to produce in discovery sufficient evidence of the decision-making process. Indeed, the algorithm that the employer is required to defend might be different from the version that was used at the time of the hiring decision. Oftentimes, even the vendor/data scientist who created the algorithm does not know what the algorithm is doing.

One can argue that big data analytics can lend consistency to the hiring process, reducing the subjectivity in selection decisions and potentially limiting the likelihood of a disparate treatment discrimination claim. Nevertheless, employers should be careful that the algorithm does not incorporate intentionally discriminatory factors. Moreover, employers should be aware that the increased consistency and objectivity also increases the potential for disparate impact claims. If the AI-influenced decision results in a statistically significant adverse impact on a group of candidates possessing one or more protected characteristics, employers may be more vulnerable to class or collective action allegations.

Big data analytics also presents special challenges related to its impact on persons with disabilities. Where a person's ability to use the technology constitutes an impediment to a proper assessment, the analytical tool may lead to claims of discrimination. Further, federal law precludes an employer from obtaining information about a candidate's medical history or condition before making a hiring decision. To the extent a big data tool collects information about medical history or causes candidates to disclose such information at an inappropriate time, the tool may violate discrimination law.

While a complete machine takeover of the hiring process remains unlikely, big data analytics continues to be an attractive tool to assist HR departments. To that end, employers should consider the following practical steps to safeguard against machine learning run amuck in the hiring process:

- Conduct a thorough due diligence of the vendor and its product(s), ask to view the algorithm and its different permutations, and seek indemnification to limit liability in the selection process.

- Conduct a periodic statistical sampling of the AI-selected applicant pool and candidates through an adverse impact analysis.

- Implement appropriate data security measures, such as determining how relevant data will be hosted and identifying a core group of individuals within HR who will have access to that data.

- Understand document retention obligations so as to properly comply with Equal Employment Opportunity Commission ("EEOC") guidance, U.S. Department of Labor ("DOL") regulations, and state law.

- Determine what to do with the data and how to access it, if and when the agreement with the vendor ends, or litigation occurs.

These steps are just a few of the considerations that employers should take into account when evaluating big data tools. For ultimate success, employers should be sure to involve all stakeholders, including business managers, HR, and legal counsel, in determining whether to adopt these tools.

2. Diversity in Tech: What Employers Can Do Now

By Andrea K. Douglas

While employment opportunities in the technology sector have grown at twice the rate of the national average, high-tech firms have struggled to increase diversity within the workplace. Data compiled from voluntary disclosures to the EEOC reveals large racial and gender disparities within tech workforces as compared to the private sector overall. Recent studies show that improving ethnic and gender diversity within the technology workforce presents an economic opportunity that could result in as much as $570 billion in new value for the tech industry, and could add as much as 1.6 percent to the national gross domestic product. With a new analysis of challenges to diversity in the tech industry, it is an ideal time for employers to evaluate diversity initiatives currently in use.

In the past, experts blamed the American education system for failing to provide women and minorities with the type of instruction needed for future careers in technology-driven fields, thereby causing a lack of quality applicants in selected science, technology, engineering, and mathematics ("STEM") occupations. Experts also opined that women and minorities self-selected away from STEM fields, contributing to a lack of diversity in the tech industry employment pipeline. Based upon that thinking, tech companies have focused diversity initiatives on efforts intended to increase diversity within the talent pipeline.

New research suggests that the lack of diversity in the talent pipeline is only part of the problem. In a recent report, the Kapor Center for Social Impact, an organization that aims to increase diversity and inclusion in the technology industry, opines that the lack of diversity in the technology sector results from a complex set of social and psychological barriers that occur across the length of the technology pipeline. While a lack of access to education impedes diversification of the tech industry, the report also cites environmental workplace problems, such as inhospitable corporate culture and unconscious bias, as factors that both impede the entry and facilitate the exodus of women and minorities in the tech workforce. Research also suggests that taking the following steps may address environmental factors that cause underrepresentation in the tech workforce:

- *Articulate a company-wide commitment to diversity.*

A comprehensive organization-wide diversity initiative should begin with a commitment to diversity and inclusion that is articulated by the highest levels of management in the organization. A comprehensive strategy includes the evaluation of an organization's recruitment, interviewing, performance management, and promotion processes to identify potential biases and weaknesses. While employers can specify diversity goals, employers should seek advice to ensure that the articulated goals are compliant with state and federal anti-discrimination laws.

- *Consider implementing social accountability tools.*

Employers should determine how management will be held accountable for supporting and engaging in diversity and inclusion initiatives. A corporate diversity task force can be an effective tool to promote social accountability. Diversity task forces comprised of department heads and members of underrepresented groups can be tasked with promoting events to bring awareness to diversity and inclusion in the workplace, engaging teams in diversity and inclusion conversation, and reviewing and proposing policies and procedures to promote workplace diversity and inclusion.

- *Promote inclusion with targeted training.*

In addition to anti-harassment training, employers should consider providing training with exercises such as perspective taking and goal setting. Evidence suggests these exercises can improve attitudes towards diversity. Perspective-taking exercises ask participants to mentally walk in someone else's shoes. Goal-setting exercises can be adapted to ask participants to set specific goals related to diversity in the workplace (e.g., challenging inappropriate comments overheard in the future, coupled with training about response and reporting such incidents).

- *Consider implementing a mentoring program.*

Workplace mentoring programs can both engage management in diversity efforts and help retain underrepresented employees in the tech industry. Formalized mentoring programs can provide a mechanism for managers to develop assigned protégés, and these programs can help underrepresented groups who may need greater assistance finding a mentor. When successful, mentorship programs encourage mentors to sponsor their protégés for key training and assignments, regardless of their gender or ethnicity, which can lead to increased representation of women and minorities in management ranks.

Conclusion

Issues regarding diversity and inclusion are not static. Employers may need to periodically revisit diversity initiatives and goals. By utilizing empirically supported activities, however, employers can fine-tune initiatives to progress towards a more diverse workforce.

3. Pay Equity Audits: Holding a Mirror to Current Compensation Practices

By Jeffrey M. Landes, Nancy Gunzenhauser Popper, and Alyssa Muñoz

In addition to recent legislative changes in California, Delaware, Maryland, Massachusetts, New Jersey, New York, and Oregon, pay equity in the workplace continues to garner widespread attention and has employers asking what they can do to better prepare. Developing a strategy to proactively engage in a pay equity audit is often the first and most effective step to ensure pay equity and minimize potential legal risk.

What Should Employers Expect When Conducting a Pay Equity Audit?

The scope and complexity of a pay equity audit may vary by employer, but, ultimately, the goals are to (i) identify whether pay inequity exists that cannot be explained by neutral, bona fide factors, and (ii) determine whether an employer's current policies are creating, or contributing, to these inequities. Employers should take these steps:

1. *Identify the Scope of the Audit*

It's important to first identify what departments, positions, and/or locations will be addressed in the audit. However, this step should be treated as an ongoing conversation and updated as needed throughout the process. In addition, employers should do the following:

- Know the specific positions and geographic locations in the scope to anticipate the state or local equal pay laws that may apply. Consider evaluating the pay rates of all employees or targeting specific departments, locations, or positions.

- Compare apples to apples. This generally involves substantially similar skills, effort, responsibilities, and the performance of such responsibilities under similar working conditions; however, it is important to consult state law to determine the relevant factors.

- Whether partnering with outside counsel or in-house counsel, request that steps are taken to preserve the attorney-client privilege and work product.

2. *Conduct the Audit*

In general, a pay equity audit will compare the average pay of men to the average pay of women (or other protected categories, where covered by applicable law) within relevant positions/grades. Employers should examine procedures and processes currently in place—performance evaluation and compensation systems, job descriptions, training programs, and any additional factors it uses to determine pay rates. Here, employers can expect to dig into their pay data to analyze whether disparities exist. Employers should also do the following:

- Because pay equity is not limited to gender, gather any data maintained on the demographics of the workforce. This will assist with reviewing where in the company women, minorities, and older workers may occupy certain positions/grades.

- Perform a statistical analysis to determine if sex (or any other protected category) has an impact on pay rates. Here, separate out and compare the salaries of men and women looking purely at position and grade, considering whether other factors explain any applicable disparities.

- Identify the factors used in deciding how employees are paid. This might include factors such as length of service, education, geographical location, or years of experience in the industry.

- Review performance evaluation procedures, identify factors used regarding compensation decisions, and consider whether they are applied consistently. Additionally, review factors used to determine employees' raises and bonuses. Consider sending questionnaires to the managers that make these decisions, or ask them to submit descriptions of how they determine bonus and raise amounts.

3. *Take Remedial Actions*

After the audit has concluded, a subsequent review of specific employees' pay or particular classifications/positions may be needed to determine whether the disparity is based on legitimate and neutral factors. If not, employers must be prepared to address any unjustified disparities and increase the affected employees' pay rate so that such rates are comparable to the work that he or she is performing. In addition, employers should do the following:

- Be cautious when making ad-hoc or non-routine pay adjustments. It's important to communicate changes effectively and in a manner that does not diminish employee engagement or morale.

- Give honest, brief, and general reasons for pay adjustments. For example, communicate that the adjustment is a result of ongoing compliance efforts.

What Should Employers Do After a Pay Equity Audit?

- Review and, if necessary, revise job descriptions/grades and consider implementing standard pay ranges or guidelines for each grade or job classification that may be useful when hiring new talent or acquiring companies with differing pay systems.
- Review and, if necessary, revise and distribute existing procedures on performance evaluations and factors contributing to bonuses and raises to ensure consistency in managerial decisions and positions/grades.
- Provide training to management, HR staff, recruiters, and compensation partners on the requirements of applicable state and local laws.

Conclusion

Audits of any sort can be overwhelming for employers, but engaging proactively in a pay equity audit helps employers identify and correct disparities as well as implement best practices going forward.

4. The Time to Develop a Benefit Plan Cybersecurity Policy Is Now!

By Michelle Capezza and Christopher Lech

There is widespread concern for the security of the employee data that is collected, transmitted, and stored with regard to employee benefit plans and for the security of the assets in participant accounts. Further, the array of technological tools that have emerged to aid in the administration and delivery of employee benefits continues to grow and fuels further concern.

Retirement industry groups such as the Spark Institute and the Financial Services Information Sharing and Analysis Center recently joined forces to establish the Retirement Industry Council to share information about new data security threats and strategies for improving security in the retirement market. Plan sponsors and fiduciaries must be cognizant of these developments and do their part to ensure that they have controls in place to prevent security breaches of plan participant data and assets, and that they have addressed these considerations with service providers. Although there is no clear fiduciary mandate under the Employee Retirement Income Security Act of 1974 ("ERISA") with regard to cybersecurity, plan fiduciaries do have a duty to carry out their responsibilities prudently and in the best interests of plan participants and beneficiaries. Employers that take the time to develop a benefit plan cybersecurity policy ("Policy") will be well positioned to demonstrate prudence and diligence in these efforts, and prepared in the event of a data breach.

At a minimum, consider taking the following actions, which are by no means exhaustive:

Assemble a qualified team. The team may include individuals from HR, IT, legal, compliance, risk management, and any organizational cybersecurity leaders. Make sure that the team defines its protocols around data collection, processing and storage, encryption, outsourcing, areas of risk, and breach notification and response, and ensure that its protocols are properly executed and updated in compliance with applicable laws. Designated plan fiduciaries should also provide input and adopt the Policy as part of its fiduciary best practices. If your organization does not have adequate in-house resources to develop a Policy, obtain qualified outside assistance.

Identify the data. Define the types of data that are at issue, and set parameters regarding their maintenance and security. Employee benefit plans store extensive personally identifiable information ("PII") for participants and beneficiaries, such as Social Security numbers, addresses, dates of birth, and financial information. Such information may be accessed by various personnel and service providers, which makes it vulnerable to data breaches. Further, depending on the type of benefit plan program, privacy and security may require vetting through different channels. For example, the use or disclosure of protected health information ("PHI") will need to comply with Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy and security policies (and electronic transmission of health information will need to comply with the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009). This can become further complicated when participants use health-tracking wearable tools, which interact with health plans—the plan may need a business associate agreement with cloud or storage providers receiving PHI. With a retirement investment advice tool, plan fiduciaries should undertake due diligence of its privacy and security measures to protect PII.

Train employees. Ensure that all personnel who have access to employee data are properly trained in safeguarding it, including securing the transmission of any data to third-party service providers. Designate individuals to respond to any benefits-related data breach and follow procedures for reporting breaches through the appropriate channels of the organization. Properly vet internal personnel handling this data, and take measures to protect against security breaches from within the company.

Develop additional standards for selecting and monitoring service providers. Establish cybersecurity guidelines for engaging, monitoring, and renewing service providers, such as confirmation of their cybersecurity program and certifications, details regarding how they encrypt and protect data, their breach notification procedures, and a review of Service

Organization Control reports regarding their privacy and security controls, levels of insurance, and scope of their assumption of liabilities. Understand whether the service provider utilizes agents or subcontractors to perform the services and the chain of security measures. Establish rules for any IT security review of service provider systems, including requests for penetration tests to detect security risks. Address data privacy and security, breach notification procedures, liability, and indemnification provisions in service agreements in accordance with the standards of the organization's Policy.

Address data interactions. Understand how data is accessed by participants and third parties, such as through online access or requests for retirement account distributions or transfers. If not already doing so, request that the service provider utilize enhanced measures such as two- or even three-step authentication for participants to access to the information. Consider having the service providers generate and issue more complex usernames and passwords, as participants frequently use the same passwords and usernames across different websites. Consider setting up alerts for unusual behavior. Also, educate employees on the steps they can take to protect their benefit plan information.

Review security of mobile apps. Many new mobile apps allow plan participants to check account balances, contributions, and investment changes; request loans or distributions; and receive alerts and educational information. Apps also track financial and physical wellness, and collect and convey such information to benefit plans. Despite their convenience, however, the use of mobile apps provides yet another opportunity for data breaches or the actual theft of assets and benefit payments. Make sure that the Policy sets forth the protocols that should be followed when introducing apps into any benefits program.

Cybersecurity insurance. In addition to errors and omissions and fiduciary liability insurance policies, cybersecurity insurance has emerged in recent years and can offer various types of coverage, including coverage for certain disaster recovery and response assistance that can be triggered by a benefit plan upon a breach. Assess existing coverages to ascertain how cybersecurity insurance can fit with your employee benefits needs.

Conclusion

It is time to develop a prudent benefit plan cybersecurity policy that will enable employers and plan fiduciaries to face challenges head-on and reduce potential liabilities.

5. Are Genetic Screening Benefits Truly Beneficial?

By Cassandra Labbees and Katie Smith

The tech industry is known for creativity, including its resourcefulness in offering enticing benefits to help employers effectively recruit and retain talent. Some of this creativity is stoked by a desire to combat higher-than-average employee mobility, and to accommodate a large percentage of millennial and Gen Z employees who, as a recent survey indicates, may value unique and plentiful benefits over pay raises. Creativity is also a function of access: many service providers are themselves tech companies, in close proximity with, and able to market effectively to, tech employers whose business mindsets already welcome experimentation.

This is certainly the case with genetic screening services, a trendy employee benefit made possible, in part, by tech startups that have reduced costs and increased direct-to-consumer availability of these tests through robotics, automation, and the app-made-easy delivery process.

The New York Times recently published an article highlighting the trend, which also addressed some of the unintended consequences of increased screening—namely, an unnecessarily heavy reliance on results that may create a false sense of security for individuals whose screens do not indicate a genetic predisposition to certain conditions, or may prompt unnecessarily drastic countermeasures (e.g., an elective double mastectomy) for individuals who may have a genetic marker for a condition but lack other factors like family history, which would make the condition more likely to manifest eventually. In fact, a study published in *Nature* recently found that as many as 40 percent of variants in certain genes reported by a direct-to-consumer test were false positives, including some benign variants marked as "increased risk."

These two stories highlight a potential dissonance for employers that choose to offer screening benefits. Preventative-care-focused health benefits generally appeal to both employers and employees alike because employers see them as a way to increase workers' productivity through improved health, while reducing the total cost of providing other benefits, such as health and life insurance, and employees see them as an opportunity to take advantage of a service that they might not otherwise want to purchase for themselves.

However, reliance on genetic screening results provided without nuanced interpretation from a genetic counselor may actually increase employer-provided health care costs, specifically for employers that sponsor self-insured health plans. Because some employees may opt for drastic surgical procedures as a preventative measure, the employer may increase its costs for these tests and procedures. Additionally, employees may take off more time from work for medical exams and surgery, creating additional costs for the employer.

Genetic screening can also create privacy and compliance concerns for employers charged with responsibilities under HIPAA, the Americans with Disabilities Act ("ADA") and, specifically concerning genetic information, the Genetic Information Nondiscrimination Act ("GINA"). The ADA prohibits employers from discriminating on the basis of disability or perceived disability, which can include genetic conditions, while GINA prohibits employers and health insurers from discriminating on the basis of genetic information, and bars employers from requesting genetic information from employees or prospective employees. Group health plans are also prohibited from collecting genetic information.

GINA does not apply to life insurance, long-term care, or disability insurance (although state laws may provide protections). As a result, these types of insurers can and do ask about health, family history of disease, or genetic information and may use the presence of certain genetic markers to limit coverage to individuals, even though they may not result in an actual disease. Thus, there is a concern that genetic testing results may lead to discrimination against individuals attempting to obtain these other types of insurance.

Employers that choose to offer genetic screening benefits can reduce their risk by taking several steps, such as offering the benefit via an independent third-party provider with appropriate data privacy and security procedures. Further, to ensure compliance with GINA and to avoid the appearance of discrimination on the basis of genetic information, employers should not seek to obtain employees' test results directly from the third-party provider (including aggregated, "sanitized" data), and should neither require nor encourage employees to share the results of their screening with the employer or their health plan.

Conclusion

Time will tell whether genetic screening benefits are a fad or destined to become part of the generally accepted preventative care standard. But for now, when properly administered in compliance with all applicable laws, they may have the wow factor that tech employers seek to appeal to their employees and potential hires.

* * * *

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:*

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

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

Andrea K. Douglas
Los Angeles
310-557-9527
adouglas@ebglaw.com

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

Nathaniel M. Glasser
Washington, DC
202-861-1863
nglasser@ebglaw.com

Cassandra Labbees
New York
212-351-4941
clabbees@ebglaw.com

Jeffrey M. Landes
New York
212-351- 4601
jlandes@ebglaw.com

Christopher Lech
New York
212-351-3736
clech@ebglaw.com

Alyssa Muñoz*
New York
212-351-4757
amunoz@ebglaw.com

Nancy Gunzenhauser Popper
New York
212-351- 3758
npopper@ebglaw.com

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

Katie Smith
Washington, DC
202-861-1882
kcsmith@ebglaw.com

Alyssa Muñoz, a Law Clerk – Admission Pending (not admitted to the practice of law) in the firm's New York office, contributed to the preparation of this* Take 5.

This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

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 locations throughout the United States and supporting domestic and multinational clients, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.

Attorney Advertising