EPSTEIN
BECKER
GREEN

Michelle Capezza

mcapezza@ebglaw.com

New York
Tel: 212-351-4774
Fax: 212-878-8600

- Join My LinkedIn Network
- Follow Me on Twitter
- Download My vCard
- Download My Resume

Upcoming Event

Boardrooms on Edge: HR's Role in Protecting Your Brand's Reputation – Epstein Becker Green's 37th Annual Workforce Management Briefing
October 25, 2018
New York, NY

More ›

News & Publications

AI in the Workplace: The Time to Develop a Strategy Is Now

HR Dive
August 23, 2017
Michelle Capezza, Adam S. Forman

Michelle Capezza, a Member of the Firm in the Employee Benefits and Health Care and Life Sciences practices, in the firm's New York office, and **Adam S. Forman,** Member of the firm in the Employment, Labor & Workforce Management practice, in the firm's Detroit and Chicago offices, authored an article in *HR Dive,* titled "AI in the Workplace: The Time to Develop a Strategy Is Now."

Following is an excerpt:

> When it comes to artificial intelligence (AI), or intelligence exhibited by machines, most people immediately think of cinema's sentient computers, such as HAL, Skynet or Samantha.
>
> Although those machines are just Hollywood's fictional creations, the underlying notion that AI will play an integral role in every aspect of our lives is very real indeed. With the exponential rate of technological change, AI will continue to affect our lives more quickly and pervasively than ever before. One area that is already being impacted is the workplace.
>
> From algorithms analyzing employee data, to computer and robotic laborers in retail and manufacturing, to the rise of the on-demand worker, AI has already disrupted how virtually every workplace operates. There is little doubt that the time to develop a workplace strategy is now. Some of the issues that organizations should consider as they introduce AI into the workplace include…

ISSUE 24, FALL 2018

CONFERO

MAGAZINE

EMPLOYEE BENEFITS

A quarterly publication of Westminster Consulting, LLC

DESIGNING EMPLOYEE BENEFITS TO ADDRESS EDUCATIONAL DEBT

Assisting Employees Reduce Educational Debt Through Employer-Provided Student Loan Repayment and Educational Assistance Programs

BY MICHELLE CAPEZZA, ESQ.

Michelle Capezza is an employee benefits and executive compensation attorney and a Member of EpsteinBeckerGreen, resident in their New York office. She can be reached at mcapezza@ebglaw.com and 212-351-4774.

It has been widely reported that student loan debt is at an all-time high, which in turn causes many workers financial stress and influences their decisions to delay family planning and home purchases. In addition, educational debt is often cited as a major reason why individuals are unable to save any additional compensation for retirement as well as meet their many immediate expenses. However, not only is educational debt an issue for young workers entering the workforce, but also it will become increasingly more prevalent as a financial stressor as more workers find themselves in the position of re-skilling for future jobs as a result of increasing automation and artificial intelligence in the workplace. With renewed attention to these issues, and overall financial wellness initiatives, student loan repayment and educational assistance programs have been garnering increased interest as employers consider new ways to expand their employee benefit programs in a manner that will provide meaningful benefits to workers.

Employers that desire offering a student loan repayment program or educational assistance program to their employees should consider the following:

1 Taxable Student Loan Repayment Benefits

To date, a small percentage of private-sector employers offer student loan repayment assistance for expenses incurred prior to employment, which is taxable and includible in wages under current law. However, interest in these types of programs is growing. There is no required design for this type of program, but some studies show that a typical payment offered may be $100 per month toward the principal balance of a student loan. There have been legislative proposals to exclude from gross income the amounts paid by an employer under student loan repayment assistance programs, but to date they have not moved forward (see e.g., the Student Loan Employment Benefits Act of 2016 (to exclude up to $5,000 per year from income) and the Student Loan Repayment Assistance Act of 2015 (to exclude up to $6,000 from income)).

Despite the current inclusion of this type of benefit in income, employees may still find this extra monthly payment attractive to assist in the repayment of their monthly student loan bills. Also, it provides increased wages without adjusting base salary per se because the income is specifically attributable to the student loan repayment program. Employers interested in offering this type of program have latitude in their design and should consider how they wish to define eligibility, the types of education and loans that qualify for repayment assistance, amount of the repayment, communications, and administrative issues and coordination with other financial wellness programs, including service providers in this space that can integrate and facilitate employer payments to the educational institutions.

2 Potential Coordination of Student Loan Repayment with Retirement Plan Savings

There has been interest in finding a way to coordinate student loan repayments with employer contributions to defined contribution plans, such as the 401(k) plan, in order to avoid the immediate inclusion of such contributions in income. Obvious hurdles have included

requirements to pass nondiscrimination and coverage tests for these plans and overall maintenance of qualified plan status. A recent private letter ruling has fueled renewed interest in the retirement plan integration approach.

In Private Letter Ruling 201833012, the IRS ruled that a 401(k) plan design allowing an employer to make a nonelective contribution for an eligible employee who makes a student loan payment under the program would not violate the contingent benefit rule under the tax code. These employees could also still make elective deferrals to the plan, but they would not be eligible for regular matching contributions; they would be eligible for the nonelective contribution and a true-up match. The employer also represented that it would not extend any student loans to employees eligible for the program. Notably, however, the ruling did not express an opinion on the federal tax consequences of any aspect of the issues referenced in the letter, and no opinion whether the plan satisfies the qualified plan requirements under the code.

This ruling has garnered widespread interest and more developments on this front are anticipated.

Employers interested in exploring similar plan design options should consider obtaining their own private letter ruling since such rulings may only be relied on by the applicant. Further, the approach should be vetted with service providers that conduct applicable testing for the plan to project passage of such tests. A request for a determination letter as to the qualified status of individually designed plans with such a feature would also be prudent, pending the IRS' status of such review programs or acceptance by the IRS for review of the plan as a new approach to plan design. Employers should also monitor future legislation that could potentially amend the tax code and provide a means for such integrated programs.

“EMPLOYEES WILL FIND PROGRAMS RELATED TO STUDENT LOAN REPAYMENT OR EDUCATIONAL ASSISTANCE ATTRACTIVE AND BENEFICIAL.”

3 Qualified Educational Assistance Programs

Under tax code Section 127, employers can offer employees educational assistance tax-free up to $5,250 per calendar year pursuant to a written program. The assistance can include reimbursement for tuition, fees and books as well as for graduate-level courses. The program must also pass applicable nondiscrimination tests. Employers can design their programs to reimburse the employee for qualified expenses, directly make payment to the educational institution, and/or the employer can provide the education to the employee. The educational assistance does not necessarily have to be work-related under these programs, but it cannot be for a sport, game or hobby unless reasonably related to the employer’s business or required as part of a degree program.

These programs do not address existing student debt incurred prior to the time of employment with the employer. It will be important to monitor legislative proposals in this regard that could serve to address extension of these types of programs to existing loans. There have been legislative proposals to increase the amount of tax-free tuition assistance, which to date have not moved forward (see e.g., the Upward Mobility Enhancement Act of 2017 (to exclude up to $11,500 of tuition assistance per calendar year)).

4 Working Condition Fringe Benefits

Under tax code Section 132, working condition fringe benefits, which are property or services to an employee that an employee could otherwise have deducted from income, are not included in gross income. These may include educational costs that maintain or improve required skills or are a condition to maintain a particular job as defined under tax code Section 162 and regulations thereunder. Expenses to meet minimum educational requirements of the individual’s current business or as part of a program to qualify the individual for a new business would not qualify. Employers that can provide educational benefits that meet these tax code requirements may be able to provide such benefits on a tax-free basis.

Employers should carefully consider working condition fringe benefits as they introduce automation and artificial intelligence into the workplace. As it becomes increasingly more important for certain employees to re-skill and re-tool to work alongside machines, employer provision of the requisite education to perform these new jobs may qualify as a working condition fringe benefit.

Certainly, employees will find programs related to student loan repayment or educational assistance attractive and beneficial. Employers interested in offering these types of benefits should consider the available approaches under current law, communicate programs in a meaningful way, and monitor ongoing developments as new methods emerge in this trending area.

Confero Fall 2018: Employee Benefits
Used with permission of
Westminster Consulting, LLC

EPSTEIN
BECKER
GREEN

Technology Employment Law

Legal Insight for Technology, Media, and Telecommunications Employers

Illinois Experiences Surge of Lawsuits Regarding Biometric Information Privacy

By Adam S. Forman, Nathaniel M. Glasser & Maxine Adams on November 1, 2017

POSTED IN CYBER SECURITY AND INSIDER THREAT MANAGEMENT, EMPLOYMENT LITIGATION

Employers continue to incorporate the use of biometric information for several employee management purposes, such as in systems managing time keeping and security access that use fingerprints, handprints, or facial scans. Recently, Illinois state courts have encountered a substantial increase in the amount of privacy class action complaints under the **Illinois Biometric Information Privacy Act** ("BIPA"), which requires employers to provide written notice and obtain consent from employees (as well as customers) prior to collecting and storing any biometric data. Under the BIPA, the employer must also maintain a written policy identifying the "specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used." **740 ILC 14/15**(b)(2).

Although the BIPA was enacted almost 10 years ago, individuals did not start filing lawsuits until 2015. Since September 2017, there have been over twenty-five new filings in Illinois state courts including class actions against prominent international hotel and restaurant chains. These lawsuits tend to target employers utilizing finger print recognition machines as part of their time keeping systems. Where the employer uses a third-party supplier for its time-tracking system, the claims have also included allegations that the employer improperly shared the biometric information with the supplier without obtaining the proper consent. In these cases, the claims generally allege that the employer failed to provide proper notice.

Though there is no definitive reason for the increase in filings over the past months, the claims may be related to the increased use of biometric information in the workplace since the initial case filings in 2015. While **Texas** and **Washington** also have laws governing employer use of biometric information, Illinois is the only state that currently provides a private right of action, including class actions. Additionally, potential damages associated with BIPA violations, particularly for class actions, can be extensive, including liquidated damages of $1,000 per negligent violation (or the amount of actual damages, whichever is greater), liquidated damages of $5,000 per intentional or reckless violation (or the actual damages, whichever is greater) and attorney's fees.

What Can Employers Do?

- Prior to collecting or storing biometric data, employers in Illinois should: (1) create a written policy regarding the retention and destruction of biometric data; (2) obtain written acknowledgment and release from the employees; and (3) store the biometric information securely, similar to other confidential information, such as personal health information or personally identifiable information.
- Employers who use a third party to assist with the collection or storage of biometric data should include the third party in the acknowledgement and release, which employees execute.
- Employers also should be aware that most states, including **Illinois**, have legislation governing how employers respond to data breaches and the required notifications to employees. If a data breach occurs, employers are advised to immediately contact counsel to devise and implement a response plan.
- In the event of litigation, employers should remove BIPA cases to federal courts when possible, particularly where the allegations focus on notice and consent issues, as employers can argue that plaintiffs cannot establish the necessary harm to establish

standing as required by the Supreme Court case ***Spokeo, Inc. v. Robins*****, 136 S. Ct. 1540 (2016)** (requiring more than a "bare procedural violation" to establish harm). Because employees likely will have difficulty establishing actual harm where the biometric data was stored in a confidential and secure manner, employers may be successful in getting such claims dismissed.

As the laws regulating biometric data continues to evolve, employers should monitor this issue closely and consult with counsel as further developments occur to ensure compliance with any relevant regulations.

Technology Employment Law

EPSTEIN
BECKER
GREEN

Adam S. Forman

aforman@ebglaw.com

Detroit
Tel: 248-351-6287
Fax: 248-351-2699

Chicago
Tel: 312-499-1468
Fax: 312-277-2376

Join My LinkedIn Network

Download My vCard

Download My Resume

Upcoming Event

Boardrooms on Edge: HR's Role in Protecting Your Brand's Reputation – Epstein Becker Green's 37th Annual Workforce Management Briefing
October 25, 2018
New York, NY

More ›

News & Publications

Minimize Risks When Using Big Data Analytics in Hiring

SHRM.org
July 12, 2018
Adam S. Forman, Nathaniel M. Glasser, Matthew Savage Aibel

Adam S. Forman, Nathaniel M. Glasser, and **Matthew Savage Aibel,** attorneys in the Employment, Labor & Workforce Management practice, co-authored an article in *SHRM.org,* titled "Minimize Risks When Using Big Data Analytics in Hiring."

Following is an excerpt:

> Despite the many advantages of "big data" analytics, employers must be ready to manage the potential risks, particularly when hiring.
>
> 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. HR departments increasingly consider whether and how to incorporate big data tools into their hiring processes.
>
> The promise offered by big data analytics 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. ...
>
> Before 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.

EPSTEIN
BECKER
GREEN

Recruitment and Selection in the Digital Age

Presented to:

The American Employment Law Council
26th Annual Conference

The Breakers, Palm Beach, Florida
October 12, 2018

Adam S. Forman, Esq.*
Epstein, Becker & Green, P.C.
AForman@ebglaw.com

2000 Town Center, Suite 1900 | Southfield, MI 48075
248.351.6287

227 W. Monroe Street, Suite 3250 | Chicago, IL 60606
312.499.1468

in @Adam Forman
t @AdamSForman

* The author acknowledges the contributions of Nathaniel Glasser, Member, and Katherine Smith, Associate, Epstein, Becker & Green, P.C.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Regulations

I. INTRODUCTION

What is the most efficient and effective way to recruit and retain the best employees? Recruiters, talent acquisition professionals, human resources generalists, and hiring managers have grappled with this question for years. A host of technologies introduced over the past several years aim to answer this age-old question definitively. The technologies are premised on the simple notion that recruiting and selecting new employees are time-consuming and expensive processes, and companies have a vested interest in making the best possible decisions the first time, every time, to maximize the return on their investment.

This paper offers a primer on the ways in which recruitment and selection technologies have begun reshaping how companies think and go about sourcing and hiring candidates. At the outset, the paper defines some of the key terms and phrases used with respect to these technologies, sets forth some of the current trends in recruitment and identifies some of the more well-known vendors in this space. Next, the paper examines some of the legal issues that companies should consider before or during the process of implementing recruitment and selection technologies. Finally, the paper provides several recommended steps to mitigate potential legal risk attendant with using these technologies, as well as a sample checklist of considerations when deciding which solution makes the most sense for a given organization and its needs.

II. DEFINITIONS, TRENDS AND VENDORS

A. Definitions

As the digitally driven recruitment and selection industry continues to evolve, terms used to describe the functions and services provided by vendors in this space are not always uniform. Often, individuals use similar, but technically different words, interchangeably (e.g., "artificial intelligence" ("AI") and "machine learning" ("ML")). The intent of the following definitions is to give the reader a simplified foundation for understanding the new recruitment and selection technologies.

Term	Definition(s)
Algorithm	Unambiguous specification of how to solve a class of problems, through calculation, data processing and automated reasoning tasks.
Analytics	Discovery, interpretation, and communication of meaningful patterns in data. Relies on the simultaneous application of statistics, computer programming and operations research to quantify performance.
Applicant Tracking System ("ATS")	Software application that enables the electronic handling of recruitment needs.

Term	Definition(s)
Artificial Intelligence ("AI")	Intelligence demonstrated by machines. Machine mimicking "cognitive" functions that humans associate with other human minds, such as "learning" and "problem solving."
Big Data	Study and applications of data sets that are so big and complex that traditional data-processing application software are inadequate to deal with them. Use of predictive analytics, user behavior analytics, or certain other advanced data analytics methods that extract value from data, but seldom to a particular size of data set.
Candidate Relationship Management ("CRM")	Method for managing and improving relationships with current and potential future job candidates. Used to automate communication process with candidates, encourage engagement and improve candidate experience.
Chatbots (a.k.a. "talkbot," "chatterbot," "Bot," "IM bot," "interactive agent," or "Artificial Conversational Entity")	Computer program or an artificial intelligence that conducts a conversation via auditory or textual methods. Application that runs highly repeated series of automated scripts with observable answers.
Data Mining	Process of discovering patterns in large data sets involving methods at the intersection of machine learning, statistics, and database systems.
Human Capital Management ("HCM")	Comprehensive set of practices for recruiting, managing, developing and optimizing the human resources of an organization.
Machine Learning ("ML")	Field of computer science that uses statistical techniques to give computer systems the ability to "learn" (e.g., progressively improve performance on a specific task) with data, without being explicitly programmed. Process by which machines learn to become intelligent for themselves.
Natural Language Processing ("NLP")	Area of computer science and artificial intelligence concerned with the interactions between computers and human (natural) languages, in particular how to program computers to process and analyze large amounts of natural language data.
People Analytics (a.k.a. "talent analytics" or "HR analytics")	Method of analytics that can help managers and executives make decisions about their employees or workforce.

Term	Definition(s)
Predictive Analytics	Variety of statistical techniques from data mining, predictive modelling, and machine learning, that analyze current and historical facts to make predictions about future or otherwise unknown events. Provides a predictive score (probability) for each individual (e.g., prospective employee) in order to determine, inform, or influence organizational processes that pertain across large numbers of individuals.
Recruitment Marketing	Strategies and tactics an organization uses to find, attract, engage, and nurture talent before they apply for a job, also called the pre-applicant phase of talent acquisition.
Robotic Process Automation ("RPA")	Emerging form of business process automation technology based on the notion of software robots or artificial intelligence workers. Readily available script writing technologies that allow users to link events in a process based on "if/then" statements.

B. Recruiting and Hiring Trends

Performing a simple search on one's favorite internet browser quickly reveals that AI, big data and data analytics are amongst the top trends in recruitment for 2018.[1] According to the 2018 Deloitte Global Human Capital Trends report, "[l]eading companies increasingly recognize that [AI] technologies are most effective when they complement humans, not replace them."[2] That report notes that seventy-two percent of its respondents rate "AI, robotics, and automation" trends as "very important or important," with only thirty-one percent reporting that their organization is "very ready or ready" to meet expectations in those areas. Forty-seven percent report that their organizations are "deeply involved in automation projects," while twenty-four percent claim to use AI and robotics to "perform routine tasks," sixteen percent use AI to "augment human skills," and seven percent use AI to "restructure work entirely."[3] Finally, forty-two percent of respondents – an increase of four percent from 2017's Report – predict, "AI will be widely deployed at their

[1] *See*, *e.g.*, *2018 Recruitment Trends According to Experts*, *available at* https://gethppy.com/hr-infographics/2018-recruitment-trends-according-to-experts (last visited on September 12, 2018); *10 Recruiting Trends in 2018*, *available at* https://www.talentlyft.com/en/blog/article/114/10-recruiting-trends-in-2018-infographic (last visited on September 12, 2018); and *Six Top Recruiting Trends*, *available at* http://www.humanresourcestoday.com/2018/recruitment/trends/?open-article-id=7985508&article-title=six-top-recruiting-trends&blog-domain=hr-gazette.com&blog-title=hr-gazette (last visited on September 12, 2018).

[2] DELOITTE UNIV. PRESS, REWRITING THE RULES FOR THE DIGITAL AGE: 2018 DELOITTE GLOBAL HUMAN CAPITAL TRENDS 74 (2018), *available at* https://bit.ly/2q3DSsx (last visited on September 12, 2018).

[3] *Id.* at 73.

organizations within three to five years."[4] In all, the Deloitte found that more than 1,000 AI-based start-ups have invested over $6 billion over the past three years, including those in the HR field.[5]

Likewise, in its recent "2018 Global Recruiting Trends" report, LinkedIn surveyed over 9,000 global talent leader and hiring managers and identified the following four trends shaping the future of recruiting and hiring: (1) diversity; (2) new interviewing tools; (3) data; and (4) artificial intelligence.[6]

With respect to "new interviewing tools," fifty-six percent of talent professionals and hiring managers reported to LinkedIn that new interview tools are the top trend affecting how they hire. The new tools most frequently cited were online soft skills assessments that measure traits like teamwork and curiosity and give a more holistic picture of candidates earlier in the process. Employers are also using virtual reality by immersing candidates in simulated three-dimensional environments to test their skills in standardized ways. Video interviews – live or recorded – are also very popular, because employers believe they help in tapping a broader talent pool in far less time.[7]

That LinkedIn found that employers are using data to inform their decisions, in and of itself, is not new. What is new, however, is the *volume* of data available and the *speed* with which computers can analyze it, as well as the way that computers use data to *predict* hiring outcomes, not just track them. Perhaps that is why fifty percent of those surveyed said that data is the top trend influencing how they hire. According to LinkedIn, top uses for data in talent acquisition include to: (1) increase retention (56%); (2) evaluate skills gaps (50%); (3) build better offers (50%); (4) understand candidate wants (46%); (5) do workforce planning (41%); (6) predict candidate success (39%); (7) assess talent supply and demand (38%); (8) compare talent metrics to competitors' (31%); and (9) forecast hiring demands (29%).[8]

Over a third – thirty-five percent – of talent professional and hiring managers reported to LinkedIn that AI was the top trend affecting how they hire. Use cases, however, were less clear amongst respondents, as AI's utility appeared to decrease as the complexity of the recruiter-related task increased. For instance, whereas fifty-eight percent of those surveyed stated that they used AI for sourcing candidates, only six percent reported using AI for interviewing candidates. Rounding out the remaining top uses for AI in recruitment were: (1) screening candidates (56%); (2) nurturing candidates (55%); (3) scheduling candidates (42%); and (4) engaging candidates (24%). Building relationships with candidates, seeing candidate potential beyond credentials,

[4] *Id.*

[5] *Id.* at 74.

[6] *The 4 Trends Changing How You Hire in 2018 and Beyond*, *available at* https://business.linkedin.com/talent-solutions/blog/trends-and-research/2018/4-trends-shaping-the-future-of-hiring (last visited on September 12, 2018).

[7] *Id.*

[8] *Id.*

judging "culture fit," gauging candidate interpersonal skills, and convincing candidates to accept offers, were the skills least likely replaced by AI, according to respondents.[9]

Even though talent professional and hiring managers are not reportedly flocking to AI for their recruiting and selection needs, there is little doubt that AI will continue to play a prominent role in candidate sourcing and hiring going forward. AI's efficiencies in the hiring process are compelling from a business perspective. Pre-screening countless resumes with algorithms matching skills listed on the resumes with those require of the job, will save decision makers valuable time. Chatbots can also streamline the initial communication process by scheduling interviews with those candidates who pass the initial screening process. Where appropriate and lawful, AI can even perform certain background checks on candidates, including reviewing their social media activities. Theoretically, offloading these type of tasks will free up the human decision maker(s) to spend more time with a shortlist of qualified candidates, deserving of thoughtful consideration. Still up for debate is whether these technologies will ever eliminate the need for the personal touch, which is often critical to building relationships with potential recruits and attracting other quality candidates.

C. Sample Vendors

Dozens of vendors have entered (and quickly exited) the digital recruitment and selection space, offering services that in whole, or in part, seek to replicate the roles that humans play in sourcing employees. While each vendor's "secret sauce" may differ, each uses some form of a proprietary computer algorithm to gain insight into prospective candidates and job applicants and predict the best talent based on criteria that the technology is programmed to analyze. The following is a non-exhaustive list of vendors and a summary of their primary focus, demonstrating the broad range of services offered in this space.

Company/Website	Description of Service(s)
Burning Glass burning-glass.com	Skills-based approach uses "big data" techniques to help managers find applicants most likely to succeed. Also helps employers develop internal talent, allowing career advancement by showing employees necessary skills.
Ceridian cerdian.com	Flight risk assessment based on time-keeping data, embedded client performance.
Cornerstone OnDemand cornerstoneondemand.com	Talent management system providing recruitment, training, management and collaboration solutions.
Crowded crowded.com	Updates resumes in ATS with latest jobs, skills, location, certifications and education data, pulled from numerous sources using proprietary data-sourcing and validation algorithm. Matches, ranks and warms up best talent for open jobs.

[9] *Id.* *See also Sierra-Cedar HRTechnology Industry Survey*, *available at* https://www.sierra-cedar.com/research/annual-survey/ (last visited on September 12, 2018) (finding that fewer than seven percent of surveyed companies are using or considering using ML technologies in HR).

Company/Website	Description of Service(s)
Engage Talent engagetalent.com	AI-powered platform combining talent mapping, competitive intelligence, passive candidate sourcing, and outbound recruiting to enable recruiters to efficiently source from a live stream of over 100 million passive candidates or enrich their own CRM and ATS candidates with predictive, AI-based insights. Continuously monitors candidates and sends alerts with predictive availability signals when a candidate is likely ready for new opportunity.
Glint glintinc.com	Real-time employee surveys with predictive capacity.
HireMya hiremya.com	Bot supporting most time-consuming aspects of recruiting process, empowering recruiters to refocus efforts on value-added activities.
HireVue hirevue.com	Several products in the recruitment space, including on-demand video interviewing for asynchronous recorded interviews, recorded live video interviews, predictive assessments and real-time self-scheduling for candidates and event management.
Humanyze humanyze.com	People analytics platform that analyzes corporate communication data to understand how people work and benchmarks behaviors against organizational outcomes.
IBM Watson Recruitment ibm.com	AI powered cognitive talent management solution that increases recruiter efficiency to allow HR to improve and accelerate people's impact on the business. Automatically predicts best suited candidates who are most likely to succeed in an organization.
Karen karen.ai	Recruiting bot that assesses candidates by matching team personality and culture fit. Interacts with candidates via chat or SMS.
Koru joinkoru.com	Predictive hiring software that identifies an organization's performance drivers to increase high quality hires and reduces bias.
Leap leap.ai	Integrates technical and cultural fit for recruiting based on performance prediction.
LinkedIn Recruiter business.linked.com	Automates candidate searches to find quickly prospects matching an organization's criteria.
Montage Talent montagetalent.com	On-demand voice and video interviewing software allowing candidates to complete interviews on their own time. Interviews configured according to each job's requirements and skills.
MS Dynamics 365 dynamics.microsoft.com	Leverages the power of Office 365 and LinkedIn to quickly find and onboard the right people.
PhenomPeople phenompeople.com	Combines personalized career site experience to attract top talent with tools to make recruiters more efficient and provide talent leaders actionable insights into the recruiting funnel.
Pymetrics pymetrics.com	Applies proven neuroscience games and cutting edge AI to reinvent the way companies attract, select, and retain talent.
Scout goscoutgo.com	Data-driven way to connect employers and search firms to fill jobs with great talent.

Company/Website	Description of Service(s)
SmartRecruiters smartrecruiters.com	Recruiting solution using pattern detection for improved recruiting decisions.
Swoop swooptalent.com	Automatically connects organization's talent data and world's talent data to power everything organization needs to do with data across the full talent lifecycle, including integrations, data refresh, analytics, migrations, or machine learning.
TalVista talvista.com	Optimizes job descriptions, conducts redacted resume reviews and follows structured interview process. Enables team or company to be aware of and manage unconscious bias.
Textio textio.com	Augmented writing fueled by massive quantities of data, contributed by companies across industries and around the world. Predictive engine uses this data to uncover meaningful patterns in language, guiding employer to prepare more effective job ads.
Ultimate Software ultimatesoftware.com	Cloud provider of HCM solutions for HR, payroll, talent, compensation, and time and labor management that seamlessly connect people with information and resources needed to work more effectively.

III. LEGAL ISSUES

As set forth above, there is likely no putting the genie back into the bottle when it comes to the use of technology in recruitment and selection. To be sure, technologies offered by the vendors identified above offer significant advantages. Data-based hiring promises to help organizations efficiently sort through massive numbers of applicants, increase diversity and more accurately and effectively identify top talent and reduce attrition. Vendors also advertise the reduction in time and cost associated with the hiring process.

In practice, by reducing decision-making subjectivity, employers can cut back on the "affinity bias" that can steer managers to hire candidates like themselves.[10] This, in turn, will allow them to consider nontraditional candidates and solutions who they might otherwise have overlooked or ruled out.

There are, however, many significant legal risks attendant to using recruitment and selection technologies. On the other side of the possibility of identifying hidden biases is "the potential for incorporating errors and biases at every stage – from choosing the data set used to make predictions, to defining the problem to be addressed through big data, to making decisions based on the results of big data analysis."[11]

Before implementing a new recruitment or selection technology, employers and/or their legal counsel should consider several legal and ethical issues. Of course, these technologies are

[10] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: A REPORT ON ALGORITHMIC SYSTEMS, OPPORTUNITY, AND CIVIL RIGHTS 14 (2016), https://bit.ly/2lCSs8H.

[11] Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues, 25 (2016), https://bit.ly/1n52gG6.

developing more rapidly than the law. Consequently, the following are just some of the main issues that are ripe for consideration. Other legal issues will continue to evolve as the technologies become more widespread, are tested in the courts and/or examined by federal and state administrative agencies and legislatures.

A. Disparate Treatment

Title VII of the Civil Rights Act of 1964 ("Title VII") forbids employers from discriminating in any term or condition of employment on the basis of race, color, national origin, religion, or sex.[12] Among other things, Title VII specifically prohibits an employer from failing or refusing to hire any individual, because of the individual's protected characteristics.[13] Perhaps the single greatest legal risk to employers using recruitment and selection technologies is that the technologies, by their very design, provide decision makers with notice of protected characteristics about which they otherwise would not have been aware. Indeed, for years, enforcement agencies, such as the Equal Employment Opportunity Commission ("EEOC"), have encouraged employers to remove questions from their job applications that ask applicants to identify the years that they attended and/or graduated from high school or college. Such questions do not directly violate the Age Discrimination in Employment Act ("ADEA"),[14] but rather, an applicant could interpret them as a method of discriminating against applicants based on age.[15] Whereas most prudent employers comply with the EEOC's position and do not affirmatively ask applicants questions that would provide them with information regarding the applicant's protected characteristics, the use of technological solutions to recruit and select employees has arguably called into question those efforts.[16] Job seekers frequently share information online – in their professional profiles, social media sites and other online activities – that they would never voluntarily share with a prospective employer and which the prospective employer would never request.

Consider, for example, the vendors that offer video interviews at the first phase of the interview process to pare down the pool of individuals who will receive in-person interviews. A decision maker may learn not only the individual's gender and race, but she may also learn the individual's relative age, religion (e.g., by the garments worn) and the individual's mental or

[12] Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e, *et seq.*

[13] *Id.* at § 2000e-2.

[14] 29 U.S.C. § 621, *et seq. See also* 29 C.F.R. § 1625.5 ("A request on the part of an employer for information such as Date of Birth or age on an employment application form is not, in itself, a violation of the Act. But because the request that an applicant state his age may tend to deter older applicants or otherwise indicate discrimination against older individuals, employment application forms that request such information will be closely scrutinized to assure that the request is for a permissible purpose and not for purposes proscribed by the Act.").

[15] *See, e.g.*, EEOC, ALL STATUTES: PRE-EMPLOYMENT INQUIRIES (2004), https://www.eeoc.gov/eeoc/foia/letters/2004/all_statutes_inquiries.html.

[16] *See, e.g.*, *Neiman v. Grange Mut. Cas. Co.*, No. 11-3404, 2012 U.S. Dist. LEXIS 59180 (C.D. Ill., Apr. 27, 2012) (applicant put employer on notice that he was subject to protection of the ADEA where information on his LinkedIn account – which the employer requested – contained his college graduation year).

physical impairment (e.g., speech impediment). Applicants not hired may claim that the employer subjected them to disparate treatment based on their protected categories. Concededly, the risk of a disparate treatment claim for a hiring decision made using a video-based platform is similar to the risk inherent in any in-person interview. The primary difference appears to be the scope of potential claims. Whereas an in-person interview typically does not take place until after the hiring manager reviews candidate resumes or applications and narrows the pool of interviewees, with a video-based service, the hiring manager receives all of this information at the same time.

In addition, a candidate may be more likely to raise a disparate treatment claim if he or she suspects that the algorithm used by the employer incorporates intentionally discriminatory factors. One such example is vendor algorithms that purportedly analyze an organization's own past performance and hiring data to predict the candidate(s) who will be the "best fit" for the position. Where the employer provides the vendor with biased data – either explicitly or implicitly – the outcome from the vendor will likely similarly be suspect. As they say, garbage in, garbage out. Another example is vendor algorithms that account – either positively or negatively – for linguistic or behavioral differences that might implicate one's age, sex, national original, race, regional dialect, or mental or physical impairment. Similarly, algorithms that purport to correct job advertisements so that they are more attractive to members of one protected category, rather than others, are also potentially problematic. Efforts to increase the diversity of one's candidate pool may be legitimate and lawful, but intentionally crafting a job advertisement so that it attracts more women, for instance, could be unlawful disparate treatment. Arguably, such job advertisements are analogous to the "micro-targeting" which is presently at issue in litigation alleging that companies are unlawfully limiting the audience for their employment ads on Facebook.[17]

[17] *See Bradley v. T-Mobile US, Inc.*, No. 5:17-cv-07232-BLF (N.D. Cal. filed Dec. 20, 2017). In *Bradley*, the Communications Workers of America and several named plaintiffs sued T-Mobile, Amazon.com, Cox Communications, and "a Defendant Class of hundreds of major American employers and employment agencies" alleging that defendants "routinely exclude older workers from receiving their employment and recruiting ads on Facebook, and thus deny older workers job opportunities." *Id.* The putative plaintiffs' claims rely, in part, on a targeted Facebook post from T-Mobile that, when expanded, explains that the recipient may be seeing the ad because "T-Mobile Careers wants to reach people ages 18 to 38 who live or were recently in the United States." Second Amended Complaint ¶2. Putative plaintiffs also cite a post from Facebook, acting as an employer, stating that the viewer may be seeing the ad because "Facebook Careers wants to reach people ages 21 to 55 who live or were recently in the United States." Second Amended Complaint ¶ 3. Without admitting liability or wrong-doing, in July 2018, Facebook entered into an agreement with Washington State pursuant to which it agreed to "make significant changes to its advertising platform by removing the ability of third-party advertisers to exclude ethnic and religious minorities, immigrants, LGBTQ individuals and other protected groups from seeing their ads." Washington State Office of the Attorney General, *AG Ferguson Investigation Leads to Facebook Making Nationwide Changes to Prohibit Discriminatory Advertisements on its Platform* (July 24, 2018), *available at* https://www.atg.wa.gov/news/news-releases/ag-ferguson-investigation-leads-facebook-making-nationwide-changes-prohibit (last visited on September 10, 2018). Subsequently, in August 2018, Facebook announced that it would eliminate five thousand customization options related to "sensitive personal attributes" enabling advertisers on its platform to limit their recipient audiences. https://www.facebook.com/business/news/keeping-advertising-safe-and-civil. More recently, on September 18, 2018, the American Civil Liberties Union ("ACLU") filed a charge with the EEOC alleging that Facebook discriminated against older women and gender-nonbinary job-seekers by allowing employers to use its services to

Similarly, if the algorithm uses linguistic differences as a proxy for race or national origin, for instance, the employer may face a disparate treatment claim.

B. Disparate Impact

While many companies are motivated, at least in part, to utilize recruitment and selection technologies in order to reduce subjectivity in the process, and thereby reduce the risk of disparate treatment claims, companies must be aware of the risks of potential disparate impact claims. In addition to prohibiting employers from disparately treating individuals based on their protected characteristics, Title VII, the ADEA, and the ADA also prohibit the use of facially neutral procedures that have a disparate impact, or disproportionately exclude people in a protected group, under certain circumstances.[18] Recruitment and selection technologies can raise particular issues in disparate impact discrimination challenges due to the large number of potential applicants and the statistical power or large populations and sample sizes.[19] In addition, these technologies often incorporate information far removed from the workplace, instead finding significance in the correlation – as opposed to causation – between non-worked-related data and various measures of job performance. Thus, an algorithm developed based on "successful" incumbents may incorporate neutral and non-discriminatory characteristics common to that population of employees, but those that are not necessarily important to job performance. Likewise, those programming the algorithms can embed their biases and values into the software's instructions.[20]

To establish a disparate impact claim under Title VII, for instance, a plaintiff must first: (1) identify with particularity the facially neutral practice being challenged; (2) demonstrate that the practice adversely impacts members of the protected group in question; and (3) shows that the

target job advertisements to younger men. *See* https://www.aclu.org/legal-document/facebook-eeoc-complaint-facebook (last visited on September 18, 2018).

[18] Title VII, 42 U.S.C. § 2000e-2(k); ADA, 42 U.S.C. § 12112(b)(6); and ADEA, 29 U.S.C. § 624(a)(2)**.** *See also Griggs v. Duke Power Co.*, 401 U.S. 424 (1971). Note, however, that claims of disparate impact against persons with disabilities are less likely, inasmuch as that group is often diverse in the mental or physical impairment that substantially limits one or more of their major life activities.

[19] While employees may assert disparate impact claims under the ADEA, whether older *applicants* may do so remains an open question. In *Villarreal v. R.J. Reynolds Tobacco Co.*, 839 F.3d 958 (11th Cir. 2016), a full panel of the Eleventh Circuit held that the ADEA does not permit a job applicant to sue an employer for using a practice that has a disparate impact on older workers. Parsing the language of the ADEA, the Eleventh Circuit concluded that the statutory language allows only *employees* to bring adverse impact claims; because applicants are not employees, they cannot assert disparate impact claims. *Id.* at 964. In the Seventh Circuit, a three-judge panel held that the ADEA does protect outside job applicants, *Kleber v. CareFusion Corp.*, 888 F.3d 868 (7th Cir. 2018), but the court has since vacated that decision and will consider the issue *en banc*. *Kleber v. CareFusion Corp.*, No. 17-1206, 2018 U.S. App. LEXIS 17148 (7th Cir., June 22, 2018). There are, however, federal district court decisions that have held that applicants may proceed with age discrimination claims under a disparate impact theory. *See, e.g.*, *Rabin v. PricewaterhouseCoopers LLP*, No. 16-cv-2276, 2017 U.S. Dist. LEXIS 23224 (N.D. Cal., Feb. 17, 2017).

[20] *See generally* Solon Barocas & Andrew D. Selbst, "*Big Data's Disparate Impact*," 104 CALF. L. REV. 671 (2016); Danielle Keats Citron & Frank A. Paxquale, "*The Scored Society: Due Process for Automated Predictions*," 89 WASH L. REV. 1 (2014).

practice caused the plaintiff to suffer an adverse employment action. The fact that a selection procedure has a disparate impact on a protected class does not automatically create liability for an employer. Pursuant to Title VII, it is not "an unlawful employment practice for an employer to give and to act upon the results of any professionally developed ability test provided that such test . . . is not designed, intended or used to discriminate."[21] Once the plaintiff meets the initial burden of establishing a *prima facie* case, the employer may defend against a claim of disparate impact discrimination by demonstrating that the practice in question is job-related and consistent with business necessity.[22]

Whether a test or selection method that produces an adverse impact is lawful under Title VII is often decided with reference to the Uniform Guidelines on Employee Section Procedures ("Uniform Guidelines"),[23] which have been jointly adopted and issued by the EEOC, the Civil Service Commission, the U.S. Department of Labor ("DOL"), and the U.S. Department of Justice ("DOJ"). The EEOC applies the Uniform Guidelines in the enforcement of Title VII and the DOL and the Office of Federal Contract Compliance Programs ("OFCCP") apply the Uniform Guidelines with respect to federal contractors in the enforcement of Executive Order 11246. The Uniform Guidelines provide employers with guidance about how to determine if their tests and selection procedures are lawful under Title VII and nondiscrimination theories.

The Uniform Guidelines consider discriminatory any selection procedure used as a basis for making employment decisions, including hiring decision that has an adverse impact on members of any racial, gender, or ethnic group unless it has been validated in accordance with the Uniform Guidelines.[24] Validation requires a showing that: (a) the content of the procedure is representative of important aspects of job performance ("content validity"); (b) the procedure measures the degree to which candidates have identifiable characteristics which have been determined to be important for successful job performance ("construct validity"); or (c) the procedure is predictive of, or significantly correlated with, important elements of work behavior ("criterion-related validity").[25]

[21] 42 U.S.C. § 2000e-2(k). *See also Griggs*, 401 U.S. at 436 (holding that employment selection instruments are non-discriminatory, provided that the employer demonstrates that they are "demonstrably a reasonable measure of job performance").

[22] 42 U.S.C. § 2000e-2(k).

[23] 29 C.F.R. Part 1607, http://www.gpo.gov/fdsys/pkg/CFR-2014-title29-vol4/xml/CFR-2014-title29-vol4-part1607.xml.

[24] 29 C.F.R. § 1607.3(A). The Uniform Guidelines, however, do not apply to discrimination based on age under the ADEA or based on disability under the Rehabilitation Act, 29 U.S.C. § 701 et seq., or the ADA, 42 U.S.C. § 12112. 29 C.F.R. § 1607.2(D).

[25] *See generally* 29 C.F.R. § 1607.5 (identifying criterion, content and construct as the three types of validation evidence that may be used to prove the validity of selection procedures). Unlike in disparate impact case under Title VII, in a disparate impact case under the ADEA, the employer need only prove that its practice is a "reasonable factor other than age," not "business necessity." 29 U.S.C. § 623(f)(1); *see also Smith v. City of Jackson*, 544 U.S. 228

Demographic information must be solicited from all applicants for which a pre-employment skills assessment is utilized. But in the context of selection procedures, there is a tension between the definitions of "applicant" utilized by EEOC and OFCCP. Initially, the four agencies that issued the Uniform Guidelines agreed that an "applicant" was a person who indicated an interest in being considered for hiring, promotion, or other employment opportunities, and who had not voluntarily withdrawn themselves from consideration.[26] The EEOC has continued to adhere to this broad view of the term "applicant."[27] The OFCCP, however, has adopted the Internet Applicant Rule, under which an "internet applicant" is defined as someone who satisfies all four of the following criteria:

> (1) the individual submitted an expression of interest in employment through the Internet or related electronic data technologies;
>
> (2) the contractor considered the individual for employment in a particular position;
>
> (3) the individual's expression of interest indicated that the individual possesses the basic qualification for the position; and
>
> (4) the individual, at no point in the contractor's election process prior to receiving an offer of employment from the contractor, removed himself or herself from further consideration or otherwise indicated that he/she was no longer interested in the position.[28]

In other words, under the EEOC's definition, applicants include any person who has expressed interest in a position, whereas the OFFCP's definition excludes individuals who do not meet the "basic qualifications" of the position. Employers must be cognizant of these different definitions when performing an adverse impact analysis and/or conducting a validation study.

Even when the employer establishes the "validity" of the test or selection procedure, a Title VII plaintiff may still prevail by proving there is a less discriminatory alternative that similarly serves the employer's needs, but which the employer refuses to adopt.[29] Likewise, the Uniform Guidelines also require an employer to consider whether there are less discriminatory alternatives to any selection procedure.[30]

(2005). Accordingly, to avoid liability once an ADEA plaintiff has proved a *prima facie* case, the employer must establish the reasonableness of its reliance on other neutral criteria.

[26] Adoption of Questions and Answer to Clarify and Provide a Common Interpretation of the Uniform Guidelines on Employee Selection Procedures, 44 Fed. Reg. 11996, 11998 (Mar. 2, 1979), *available at* http://www.eeoc.gov/policy/docs/qanda_clarify_procedures.html.

[27] *Id.*

[28] 41 C.F.R. § 60-1.3 (Feb. 6, 2006).

[29] 42 U.S.C. § 2000e-2(k).

[30] 29 C.F.R. § 1607.3(B). Title VII, on the other hand, assigns this burden of proof to the plaintiff. *Compare Ricci v. DeStefano*, 557 U.S. 557, 632 n.11 (2009) ("Under the [Uniform Guidelines], employer must conduct 'an investigation

The practical concern with the use of predictive analytics in selection procedures is that they may increase the risk of class certification for any claims of disparate impact. Because a single algorithm is applied across a large number of applicants – no matter how that term is defined – the algorithm may provide the "common questions of law or fact" necessary for a class to be certified under Federal Rule of Civil Procedure 23.[31] Importantly, employers cannot escape liability for such claims by outsourcing the technologies to external vendors, as employers are responsible for actions taken by external vendors on their behalf.

These issues will continue to grow in importance, as the EEOC continues to pursue a program to address systemic discrimination, which includes efforts to bring class-action claims challenging the use of uniform policies, tests or other employee selection procedures that allegedly have a statistically significant disparate impact and insufficient business necessity justification.[32] Additionally, the EEOC's commitment to its E-RACE (Eradicating Race and Colorism from Employment) program and the priorities outlined in its 2017-21 Strategic Enforcement Plan and 2018-2022 Strategic Plan indicate it is likely to continue to aggressively pursue the issue.[33]

C. Persons With Disabilities

Much like disparate impact challenges, the ADA also poses special challenges for employers considering using recruitment and selection technologies, because that statute imposes affirmative obligations on employers with respect to the screening and hiring process.[34] In addition, the ADA requires employers to provide reasonable accommodations to qualified

of suitable alternative selection procedures.' 29 C.F.R. § 1607.3(B)") *with* 42 U.S.C. § 2000e-2(k). *See Ricci*, 557 U.S. at 578 (citing 42 U.S.C. § 2000e-2(k)(1)(A)(ii) and (C)) ("[A] plaintiff may still succeed by showing that the employer refuses to adopt an available alternative employment practice that has less disparate impact and serves the employer's legitimate needs.").

[31] *See Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551-52 (2011) (recognizing the need for some "glue" that holds together class members' claims for relief and produces a common answer to a single question).

[32] *See* EEOC, ADVANCING OPPORTUNITY: A REVIEW OF THE SYSTEMIC PROGRAM OF THE U.S. EEOC (July 7, 2016), *available at* https://www.eeoc.gov/eeoc/systemic/review/index.cfm; EEOC, CSX Transportation to Pay $3.2 Million to Settle EEOC Disparate Impact Sex Discrimination Case (June 13, 2018), *available at* https://www.eeoc.gov/eeoc/newsroom/release/6-13-18.cfm; EEOC, Amsted Rail to Pay $4.4 Million After Court Ruled It Used Discriminatory Hiring Practices (June 12, 2018), *available at* https://www.eeoc.gov/eeoc/newsroom/release/6-12-18.cfm.

[33] EEOC, U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, STRATEGIC ENFORCEMENT PLAN, FISCAL YEARS 2017-2012, https://www.eeoc.gov/eeoc/plan/sep-2017.cfm; EEOC, U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, STRATEGIC ENFORCEMENT PLAN, FISCAL YEARS 2018-2022, https://www.eeoc.gov/eeoc/plan/strategic_plan_18-22.cfm.

[34] 29 C.F.R. § 1630.11 (It is unlawful for employers "to fail to select and administer tests concerning employment in the most effective manner to ensure that, when a test is administered to a job applicant or employee who has a disability that impairs sensory, manual or speaking skills, the test results accurately reflect the skills, aptitude, or whatever other factor of the applicant or employee that the test purports to measure, rather than reflecting the impaired sensory, manual, or speaking skills of such employee or applicant. . . .")

applicants with known physical or mental limitations, unless doing so would cause an undue hardship to the employer.[35]

From an ADA perspective, one issue with recruitment and selection technologies is that they frequently analyze an individual's voluntary activities, which may not be related to any work requirements, and because applicants may not necessarily be aware that those activities are being considered for a given job. Consider an algorithm that creates a positive correlation between individuals belonging to a gym and successful employees. A person with a disability may not belong to a gym, but that criterion may have absolutely nothing to do with his or her ability to perform the essential functions of the job, with or without a reasonable accommodation. Yet, the question, in and of itself, might exclude such a candidate in the initial screening. Stated simply, an applicant who is disabled who is subject to a recruitment or selection technology may have no reason – of which they know – to request a reasonable accommodation. Compounding the problem is that the prospective employer may have no notice that the applicant has an impairment requiring an accommodation.

Another issue is that several of the vendors offer algorithms that perform personality tests[36] to help better predict the best-qualified candidates for the job. Under the ADA, if the personality test constitutes a "disability-related inquiry" or a "medical examination," it may only take place *after* the employer gives a conditional job offer to the applicant.[37] According to the EEOC, a "disability-related inquiry" is a "question or series of questions that is likely to elicit information about a disability."[38] The EEOC defines a "medical examination" as "a procedure or test that seeks information about an individual's physical or mental impairments or health."[39] A test may be a considered a medical examination if it is: (1) administered by a health care professional; (2)

[35] 42 U.S.C. § 12112(b)(5); 29 C.F.R. § 1630.9(a) ("It is unlawful for a covered entity not to make reasonable accommodation to the known physical or mental limitations of an otherwise qualified applicant or employee with a disability, unless such covered entity can demonstrate that the accommodation would impose an undue hardship on the operation of its business.").

[36] A personality test is one of the several types of psychological tests identified by the American Psychological Association. *See Testing Issues*, American Psychological Association, http://www.apa.org/topics/testing (last visited on September 10, 2018) ("Testing issues include the development, creation, administration, scoring and interpretation of psychological tests. These tests can evaluate ability, such as intelligence, aptitudes, skills and achievement; personality characteristics, such as traits, attitudes, interests and values; and mental health, such as psychological functioning or signs of psychological or neurological disorders. When tests are standardized, psychologists can compare results from one individual with those of others.")

[37] 42 U.S.C. § 12112(d)(2); 29 C.F.R. § 1630.14(a); EEOC Questions and Answers: Enforcement Guidance on Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act (http://www.eeoc.gov/policy/docs/qanda-inquiries.html) ("EEOC Questions and Answers").

[38] *Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations*, *available at* https://www.eeoc.gov/policy/docs/preemp.html (last visited on September 10, 2018); and *Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employee Under the Americans with Disabilities Act*, *available at* https://www.eeoc.gov/policy/docs/guidance-inquiries.html#N_6_ (last visited on September 10, 2018).

[39] *Id.*

interpreted by a health care professional; (3) designed to reveal an impairment or physical or mental health; (4) invasive; (5) measures an employee's performance of a task or measures his/her physiological responses to performing the task; (6) normally is given in a medical setting; and/or (7) medical equipment is used.[40] Consequently, employers considering using a recruitment or selection technology that includes a personality test should ensure that the test, including all questions and components, does not constitute an unlawful medical inquiry. They should also ensure that the test and its components are job-related and consistent with business necessity.

Lesser known, but equally compelling is the ADA's obligation for employers to ensure that their application process is accessible to people with disabilities, or alternatively, provide a "reasonable accommodation" to allow an employee to be considered for a job opening.[41] This obligation arguably extends to tools used by employers for recruitment and selection purposes.[42] Accordingly, if the vendor's platform is not accessible – e.g., it is coded in such a way to allow a person using a screen reader or other assistive technology to use it, compelling that person to ask for an accommodation – the employer may be requiring candidates who are disabled to disclose information about their medical status prematurely. Indeed, even where the employer offers alternative ways to record interviews, such as allowing interviews to be recorded via handheld smartphones and tablets, it is not unreasonable to conclude that a candidate with a disability who is not hired could allege that the employer had knowledge of his or her disability because of the fact that he or she was required to use alternative means of participating in interviews and accordingly, state a claim for disability discrimination. Depending on the steps that the vendor has taken to make its products and services complaint with the Web Content Accessibility Guidelines ("WCAG") 2.1[43] at Levels A and AA, there may also be a risk of increased exposure to disability accessibility claims.

D. Accommodating Sincerely Held Religious Beliefs

Another factor to consider is whether an employer must accommodate an applicant who objects to participating in a technology-based interview process, such as a video-recorded interview, on religious grounds. Title VII prohibits discrimination based on an applicant's religion and requires an employer to accommodate an applicant's sincerely held religious belief, provided that doing so does not cause an undue hardship to the employer.[44] For instance, if an applicant

[40] *Id.*

[41] 42 U.S.C. § 12112(b)(5);

[42] *See*, *e.g.*, *Reyazuddin v. Montgomery County*,789 F.3d 407 (4th Cir. 2015) (court allowed case to proceed where blind plaintiff alleged employer call center violated ADA in failing to accommodate plaintiff by making software accessible or transferring plaintiff to new call center); *see also Martinez v. Alorica, Inc.*, 30-2018-987988 (Cal. Super. Ct. Apr. 24, 2018) (blind plaintiff applicant brought claim under California law alleging employer's failure to accommodate, engage in interactive process where unable to apply for job because the online application was not accessible).

[43] Web Content Accessibility Guidelines (WCAG) 2.1, *available at* https://www.w3.org/TR/WCAG21/.

[44] 42 U.S.C. § 2000e(j).

indicates that she is concerned that the device recording her interview is capturing her soul and depriving her from going to heaven, an employer might be required to accommodate the applicant's sincerely held religious belief by providing her with an alternative, non-technical, method of interviewing.[45]

E. Privacy

a. In General

The use of some of these recruitment and selection technologies also raises a host of privacy-related issues, particularly where the technology collects, or "over-collects" sensitive personal information regarding an individual. Although there is no federal statute providing candidates with the right of privacy, common law causes of action are on the rise and issues such as whether the individual must demonstrate "actual harm" to have a cognizable cause of action differ by jurisdiction.[46]

In addition, some states prohibit recording communications without the consent of all parties to the communication in circumstances where the individual reasonably believes that he or she would not be recorded.[47] An applicant that records her interview with a mobile audio or video recording device in a public location likely consented to the recording. The same is not necessarily true for the individuals in the background, who likely do not even know that the interviewing technology is recording their communications.

b. Biometric Data

Recruitment and selection technologies that collect biometric information, such as facial or retina scans, pose additional risks for employers. Several states have enacted legislation

[45] *See*, *e.g.*, *EEOC v. Consol. Energy, Inc.*, 860 F.3d 131 (4th Cir. 2017) (Employee objected to using employer's hand-scanner timekeeping system based on sincerely held belief that scanner would associate him with the "Mark of the Beast," allowing the Antichrist to identify and manipulate him, ultimately subjecting him to everlasting punishment. In affirming jury verdict for employee, court held that Title VII required the employer to accommodate the employee's sincerely held belief and could have provided him with an alternative timekeeping solution at no additional cost).

[46] *Compare Doe v. Henry Ford Health System*, 308 Mich. App. 592, 865 N.W.2d 915 (2014), *lv. app den'd*, 498 Mich. 879, 868 N.W.2d 912 (2015) (dismissing plaintiff's invasion or privacy, negligence and breach of contract claims after her defendant's contractor inadvertently placed her personal health information in unsecured served, because plaintiff could not demonstrate "actual injury") and *Santana v. Take-Two Interactive Software*, No. 17-303, 2017 U.S. App. LEXIS 23446 (2d Cir., Nov. 21, 2017) (finding no Article III standing where plaintiff willing submitting information to employer) *with Dixon v. Washington & Jane Smith Cmty.*, No. 17-cv-8033, 2018 U.S. Dist. LEXIS 90344 (N.D. Ill., May 31, 2018) (finding Article III standing where plaintiff alleged that employer disclosed her fingerprint information to vendor without informing her, because "alleged violation of the right to privacy in and control over one's biometric data, despite being an intangible injury, is sufficiently concrete to constitute an injury in fact that supports Article III standing.")

[47] *See*, *e.g.*, Cal. Penal Code § 632.

creating protections for biometric information, regulating what may be collected, how it must be stored and disposed of, and imposing stiff penalties for employers who break the rules.[48] Biometric data, or the unique, measurable human biological or behavioral characteristics that can be used for identification, may include fingerprints, voiceprint, retina or iris scans, and scans of hand or face geometry.[49] Enacted in 2008, Illinois' Biometric Information Privacy Act ("BIPA") is the most comprehensive of the state biometric privacy laws. Pursuant to BIPA, before an employer collects, captures, or obtains biometric identifiers or biometric information, it must first supply a written notice informing the information provider that their biometric data is being collected and stored, explaining the purpose for collecting, storing, and using the data, and qualifying the length of time for which it will retain the data. The employer must also procure the provider's written consent, and must only use the data as described in the notice, pursuant to the provider's consent agreement. Accordingly, using applicants' video-recorded answers to interview questions to evaluate fitness for a particular position may open an Illinois employer up to liability under BIPA.[50]

c. European Union's General Data Protection Regulations

There are also special consideration for U.S.-based companies subject to the European Union's ("EU") General Data Protection Regulations ("GDPR"). [51] Effective May 25, 2018, the GDPR regulates the processing by an individual, a company or an organization of "personal data" relating to individuals in the European Union ("EU").[52] Wherever an organization is based – even

[48] *See* Illinois, 740 ILCS 14/1; Texas, Tex. Bus. & Com. Code Ann. § 503.001; Washington, RCW 19.375.010 to 19.375.900. Additional legislation has been proposed or is pending, or the state's existing data privacy laws cover biometric data in Alaska, House Bill No. 72, An Act Relating to Biometric Information (Jan. 20, 2017), http://www.legis.state.ak.us/basis/get_fulltext.asp?session=30&bill=HB72; Connecticut, Public Act No. 15-142, An Act Improving Data Security and Effectiveness (July 1, 2015), https://www.cga.ct.gov/2015/ACT/PA/2015PA-00142- R00SB-00949-PA.htm; Massachusetts, Proposed House Bill No. 225, An Act Updating Chapter 93H Data Security Protections To Include Biometric Information (Jan. 2015), https://malegislature.gov/Bills/189/House/H225; Montana, Proposed House Bill 518, Act Establishing the Montana Biometric Information Privacy Act (2017), leg.mt.gov/bills/2017/BillPdf/HB0518.pdf; New Hampshire, Proposed House Bill 523, An Act Relative to Limitations on the Use of Biometric Information (2017), https://legiscan.com/NH/text/HB523/id/1456913/New_Hampshire-2017-HB523-Introduced.html; and Wisconsin, Wis. Stat. § 134.98 (2017).

[49] *See*, *e.g.*, 740 ILCS 14/10. *See also* Lauren A. Daming, *How to Stay Within the Law* Title *When Using Biometric Information*, SOCIETY FOR HUMAN RESOURCES MANAGEMENT (Apr. 3, 2018), https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/stay-within-the-law-biometric-information.aspx.

[50] *See Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017); *Monroy v. Shutterfly, Inc.*, No. 16C10984, 2017 U.S. Dist. LEXIS 149604, *14 (N.D. Ill., Sept. 15, 2017) (BIPA may apply to technology that scans facial photographs because the resulting facial geometry measurements constitute "biometric identifiers" as defined by BIPA). For Texas employers, it may also trigger the Texas Biometric Privacy Act, which covers voiceprints.

[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[52] *See* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en (last visited on September 10, 2018).

outside the EU – if it is processing the "personal data" of EU residents, it must comply with the GDPR. U.S.-based companies can be subject to the GDPR if they offer goods and services to EU residents or if they obtain data related to the monitoring of behavior that takes places within the EU.[53]

"Personal data" is any information that relates to an identified or identifiable living individual.[54] Examples of "personal data" covered by the GDPR include: (1) name and surname; (2) home or email address; (3) location data (for example the location data function on a mobile phone); (4) an Internet Protocol (IP) address; (5) a cookie ID; and (6) advertising identifier of one's phone.[55] Recruitment and selection technologies collect much, if not all, of this information.

U.S.-based companies who enter into contracts with recruitment and selection vendors that mine-data from EU residents must comply with the GDPR. Frequently, but not always, the employer is the "controller," because it is the entity requesting the data, whereas the vendor is the "processor," because it is collecting, storing and reporting the data to the employer. The GDPR requires that the "controller" company have a formal contract with the recruitment and selection vendor that ensures the vendor is compliant with the other provisions of the GDPR.[56] Other requirements include (a) requiring a lawful basis or the consent of subjects for data processing;[57] (b) providing data breach notifications to regulators in the EU, and potentially to individuals;[58] and (c) safely handling the transfer of data across borders.[59] The vendor ("processor") faces additional

[53] Rec. 24, GDPR; *see also* Art. 4, ¶ 2(b), GDPR.

[54] *See* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Personal data that has been de-identified, encrypted or pseudonymized but can be used to re-identify a person remains personal data and falls within the scope of the law. *Id.* Truly anonymized personal data is excluded from the law, but only if the anonymization is irreversible. *Id.* Importantly, the law protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organized in accordance with pre-defined criteria (for example alphabetical order). *Id.* It also does not matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR. *Id.*

[55] *Id.*

[56] Art. 28, ¶ 3 (a)–(h), GDPR.

[57] Art. 6, ¶ 1, GDPR.

[58] Art. 34, GDPR.

[59] Privacy Shield Framework, https://www.privacyshield.gov/article?id=OVERVIEW.

requirements from the regulations including: (a) data security requirements;[60] (b) data breach notification;[61] (c) record-keeping obligations;[62] and (d) appointment of a data protection officer.[63]

In practice, the GDPR should have a large impact on U.S.-based companies' use of recruitment and selection vendors for EU-based talent. Companies should consider steps towards compliance, especially where the potential exists for the vendor to actively or passively recruit from the EU, as the consequences of not complying could be significant. The GDPR gives EU member states enforcement authority over the regulations. Maximum fines for violations might be as high as the greater of either €20,000,000 or 4% of the total worldwide annual turnover from the preceding financial year.[64]

F. Data Storage and Security

Organizations entering into agreements with recruitment and selection technology vendors need to understand where the vendor is hosting and storing the data that it is collecting. If the vendor is hosting the data on another company's cloud-based server (e.g., Amazon Web Services) and using another company's services to store it (e.g., Amazon Simple Storage Service), the employer will be twice removed from the party (e.g., Amazon) that will be hosting the confidential information obtained from applicants. Given the prevalence of data breaches via Internet hacking, there is a risk that the vendor's data security measures (through Amazon) are insufficiently robust to protect the company in the event of a data breach.

Similarly, before entering into an agreement with a recruitment and selection technology vendor, employers need to understand what rights, if any, the vendor has to access the data, how the vendor is safeguarding the data, and when they can access the data. It is also important to

[60] Art. 32, GDPR.

[61] Art. 33, ¶ 2, GDPR.

[62] Art. 30, ¶¶ 2–5, GDPR.

[63] Art. 37, GDPR.

[64] *See* https://www.gdpreu.org/compliance/fines-and-penalties/. States are also starting to consider legislation to protect an individual's personal data. *See*, *e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE §§1798.100-1798.198, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. Effective January 1, 2020, the law gives "consumers" – defined as natural persons who are California residents – the following four basic rights in relation to their personal information: (1) the right to know, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold; (2) the right to "opt out" of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parent's, opt-in); (3) the right to have a business delete their personal information, with some exceptions; and (4) the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the law. Companies that use recruitment and selection technologies should not wait to begin the process of determining how they will comply with these new statutory obligations.

understand what happens to the data when or if there is a change in the corporate structure of the employer or the vendor, through a sale, merger or closure.

G. Litigation Risks

No published decision from a court addressing the legal issues identified in this paper could be located. A frequent recommendation to address the potential exposure an employer may face from relying on a vendor's recruitment and selection technologies is to seek indemnification from the vendor.[65] If, however, a party successfully challenged a recruitment and selection vendor under a discrimination or similar theory, it is likely that similar litigation would not be too far behind. Although subsequently-sued employers would not necessarily concede liability, it will be more difficult to defend against such a claim where the employer is using the same exact product and/or algorithm already found to be unlawful. To the extent that the vendor is willing to indemnify or otherwise assist in defending the legality of its products, the value of any such indemnification or assistance will diminish as its other customers are found liable.

IV. PRACTICAL CONSIDERATIONS

A. Mitigation Recommendations

One of the primary ways that employers can potentially mitigate any legal risks associated with using AI solutions in recruiting is to ask questions upfront before committing to a contract with a specific vendor. The answers to those questions may alleviate many, if not most, of the legal concerns described below and avoid necessitating additional mitigation measures.

As set forth above, initial video interviews of a candidate may place an employer on notice of the candidate's protected characteristics. To mitigate potential risk, employers should use the same level of care and caution when preparing structured interview questions for the vendor to use as it would for its existing hiring process. If the employer does not presently use structured interview questions, the employer should consider the option, if provided by the vendor, of inputting structured interview questions into the system to permit consistency of questions across all candidates. In addition, after each interview, the interviewer should fill out a candidate survey form, which will be stored with the candidate's application materials. The form will contain the reasons why the interviewer chose to recommend or not recommend the candidate for the next phase of the hiring process. Documenting these reasons will help mitigate the risk that comes with identifying protected characteristics by more people earlier in the process.

Before implementing a vendor solution, employers should think carefully about the individuals within the organization to whom it will give access to the vendor's capabilities. Rather

[65] Another recommendation often cited for employers is to design their job-application process to produce an enforceable arbitration agreement. In *Epic Systems Corp. v. Lewis*, 138 S. Ct. 1612 (2018), the Supreme Court of the United States ruled that employers can require employees to arbitrate disputes with the employer individually and waive their right to pursue or participate in class or collective actions against their employer.

than providing open access to final decision-makers, the employer should identify a core group of individuals within its Human Resources or analogous organization who will have the ability to "remove" – to the extent possible – protected information from the view of the final decision-makers prior to their use. Appropriate security also should be in place to prevent decision-makers from improperly or accidentally accessing protected information of candidates that they should not consider during the hiring process.

Another mitigation recommendation pertains to the assessments offered by vendors. Before completing the assessment, the vendor should conduct a thorough job analysis. Doing so will help ensure not only that the candidates responding to the job posting and being interviewed are better suited for the position, but also will mitigate legal risk by making the use of the algorithm job-related and consistent with business necessity. Better still is cross-validating with different samples to show that job-relatedness is present in multiple samples and ensuring that the job analyses are updated periodically and/or as necessary. Once a vendor's tool is used, the employer should conduct an adverse impact analysis, under attorney-client privilege, to determine whether there has been a statistically significant adverse impact on any population of protected category. Should the analysis identify an adverse impact the employer should commission a validation study, which is recommended even if adverse impact is not found. Lastly, as identified above, it is advisable for employers to conduct a reasonable search for alternatives to the solution that they are presently using.

To comply with document retention obligations, employers should work with vendors to ensure that the employer can appropriately customize its current record retention defaults to comply with EEOC guidance and DOL requirements, and so that that retention becomes perpetual as charges or complaints are made, if applicable. Employers should also note that the period for required record retention changes once the individual's status changes from applicant to employee. To the extent that the vendor becomes the tool on which the employer stores certain other employment information (including payroll and other employee information), the period for retention may be longer.

Employers should assess their ability to delete interviews/materials and job ads at any time during their engagement with the vendor. So as to prevent unauthorized users from deleting interviews/materials and job ads that should be maintained, employers should work with their vendors to prepare a form documenting the reasons for the deletion, the person who made the request to delete, the date on which the deletion was requested, and the date on which the deletion occurred. Employers should also ensure that the vendors do not delete interviews/materials and job ads unless the designated representative of the employer approves.

On a similar note, employers should keep in mind that vendors are sources of Electronically Stored Information ("ESI") in future litigation. Thus, it is worthwhile to ask the vendor about the type of search terms it can apply within its operating system for purposes of ESI searches and protocols, and whether it can export information into a spreadsheet aggregating candidate information, or whether it must access each candidate's information separately. Employers may want to consider having an ESI vendor evaluate the service from an ESI expert perspective because ESI is among the most costly and onerous parts of litigation and it is advisable to take steps upfront to mitigate potential ESI non-compliance.

Finally, it would be prudent for the employer's data security group to work with the vendors to ensure that the data stored by each vendor is secure. Likewise, employers must be satisfied that the vendors have taken steps to prevent security breaches.

B. Sample Checklist

In addition to basic concerns like cost and integration into existing systems and processes, organizations that are considering adopting recruitment and selection technologies should consider asking the prospective vendor the following questions, where applicable:

Factors Measured

□ Where the tool uses machine learning in determining both the factors and the weight of each factor, can you describe the factors and the weight each is given?

□ Can you tell us what the factors are?

□ Can you tell us the weight given to each factor?

□ Can we make modifications to the algorithm? For example, can we remove a factor or change the weight?

□ Will we have to sign a nondisclosure agreement to get that information?

□ Can we have that information if a government agency asks us or a court of law compels us?

□ How often does your algorithm change?

□ Do you share with your customers the changes and the purpose of the changes?

Validation

□ Have you validated or otherwise tested your algorithm to determine if the results it creates could be biased?

□ When was the last time?

□ How often do you validate?

□ By whom?

□ Can you describe the validation methodology?

- □ How do you determine if the bias is something about which to be concerned? (Ideally, the answer should reflect the 4/5ths rule of the Uniform Guidelines)

Job Analysis

- □ What do you do to analyze the jobs for which we are hiring?
- □ What resources and information do you need from us for purposes of your analysis?

Disability Accommodation

- □ Is your product compliant with Web Content Accessibility Guidelines ("WCAG") 2.1 at Levels A and AA and, if so, can we see documentation?
- □ What accommodations can your product make for applicants with disabilities?
  - □ Visually impaired applicants?
  - □ Hearing impaired applicants?

Privacy

- □ Does your product collect any biometric identifiers, such as voiceprints or other unique biological patterns or characteristics used to identify a specific individual?
  - □ If so, how to procure consent?
  - □ How is the information used?
  - □ How is the information stored?
  - □ How is the information destroyed?

Data Processing and Storage

- □ How and where does you store the data recorded?
- □ What precautions are taken to safeguard data security?
- □ How long is the data stored?
  - □ Can the retention dates be modified as individuals transfer from applicants to employees?
- □ Do you archive or maintain records showing when an algorithm was altered?
- □ Can we have access to the algorithm if we need to defend our self against an action, like before the EEOC, OFCCP, or state agency?

- □ What is the process for anonymizing individuals' information?
- □ If we are sued, we may be required to retrieve data from the tool.
  - □ Can we have access to the algorithm if we need to defend our self against an action?
  - □ What are the data searching capabilities?
  - □ Can information be exported into a spreadsheet aggregating candidate information? Or, at minimum, can each candidate's information be accessed separately?

Training

- □ What training do you offer for users?
- □ Will you offer training on what the algorithm means and/or how to use it?

Lawsuits

- □ Has your product been subject to litigation or administrative charges?
  - □ If so, when, what were the claims, what is the status of the legal action?
- □ What kind of assistance do you provide to defend discrimination claims or indemnify us against legal claims?

EPSTEIN
BECKER
GREEN

Technology Employment Law

Legal Insight for Technology, Media, and Telecommunications Employers

Shifting Obligations for Employers with the Advancement of AI-driven Automation and the Rise of Independent Workers

By Michelle Capezza on March 6, 2017

POSTED IN EMPLOYMENT LAW

As I continue to follow developments regarding the future of work, I recently attended an event co-sponsored by Cornell/ILR's Institute for Workplace Studies in NYC and the McKinsey Global Institute (MGI) addressing MGI's report last Fall entitled ***Independent Work: Choice, Necessity and the Gig Economy***. The report examines the increasing numbers of self-employed, freelance and temporary workers in the U.S. and Europe which are currently estimated to comprise 30 percent of the working-age population and rising. The report notes that many workers have chosen this autonomous path as their primary means of income, while others follow it to supplement income, and yet others have no other choice and would prefer a traditional job with fair wages and benefits.   Many factors have led to the return to this pre-industrial revolution independent worker model including the recession and the emergence of The Digital Age as workers are more mobile and have increasing access to new technologies which transform how work is performed and goods and services are bought and sold.

The independent model of work is not without its critics. Not everyone is capable of managing themselves as an independent business. Many fear that this model is more appropriate for highly-skilled workers who have special skills and can manage multiple engagements which they have cultivated and that are well paid.   For the majority of entry-level or non-specialized workers, however, this model may drive down wages and leave many others unemployed. Further, it is unclear how independent workers will be protected from pay disparities, discrimination, work injuries, unemployment and how they will obtain benefits for such needs as health care, retirement, or disability. Many have argued that employers have moved toward retention of independent workers to avoid employment and benefits legal responsibilities and erode the traditional employer-employee relationship and benefits.

Shifting worker models are also caused by advances in automation and will accelerate with the transformations that will be ushered into the workplace with artificial intelligence, machines and robots that perform many current jobs and will perform jobs of the future. In a December 2016 report from the Obama administration entitled ***Artificial Intelligence, Automation, and the Economy,*** it was noted that while the industrial revolution led to the disruptions to the lives of many agricultural workers, the technological revolution has led, and will continue to lead, to disruptions for workers in all industries. This will also continue to impact the professions (e.g., financial services, education, journalism, sales, accounting, law and medicine). The increased use of automation and the demand for highly-skilled workers and those capable of abstract thinking and creativity will result in the displacement of many workers who perform routine tasks and in lower-skilled jobs. Further, it is only a matter of time before robots are built with the manual dexterity to perform physical labor jobs. As society advances and deploys AI-driven automation, a re-thinking of worker models, our educational system and the social safety net is crucial.

With this confluence of events, it is imperative that swift policy action is taken to prepare for the transition that lies ahead and employers have an important role to play. As we have seen with the passage of the Affordable Care Act and proposals for automatic payroll-IRAs managed by states or local governments, there have been movements afoot for several years calling for more government-run forms of benefits in the U.S. which lend themselves to portability without attachment to an employer, but these models are also controversial for numerous economic and political reasons and are under attack. Policy makers continue to put forth ideas to require employers and independent contractor agencies to contribute toward a system of portable benefits for independent workers which may include multiple employer programs, pooled associations, and various types of government funds. The shifting tides will also require individuals to be financially educated and to save in their own health, retirement, and other insurance type vehicles apart from any employer-provided benefits. Employers in all industries will need to contribute to these debates and should consider the following:

- ***Develop a Workplace Transition Policy.*** As employers manage multiple generations in the workforce from the traditionalists, baby boomers, Generation X, Millenials, and Generation Z, and as society shifts to new models in the workplace, including use of AI-driven automation, impact on existing traditional-model workers should be carefully addressed. Immediate issues to consider include proper management of employee reductions and retirements (including fair and reasonable severance and related benefits (including career transitioning and re-training assistance), incentives for transfer of knowledge between generations (which may require ongoing consulting arrangements or staggered retirements), guidance for younger generations managing older generations and/or cobot relationships (which may require leadership training or new models of management training which address the newly envisioned workplace), integration of flexible work arrangements and job sharing, and deployment of AI and workplace technologies (with commensurate training and accommodations for their use). Improper handling of these issues can implicate allegations of violations of various employment laws from age, gender and disability discrimination to interference with rights to certain employee benefits.
- ***Pay a Fair and Competitive Wage.*** The call for fair wages, including a rise in the federal minimum wage, is not new. As more of the economic burden will fall on individuals to not only afford to live but also to save for all of their needs including health care, retirement, and periods of unemployment without employer assistance, fair wage initiatives are imperative and provide one way for employers to contribute to the eroding social safety net for all workers. If this can be combined with financial wellness and literacy type programs, employers can play a significant role in assisting their workers understand and meet their financial needs.
- ***Provide Employee and Independent Worker Benefits***. It is widely noted that the erosion of employer provided pensions has contributed to the retirement crisis. Further, employer provided health care also continues to be under attack. Employer sponsored programs that address retirement savings and health care benefits provide a crucial safety net for workers and should be maintained lest these needs fall on the government to provide in order to fill the void. Policy makers are also evaluating ways to make these benefits more flexible and portable and these developments should be monitored. Consideration should also be given to making these benefits available to independent workers, which would resolve many of the worker misclassification analyses as it relates to impermissible exclusions of eligible workers for plans. Among

the many other types of employer-provided benefits, additional benefits such as tuition reimbursement and student loan debt repayment programs will also assist workers to train for future job skills and ease burdens of existing debts.

- ***Contribute to Pipeline Development of Workers.*** Educational systems are in dire need of reform. Employers should consider how to partner with high schools, colleges and universities for job training, internships, and research endeavors to prepare next generations for the future of work. Thought should also be given to re–tooling the current workforce to obtain the skills needed for the marketplace. Ensure that the pipeline of workers obtains the needed skills for future jobs.
- ***Carefully Deploy AI-driven Automation and New Technologies into the Workplace.*** The increased use of machines, robots and AI in the workplace will lead to new legal questions concerning data privacy and security, workplace safety, and far ranging employment and labor issues as individuals are required to work with, or be displaced by, these tools. Whether a worker is an employee, an independent contractor, or another yet–to– be determined classification, the co-working relationship between humans and machines has yet to be defined and will require thoughtful planning.

Businesses that have goods and services to sell will need individuals to buy them. If independent work becomes more of a necessity than a choice, the social and economic consequences can be dire. As businesses gain from the increased profitability that is promised by the use of AI-driven automation, impending tax reform, and shifting worker models, it is imperative for employers to contribute to the policy debates and find ways to contribute to the economic security of the individual workers.

EMPLOYMENT, LABOR & WORKFORCE MANAGEMENT

EPSTEIN
BECKER
GREEN

TAKE 5
VIEWS YOU CAN USE

TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS

July 2017

Five Workforce Management Challenges in Unprecedented Times

Employers across all industries are deep in the midst of exciting but uncharted and fluid times. Rapid and unforeseen technological advancements are largely responsible for this dynamic. And while there is a natural tendency to embrace their novelty and potential, the reality is that these advancements are often outpacing our regulatory environment, our bedrock legal constructs, and, in some cases, challenging the traditional notions of work itself.

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.

For employers, this presents numerous challenges and opportunities—from the proper design of the portfolio of the modern workforce, to protecting confidential information in an increasingly vulnerable digital world, to managing resources across less and less predictable borders, and to harnessing (while tempering the power of) intelligence exhibited by machines.

The time is now (if not yesterday!) to develop a long-term strategy to help navigate these current issues and anticipate the challenges and opportunities of the future.

What follows in this edition of Epstein Becker Green's *Take 5* are just some of the most salient of the workplace issues of today and tomorrow:

1. Embracing the Gig Economy: You’re Already a Player in It (Yes, You!)

By Ian Carleton Schaefer and Lori A. Medley

The term “gig economy” has gotten a substantial amount of play and attention in the media and in daily life as of late—often provoking near Pavlovian mental images of ride-sharing platforms, people on bicycles frantically running errands in an urban environment, or other device-based apps and services that five years ago we couldn’t envision—and which now we cannot fathom a world being without. But that common depiction and definition of the “gig economy” is, in fact, far too narrow.

Because here’s the thing: whether you want to or not or whether you realize it or not, the stark reality is that all companies—old and new, large and small, public and private—historically, currently, or imminently are real players in the gig economy, or what some refer to as the “contingent workforce game.”

Put simply, the “contingent workforce game” or “gig economy” refers to the labor economic model of short-term work relationships or alternative, non-traditional work relationships in which workers (whether they be self-employed, employed through employment agencies, temps, consultants, contractors, freelancers, seasonal, or the all-encompassing “other”) accept assignments of various lengths from people and firms who demand their services—as opposed to the more traditional, full-time employment relationship.

While temporary employment or non-traditional working arrangements are certainly not a new concept in the U.S. economy, the ubiquity and efficiency of these arrangements today has increased the demand for new technologies and platforms to facilitate this growing human capital model. In fact, the Bureau of Labor Statistics estimates that, in 2017, as many as 40 percent of the U.S. workforce is considered contingent. This figure is expected to grow to 50 percent by 2020.

Here are five issues that all companies should be mindful of as they embark on their own journey of embracing the gig economy:

1. **Misclassification of Employees:** Identifying whether an individual is an employee or an independent contractor continues to be the most confused and contentious issue for gig workers and employers alike. The stakes are due to the afforded rights, protections, and benefits under applicable law and employer policies provided to various workers.

   The financial implications of misclassification have been known to the tech sector since at least 1997, when *Vizcaino v. Microsoft Corp.*, 120 F.3d 1006 (9th Cir. 1997), served as a wake-up call. This decision held that freelance workers who worked for Microsoft between 1987 and 1990, and who had signed independent contractor agreements noting their ineligibility for benefits, were common law employees and eligible for benefits under Microsoft’s 401(k) plan and Employee Stock Purchase Plan, pursuant to the language of those plans.

   A more recent and closely watched case is *O’Connor v. Uber Techs*, 82 F. Supp. 3d 1133 (N.D. Cal. 2015). In *O’Connor*, plaintiffs, who are individuals who worked as Uber drivers, allege that they are Uber employees and should be paid minimum wage and receive reimbursement for work expenses. Uber argues that it is a technology platform that merely partners with independent contractors to connect them with consumers who need a ride. On summary judgment, the court found that the plaintiffs had established a rebuttable presumption that they were employees, focusing on the amount of control that Uber exercised over its drivers through its interview process, unilateral determination of rates, and ability to terminate drivers who received low customer satisfaction scores. Ultimately, the question of whether the plaintiffs are employees or independent contractors was for the jury to decide. The case has yet to go to trial, and a proposed $100 million settlement was rejected by the California District Court last year. This remains a seminal case to track that will have ripple effects on the broader gig economy for years to come.

2. **Agreements with Independent Contractors:** In light of the potential for misclassification claims, it is becoming ever more important for companies to clearly define their relationships with temporary workers at the outset and memorialize the details of the relationship in an independent contractor agreement. Employers must also be mindful of applicable state law that provides a means for clarifying the independent contractor relationship. For example, on May 15, 2017, New York City's Freelance Isn't Free Act ("FIFA") took effect. Under FIFA, among other things, parties that retain "freelance workers" to provide services under a contract between them that is worth $800 or more must reduce the contract to a written agreement. Contracts with independent contractors or staffing agencies should also contain strong indemnification language to protect a company from liability should the independent contractor or temporary worker negligently or intentionally harm its customers, as well as require the contractor to maintain and furnish proof of insurance.

3. **Joint Employment/Co-Employment:** The potential to unwittingly become a joint employer with a third-party entity that is acting as an intermediary and providing the workers (i.e., a temporary staffing company) is also ranked as a chief concern among employers. The joint-employer concept looks at whether two companies share or control the essential terms and conditions of employment for a worker. If a company is deemed to be a joint employer with another employer, that company can be found equally liable for any claims or legal issues (e.g., discrimination, wage-hour violations, etc.). Any agreement with a third-party entity should, at a minimum, contain a disclaimer on joint-employer status and clearly delineate responsibilities. Contractual strategies aside, the practical difficulties involved in balancing the requisite amount of supervision to be exercised over temporary workers with the legal standards of what constitutes a joint employer makes a finding of "no joint employment" increasingly challenging.

4. **Development of Company Culture:** While the flexibility to hire individuals on a temporary basis can certainly prove beneficial, it can become increasingly difficult to cultivate a cohesive company culture in a workplace that leverages a revolving door of temporary workers, particularly in light of misclassification and co-employment risks. It is increasingly incumbent on employers to evaluate and manage their resourcing model and to assess whether the makeup of their human capital portfolio is properly balanced for their business and cultural needs.

5. **Susceptibility to Unionization:** As the demand for portable benefits and wage parity for gig workers grows, more and more non-traditional work environments may find themselves targeted for unionization and organized labor as a means of providing protection and benefits to gig workers. As a recent example, the Huffington Post editorial workers voted to unionize in 2016 and recently voted to approve their first collective bargaining agreement with the Writers Guild of America East ("WGAE"), guaranteeing a minimum pay base for editorial workers and $16 per hour pay for comment moderators. WGAE has also approved union contracts for other digital content providers.

   The rise of the gig economy has also resulted in the birth of nonprofits created to provide benefits for, and to lobby on behalf of, independent contractors, most notably the

Freelancers Union (a strong supporter in the passage of FIFA, and one whose membership has surpassed 300,000).

In the end, whether you are a company that approaches the gig economy with open arms or with some resistance—make no mistake—this not-so-new normal is here to stay, and you are already operating in it. So embrace the reality, but do take caution along your journey.

2. AI in the Workplace: The Time to Develop a Workplace Strategy Is Now

By Michelle Capezza and Adam S. Forman

When it comes to artificial intelligence ("AI"), or intelligence exhibited by machines, most people immediately think of cinema's sentient computers such as HAL, Skynet, or Samantha. Although those machines are just Hollywood's fictional creations, the underlying notion that AI will play an integral role in every aspect of our lives is very real indeed. With the exponential rate of technological change, AI will continue to affect our lives more quickly and pervasively than ever before. One area that is already being impacted is the workplace.

From algorithms analyzing employee data, to computer and robotic laborers in retail and manufacturing, to the rise of the on-demand worker, AI has already disrupted how virtually every workplace operates. There is little doubt that the time to develop a workplace strategy is now. Some of the issues that organizations should consider as they introduce AI into the workplace include:

- **HR Technology:** Whether it is people analytics, digital interview platforms, or chat bots, AI is quickly becoming mainstream in human resource departments. Fueled by efficiencies and other benefits, these AI technologies seek to combine "big data" with human insight to glean unique information about talent for and within an organization. Employers introducing these technologies should make sure to review the vendor contracts and algorithms for employment law issues, such as whether the AI accounts for people with disabilities. Monitoring to make sure that the technologies do not have a disparate impact is also advisable.

- **Union Issues:** Employers that have represented workforces may need to bargain with their labor unions over the introduction of AI into the workplace, as well as the effects of AI on represented employees. Non-represented employers should make sure that the AI does not unlawfully interfere with its employees' right to engage in organizing activities, discuss wages, hours, and other terms and conditions of employment. Care should also be taken to make sure that data captured and stored with AI is not used for purposes prohibited by federal labor law, such as for unlawful surveillance.

- **Data Privacy & Security:** Many workplace AI solutions, by their very nature, collect and store large amounts of employee personally identifiable information ("PII"). Organizations utilizing such AI should take steps to make sure that they properly store and protect their employees' PII from unauthorized access by third parties or exposure through a data breach.

- **Employee Benefits:** As more workers and jobs are displaced and/or transitioned into new workplace models, in whole or in part, by AI, the ability of workers to obtain employer-provided benefits will be compromised. As a result, the traditional social safety net that has historically been supported by employer-provided benefits, such as retirement savings and health care coverage, is ripe for increased disruption. Policymakers are already proposing solutions to the workplace reality that employers will need fewer full-time employees. For example, on May 25, 2017, U.S. Senator Mark

Warner introduced in the Senate the Portable Benefits for Independent Workers Pilot Program Act (Representative Suzan DelBene introduced a companion bill in the House), which seeks to address the lack of an employer-provided safety net for workers who are not employed in traditional full-time positions and are not eligible for such benefits. While the bill seeks to provide grants to states, local governments, and nonprofit organizations to design and innovate existing benefit approaches, it also contemplates the future creation of a national portable benefits model that would require contributions from contingent workers as well as the entities that employ them. Employers should monitor these trends as well as navigate the design and compliance of their current benefits programs in light of such realities as (1) Affordable Care Act repeal and replace efforts; (2) increased appeal of health savings accounts; (3) policy efforts to move toward payroll IRAs for retirement savings; and (4) trends to de-risk and terminate pension plans, which can also involve pension withdrawal liability. Employers should also evaluate the types of benefits their workforce values in an AI-driven workplace so that they can continue to offer programs that attract and retain their desired talent.

- **Workplace Transition Policies:** With the inevitable disruption and displacement of certain jobs as workplace models transition to the new AI realities, employers should consider developing a workplace transition policy that may include establishing guidelines for employee reductions and retirements, severance and career-transitioning programs, skills development and tuition reimbursement programs, job-sharing, and flexible work arrangements.

The proverbial genie is out of the bottle with AI in the workplace, and there is no going back. Organizations should embrace the changes but do so thoughtfully and responsibly. Just as there no single AI solution that will work for every organization, there is no one-size strategy for introducing AI into the workplace. Nevertheless, prudent organizations should evaluate their workplace management goals and objectives and start developing strategies for introducing AI into the workplace. The future is now.

3. Best Practices to Manage the Risk of Data Breach Caused by Your Employees and Other Insiders

By Brian G. Cesaratto and Robert J. Hudock

The *bad news* is that most data breaches are caused by employees and other insiders (e.g., vendors), whether intentionally or inadvertently. For example, IBM Security found that insiders were responsible for 68 percent of all network attacks targeting health care data in 2016. Hackers regularly use email and social media to conduct social engineering attacks targeting unknowing employees. Not surprisingly, the highly publicized cyber threats are increasingly concerning corporate counsel. Recently, 74 percent of corporate counsel named data breaches as their top data-related legal risk. Another survey reports that 31 percent of general counsels identify cyber security as their top concern.

The *good news* is that many insider data breaches are preventable through a formalized, well-documented, and consistently applied insider threat program compliant with applicable law, including the screening, monitoring, and regular training of employees. Indeed, a comprehensive insider threat program is now a requirement for federal contractors pursuant to Executive Order 13587, which was issued in 2011 in response to the massive data leaks by Chelsea Manning. All employers should proactively address insider threats because a failure to institute best practices to prevent insider data breaches may result in significant financial loss, negative publicity, and expensive legal action should a breach occur.

Because insider threats can be divided into malicious and unintentional threat actors, the employer's program must address both:

- A *malicious* insider is a current or former employee or a business partner who has or had authorized access to the organization's network and intentionally exceeds or misuses that access in a manner that negatively affects the confidentiality, integrity, or availability of its information or information systems.
- An *unintentional* insider is someone who, through his or her action/inaction without malicious intent, causes harm or substantially increases the probability of future harm to the confidentiality, integrity, or availability of the information or information systems.

The employer's first step is to conduct a vulnerability assessment to evaluate risks according to job position and to the most sensitive data. For example, employers routinely maintain sensitive PII on its workers (e.g., benefits information, medical leave requests, health insurance and tax information, Social Security numbers, and addresses). An employer should identify where PII, trade secrets, and other confidential business information are maintained on its systems, and the employees who have access to this critical data. Job positions that permit access to critical data or systems, or grant administrative or super user privileges, should be identified.

Once the vulnerability assessment is conducted, the employer's program may be tailored to prevent, detect, and mitigate the identified risks by these employees and to the key data. The program should include personnel policies, such as pre-hire and periodic background checks and credit monitoring, employee training, access control and electronic monitoring of employee system use, strong passwords, acceptable use policies, and employer controls on the Internet of Things ("IoT") in the workplace and Bring Your Own Devices To Work ("BYOD"). The risks of BYOD and the IoT (and resulting risks from wireless connectivity) should be addressed, including regulating the types of devices that can be worn or used in the workplace. The use of encryption for confidential data in transit and at rest, and training employees in the proper use of encryption technologies, is a critical component.

Risks from disgruntled employees, or employees with a financial motive to participate in a data breach, should be documented and monitored using baselines and other objective measures. A deviation from normal baseline system activity or a high-risk event (e.g., demotion) should result in an objective trigger for increased scrutiny. For example, federal contractors are required to institute personnel-related measures to screen for 13 areas of risk, including personal conduct that involves "questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty or unwillingness to comply with rules and regulations"; financial considerations, including a history of not meeting financial obligations, overextending financially, or financial problems that are linked to gambling or drug abuse; illegal drug use; criminal conduct; security violations; outside activities that pose a conflict with an individual's security responsibilities; and the misuse of technology systems.

Ongoing training is very important both in preventing breach and in defending against legal claims if a breach occurs. Training should occur regularly and address recent social engineering attacks (e.g., ransomware) so that employees know what to look out for. The importance of training is highlighted because one click by an employee on a link containing malware may quickly disseminate across the employer's entire system. Preventing an event from occurring is critical, particularly because an intrusion may go undetected for months or even years.

Lastly, the program must anticipate the likelihood that a breach will occur and outline a response plan. Forensic artifacts can always be used to determine who, what, when, where, and why something occurred after a breach. The employer's policies in place (e.g., consensual monitoring) should enable and facilitate any future forensic investigation and a quick response time.

In sum, cyber security is a shared organizational responsibility best addressed through an insider threat program.

4. News Media Companies Entering the Non-Compete Game

By Asa F. Smith

Non-compete agreements—agreements that restrict employees from leaving a job and working for a competitor—are standard in many industries but are relatively scarce in the media and journalism sectors. Outside of television companies restricting star talent and media companies restricting executives, it has rarely been common practice for journalists to be subject to non-compete restrictions. This landscape, however, may be changing.

Two online-based news companies (both founded in 2012) are now incorporating non-competes into their contracts. NowThis (a left-leaning social media news company with a large presence on Facebook and Twitter) and the Independent Journal Review (an opinion and news website founded by former Republican staffers) have both made news in the last month for inserting broad non-compete clauses into new hire contracts.

The Independent Journal Review clause bars employees from working at "any competing business … anywhere in the world" for six months after an employee's departure. "Competing businesses" are defined as any business that is involved in the practice of publishing news content. The NowThis clause is narrower in scope; it bars employees from working at a specified list of news media companies, including CNN, BuzzFeed, and Conde Nast.

Both of these companies may have trouble enforcing their non-compete provisions. In recent years, as companies invest more in their new hires, it has become common to try to use non-competes to prevent competitors from poaching employees and benefiting from that investment. There has been a corresponding rise in regulation and backlash on the part of those who believe this to be an unnecessary and even harmful tactic. For example, the state of California has banned the use of non-compete clauses in nearly all circumstances, and other states have seen judges increasingly refuse to enforce non-compete clauses. Additionally, the New York Attorney General's office has pursued media companies (e.g., Law360) for the use of non-compete clauses.

Takeaway

As this back and forth between employers and employees (frequently with the state on their side) continues to play out, it is best for employers to ensure that, if they include a non-compete clause in their standard contracts, it is narrowly tailored in scope and geography to ensure that it is most likely to be enforced. As always, it is best to be cognizant of each applicable state's law and craft employment agreements accordingly.

5. Employers Dodge Bullet in Recent U.S. Supreme Court Travel Ban Order

By Monica Bathija

On June 26, 2017, the U.S. Supreme Court decided to partially lift lower court injunctions that had prevented any part of President Trump's March 6, 2017, executive order ("March 6 EO") to take effect.

In pertinent part, the March 6 EO barred foreign nationals ("FNs") from six predominantly Muslim-majority countries—Iran, Libya, Somalia, Sudan, Syria, and Yemen (collectively, the "Six Countries")—from entering the United States for 90 days (and 120 days for refugees), unless they were exempt from the order. The March 6 EO replaced a much broader travel ban contained in the President's January 27, 2017, executive order ("January 27 EO"). Lower federal courts in New York and Massachusetts enjoined enforcement of both the March 6 EO and the January 27 EO based on a strong likelihood that these executive orders violated the Due Process and Equal Protection clauses of the U.S. Constitution, among other grounds.

The U.S. Supreme Court's Partial Travel Ban Order

The U.S. Supreme Court's partial travel ban order, which went into effect at 8:00 p.m. EDT on June 29, 2017, lifted limited portions of these lower court injunctions against enforcement of the March 6 EO. In its decision, the Supreme Court held that the following FNs are exempt from the partial travel ban: (1) FNs in the United States with a valid visa or a travel/entry document as of June 26, 2017; (2) U.S. permanent residents; (3) dual FNs traveling on passports issued by a non-designated country; (4) FNs seeking admission to the United States in immigrant or nonimmigrant visa classifications that reflect a "bona fide relationship" with organizations or immediate family members in the United States; (5) certain diplomatic and North American Free Trade Agreement ("NAFTA") visa holders; and (6) FNs already admitted to the United States as asylees and refugees. In the Supreme Court's view, FNs seeking admission in each of these classifications had relationships with American citizens or organizations that mitigated against the security concerns that the March 6 EO was designed to address.

After the Supreme Court's decision, both the Department of State ("DOS") and Department of Homeland Security ("DHS") offered some guidance in terms of how the partial travel ban will be applied to FNs from the Six Countries. Most importantly, both the DOS and DHS confirmed that the partial travel ban does not apply to most family-based and employment-based visa classification applications. This includes FNs seeking admission in F, H, J, K, L, M, O, P, Q, and R nonimmigrant visa classifications, because each of them reflects the "bona fide" relationship required to offset the President's security concerns. Possibly excluded from this automatic exemption are certain employment-based applications, such as those by self-petitioning individuals in the EB-1 extraordinary ability classification, that are not based upon standing job offers from U.S. employers. These individuals may have to demonstrate a formal, documented relationship with a U.S. entity or citizen to secure admission.

Bona Fide Relationship

The June 26, 2017, U.S. Supreme Court decision did not define the term "bona fide relationship;" however, the Court provided a number of examples, stating that the test is based on whether a close familial relationship exists between the individual-sponsor and beneficiary. In one of its examples, the Supreme Court noted that a close familial relationship exists between an FN and his or her mother-in-law. The guidelines issued by the DOS, however, did not recognize this as a sufficiently close relationship with respect to family-based immigration. The DOS guidance reflected a very narrow approach and indicated that only parents, mothers-in-law, fathers-in-law, spouses, fiancés, children, adult sons, adult daughters, siblings, and half-siblings are considered to have the required close family relationship. Missing from the list were grandparents, grandchildren, brothers-in-law, sisters-in-law, aunts, uncles, cousins, nieces, and nephews.

On July 13, 2017, the U.S. District Court for the District of Hawaii rejected the DOS's definition of "close familial relationship" and ruled that grandparents, grandchildren, brothers-in-law, sisters-in-law, aunts, uncles, cousins, nieces, and nephews must also be included in the definition. As a result of this ruling, the DOS updated its FAQs on July 17, 2017, to reflect the District Court in Hawaii's broader definition.

On July 19, 2017, the Supreme Court weighed in on the District Court in Hawaii's decision. The Supreme Court affirmed the District Court in Hawaii's expanded interpretation of the family relationships exempt from the travel ban. As such, grandparents, grandchildren, brothers-in-law, sisters-in-law, aunts, uncles, cousins, nieces, and nephews will continue to fall within the broader definition of "close familial relationship" and, will, therefore, remain exempt from the travel ban.

Waiver Process

Any FNs not automatically exempt from the partial travel ban permitted by the U.S. Supreme Court's interpretation of the March 6 EO may still qualify for exemption so long as they can show that they each have a bona fide relationship with the United States—either with the individual or U.S. entity sponsor. Those FNs unable to show such a bona fide relationship may still be permitted to obtain a visa if they qualify for a waiver. In order to qualify for a waiver, the FN is required to prove each of the following: (1) the denial of entry will cause undue hardship, (2) his or her entry will not pose a threat to national security, and (3) his or her entry into the United States would be in the national interest. It is unclear how such waivers will be processed or even adjudicated.

Lastly, it is important to note that, even if an FN from one of the Six Countries is successful in obtaining a visa to travel to the United States, he or she must still demonstrate admissibility at the port of entry to the U.S. Customs & Border Protection ("CBP"). The CBP retains significant discretion to deny admission to FNs, even those with valid visas, if the agency feels that the FN presents a security or other threat. Time will soon tell how CBP decides to handle the entry of FNs from the Six Countries.

Takeaway

The partial travel ban allowed by the U.S. Supreme Court does not impact employers or those they sponsor. The Supreme Court issued only an interim order, so further changes could be made once the Court hears the case in October and makes its final decision. That being said, employers should identify all employees who were born in, or are citizens of, one of the Six Countries in order to be prepared to respond to any future developments.

* * *

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:*

Monica Bathija
San Francisco
415-399-6027
mbathija@ebglaw.com

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

Brian G. Cesaratto
New York
212-351-4921
bcesaratto@ebglaw.com

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

Robert J. Hudock
Washington, DC
202-861-1893
rhudock@ebglaw.com

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

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

Asa F. Smith
New York
212-351-4599
afsmith@ebglaw.com

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 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.

Attorney Advertising

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.

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.

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.

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

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