July 2017

Five Workforce Management Challenges in Unprecedented Times

Employers across all industries are deep in the midst of exciting but unchartered 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!)**
2. **AI in the Workplace: The Time to Develop a Workplace Strategy Is Now**
3. **Best Practices to Manage the Risk of Data Breach Caused by Your Employees and Other Insiders**
4. **News Media Companies Entering the Non-Compete Game**
5. **Employers Dodge Bullet in Recent U.S. Supreme Court Travel Ban Order**

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

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.