Future Workforce – 2018 Thought Leadership Roundtable Report

By: Garry Mathiason, Natalie Pierce, Matthew Scherer, and Jill Weimer

Littler

The development and deployment of increasingly sophisticated artificial intelligence (AI), robots, and other automated systems are transforming workplaces globally, redefining needed workforce roles, skills, and jobs, and reinventing work itself. Big data, predictive analytics, deep learning, biometrics, algorithmic bias, blockchain tokens, and collaborative robot safety standards are just a handful of terms now becoming commonplace in human resource management. While technology has been "the" instrument of change for much of human history, its exponentially accelerating arrival, fueled by increasingly nimble robots, mining of big data, and the automation of predictive analytics through deep learning, is beyond anything experienced. At the same time, most workplace policies, regulations, and laws were established long before such changes were even foreseen.

As Littler Mendelson P.C. developed the largest employment and labor practice in the world, it closely monitored the accelerating global infusion of technology into the workplace. It became increasingly predictable that robotics, AI, and advanced automation would become the largest collective industry reaching into almost every business, organization, and employer worldwide.

In 2013, Littler established a Robotics, AI, and Automation Practice Group to spotlight the technologically-induced workforce changes, unmask the workplace legal issues created, and innovate compliance solutions. Regulations clearly would not keep pace with technology, and employers need guidance to help speed the pace of workplace adoption of transformative technologies to keep competitive in global markets.

On November 12, 2018, Littler's Robotics, AI and Automation Practice Group hosted its third Future Workforce Roundtable, this time also inviting Littler's Workplace Policy Institute® (WPI™) to co-host the event. Littler's Robotics and AI practice and WPI assembled 40 world-class thought leaders and authorities in science, government, academia, law, ethics, and business to address the formation and challenges of the future workforce. The multi-disciplinary expertise, diversity, and global representation of the distinguished participants (many of whom returned to participate for a third time on the Roundtable) provided for intense discussions, debate, and deliberations with all members contributing.

Building on past thought leadership forums, the 2018 Future Workforce Roundtable participants addressed eight critical inquiries.[1] With respect to the first three inquiries, participants generally agreed that disruptive technology's principal challenge was how to qualify displaced workers for new roles and jobs created by the technology. Participants were also in general agreement that the contingent workforce is a significant part of the workforce, would continue to expand, and would require—and in fact, welcome—upskilling and lifelong learning. These contingent workers include those participating in the gig economy, as well as temporary, part-time and full-time workers, independent contractors, staffing employees and direct hires with short-term assignments. Finally, while most participants determined that precise future roles and jobs could not be identified at present, they described the skills that workers will need, and called for lifelong training. According to the participants, business will need to be a primary provider of such training, with government and academia supporting these efforts.

Littler's WPI has issued a separate brief report[2] on these three inquires and the guidance participants offered on how to prepare American businesses for "technology-induced displacement of employees" (TIDE), which is the mission of the EMMA Coalition, a nonprofit, nonpartisan organization developed by Littler's WPI and Prime Policy Group, a preeminent bipartisan government relations firm.

---

1 (1) Is the principle challenge of disruptive technology qualifying displaced workers for newly created roles and jobs, rather than attempting to preserve jobs that would otherwise be eliminated? (2) What are the future roles and jobs created by disruptive technologies, how does the current workforce become qualified for those positions and who in our society is or should be responsible for the transition? (3) How will the global contingent workforce be transformed as disruptive technologies mold the future workforce within the context of current and changing workforce laws and regulations? (4) Can and how are privacy and cybersecurity being redefined and maintained within the future global workforce? (5) Is full transparency possible, needed, or counterproductive in the context of identifying, reducing, or preventing algorithmic bias? (6) How is a workable legislative, regulatory and judicial roadmap developed that identifies needs, respects the role of innovation and considers unintended consequences? (7) Will AI and Robotic competition among governments accelerate the arrival of disruptive technologies in U.S. and EU workplaces? Do existing workplace laws protecting privacy and prohibiting discrimination based on protected categories inhibit U.S. and EU competitiveness? (8) What are the most important and immediate ethical challenges of AI in the workplace? In recognizing the AI imperative and building a practical roadmap for businesses, what are the best responses to these ethical challenges?

2 Michael J. Lotito and Matthew U. Scherer, *Thought Leaders Predict AI's Impact on the Workforce*, WPI Report (Dec. 3, 2018).

Redefining and Maintaining Global Workforce Privacy and Cybersecurity

Inquiry 4: Can and how are privacy and cybersecurity being redefined and maintained within the future global workforce?

In 2018, data privacy and digital identification were at the center of employers' regulatory radar. Participants agreed that companies have gained access to more and more data in recent years, and that the amount of employee data employers possess and store is increasing rapidly. Such data may be collected purposefully or inadvertently, and can be drawn from a variety of internal and external sources — from wearable devices that track health and fitness information, to security protocols that rely on biometric data, to information obtained from outside data vendors. It was discussed that over half of all employers are using and/or collecting biometric identity information on workers. Ranging from fingerprint and retinal scans to facial recognition and vein scanning, these biometrics can improve security and protect one's identity, but proper means of adoption and use is critical to avoid a host of unintended privacy and cybersecurity dangers.

Multiple federal and state statutes and regulations protect the collection, storage and privacy of health information, and workplace biometric information in particular is subject to a patchwork of legal consent and security requirements. It was reported that over 100 class actions are pending under the Illinois Biometric Information Privacy Act (BIPA). Currently, Illinois is the only state providing a private right of action for persons, including workers, who are "aggrieved by" violations of BIPA's information and written consent requirements.

While increased privacy and security controls were greatly anticipated, especially regarding the duty to protect the privacy of personnel information, some Roundtable participants noted that because actual damages were difficult to establish, many proposed privacy right-of-action statutes had been unsuccessful. Earlier this year, however, the U.S. District Court for the Northern District of California refused to dismiss a BIPA class action, finding plaintiffs had standing to bring their claims under the law. The Ninth Circuit will review the ruling.

In addition, eight days after the Roundtable, the Illinois Supreme Court heard oral argument in *Rosenbach v. Six Flags Entertainment Corporation* regarding whether to overturn a lower court decision requiring actual damages to justify a cause of action under the BIPA. Several participants reported that the pace and scope of data collection is likely to increase further as companies incorporate machine-learning systems into their operations, as most machine-learning applications require substantial data for training and validation.

While employers are finding increasing uses for (and increasing access to) employee data, as predicted, regulators worldwide have focused attention on regulating companies' ability to collect, maintain, and use that data. The EU's General Data Protection Regulation (GDPR), which took effect earlier this year, is the most visible and expansive regulatory effort in this space, but legislatures and regulatory agencies in many U.S. states are actively considering enhanced data privacy laws. GDPR has a much broader definition of "personal data" than those in U.S. breach notification laws. This will be challenging for many U.S. companies required to comply with GDPR. Employers collect "personal data" as defined by GDPR at the application phase of employment, so many will have difficulty obtaining the required level of consent from the applicant.

GDPR imposes notice obligations, requires truly voluntary consent for use of personal data, includes strict security regulations and, often, creates a need for new technologies to manage the requirements at scale. Several participants anticipated that U.S. privacy consent requirements would move closer to the GDPR standards. Other Roundtable members complained about relying on the US-EU Privacy Shield, as it is being challenged in the EU for not offering sufficient data protections, including failing until recently to nominate a State Department Ombudsman to oversee compliance complaints.

As in other areas involving new technologies, government efforts over data protection and cybersecurity may not properly account for the realities of current technology. Even though multiple means of establishing digital identity exist, many can be imitated, especially fingerprints and facial identity. These challenges are driven by the underlying digital technologies, which often were not designed to be digitally secure. But while technology is in some sense the problem in companies' efforts to comply with data privacy and security laws, it may also create solutions. Blockchains and deep learning may provide companies with new ways of

validating and securing data in their possession and creating the required roadmap for where the data goes once it is collected. The new laws require a level of monitoring and reporting nearly impossible for a human to manage regarding the collection and organization of data.

Several participants reported that monitoring technology is being developed and should be available soon. Implementation of this new and evolving technology will require cybersecurity professionals who are already scarce. Given the increasing attention that data privacy and cybersecurity are receiving from governments and the media, Roundtable participants agreed that companies must continue to closely monitor regulatory developments to ensure that their collection and retention of employee data stays compliant with laws, and invest in cybersecurity classroom and on-line training, apprenticeships, and support-focused vocational and community college cybersecurity programs. Compliance will be a process rather than a single solution, and informed regulators are critical of developing governmental oversight and controls.

The Challenge of Transparency and Explainability

Inquiry 5: Is full transparency possible, needed, or counterproductive in the context of identifying, reducing, or preventing algorithmic bias?

AI applications that rely on complex machine-learning algorithms, including applications that use multilayered neural networks whose inner workings are an indecipherable "black box," have been proliferating rapidly. Developing such algorithmic systems is spurring growing calls for tech companies to build transparency—or "explainability"—into the systems they design. Employers that adopt such technologies will increasingly face similar pressures. Several Roundtable members opined that if an employee or a member of the public sues a company because of a decision made by an algorithmic system, the company should be prepared to disclose aspects of how the algorithm operates, anticipate defending the lack or impossibility of full transparency, and show evidence of continuing human oversight. Employers should anticipate increasingly finding themselves in litigation defending their AI systems with the outside AI developers.

But the very nature of deep learning and other powerful modern forms of AI makes true explainability, much less full transparency, very difficult or impossible. Several participants commented that a blanket transparency requirement would severely limit innovation and place U.S. and European AI development at a competitive disadvantage. But participants strongly agreed that ethical standards must be applied to AI decision-making and algorithmic biases that violate legal requirements or core values. A more workable and achievable goal that companies should set as they adopt complex machine-learning systems would be focusing less on transparency or on explaining the workings of the algorithmic "black box," but instead on taking a preventive approach. Such a strategy must involve close monitoring of the inputs into such systems, and careful tracking and scrutinizing of the outputs generated from those inputs. Monitoring and periodic auditing will give companies the ability to check whether the algorithms are working as intended and to raise red flags if outcomes are different or unexpected. Having human oversight or control somewhere in the decision-making process is recommended. Several participants suggested acquiring AI programs that have been pre-tested for algorithmic biases on disclosable sample data. Even if true transparency cannot be achieved, companies can reduce their litigation and compliance risks through such proactive measures.

The Value of Informed Regulators and Developing Needed Narrowly Focused Regulations While Minimizing Both Unintended Harm and Disincentives to Innovation

Inquiry 6: How is a workable legislative, regulatory and judicial roadmap developed that identifies needs, respects the role of innovation and considers unintended consequences?

One recurring theme of the Roundtable discussions related to the uncertainty surrounding the regulatory climate for AI and robotics. While the absence of regulatory activity is generally seen as a boon to

innovation, that advantage dissipates when new technologies must comply with preexisting legal frameworks. The consensus of the Roundtable participants is numerous technologies exist that could be deployed in the workplace, but are not being embraced (or used at all) because employers are unsure whether the technologies comply with existing laws. This unsettled regulatory climate has had a negative impact on the deployment of potentially advantageous technologies in some sectors.

For example, a participant explained that until this year, potentially life-saving telemedicine technologies that could have allowed stroke specialists to examine patients in rural areas were effectively banned in Texas—the state with the largest rural population in the country—because the Texas medical board required physicians to have an in-person visit with a patient to establish care. Similarly, algorithmic employee recruitment and selection tools are already available, and many more are in development, that would allow employers to create a more diverse and equitable workforce, but some employers have been reluctant to adopt them because of uncertainty regarding how such tools will be assessed by the federal Equal Employment Opportunity Commission (EEOC) and equivalent state agencies.

Some of this regulatory inaction can be attributed to the regulators' lack of knowledge about the benefits and risk profiles of new technologies. Relatedly, some governmental institutions take a reactive, rather than a preventive, approach to regulation when assessing the novel and unfamiliar. Roundtable participants expressed concern that if regulators do not take a more proactive and preventive approach, legislatures or regulators will act only after a catastrophic event. Governmental institutions may feel political pressure to enact strict and innovation-stifling regulations rather than regulations that account for the benefits of AI and robotics, besides the risks.

All this points to an overriding need for employers, tech companies, and educators to engage with policymakers to educate them on the benefits and risks of the many applications of AI and robotics in the workplace. Helping regulators and policymakers adopt a forward-looking mindset, focusing on prevention rather than correction, will help ensure that regulation enhances, rather than hinders, the competitiveness of American companies.

Part of such an approach could be the creation of regulatory "safe harbors" allowing companies to test novel applications of AI and robotics designed to advance attempts to implement fairer hiring, retention and promotions practices, but where compliance with the letter of the law is unclear in the event of unintended and unanticipated adverse impact on certain protected categories. For example, legislatures, and where constitutionally appropriate, enforcement agencies, could permit companies to use algorithmic hiring tools to identify and recruit promising candidates from disadvantaged protected groups without facing risk of liability for disparate treatment discrimination. Another example could be providing employers a safe harbor against discrimination claims, or at least a strong presumption of compliance with anti-discrimination laws, if a third-party audit of similar algorithmic hiring tools shows no adverse disparate impact on protected groups.

Roundtable members realized that adopting forward-thinking regulations and statutes will be difficult in the current polarized political climate. But with America's economic rivals increasingly prioritizing the development and rapid deployment of new applications of AI, the need to leverage the potential of AI for the greater good of America's workers and companies could represent a rare potential space for bipartisan action. A combination of safe harbors to test tools designed for this greater good, while incentivizing employers to audit AI general population recruiting tools to identify and prevent unlawful discrimination, could gain more bipartisan support than considering the safe harbors separately.

Building a Practical and Ethical Roadmap for AI and Robotics Development While China and Russia Race to Become the World Leaders

Inquiries 7 and 8: Will AI and Robotic competition among governments accelerate the arrival of disruptive technologies in U.S. and EU workplaces? Do existing workplace laws protecting privacy and prohibiting discrimination based on protected categories inhibit U.S. and EU competitiveness?

What are the most important and immediate ethical challenges of AI in the workplace? In recognizing the AI imperative and building a practical roadmap for businesses, what are the best responses to these ethical challenges?

Most Roundtable participants agreed that a titanic global competition has formed regarding AI and robotic research, development, and deployment, both civilian and military. But there is an under-awareness of a new "cold war-type competition and our national priorities are scattered. Russian President Vladimir Putin has announced that the nation that leads in AI will "be the ruler of the world." Similarly, China has announced it will dominate the field of AI and robotics by 2030. A participant—one of the world's leading experts on robotics in China—reported that China's spending on robotics in 2017 increased three times faster than it did in the U.S. The Congressional Research Service identified China as a "leading competitor" in using AI to develop military applications. During the Roundtable, it was reported that a year earlier, China mandated that all advanced civilian technology developments be simultaneously available to the military. Meanwhile, the U.S., some worker-based anti-war groups are challenging the ethics of technology firms developing AI for military projects.

Three key takeaways from the discussion included: (1) The U.S., EU, and their allies hold the advantage in developing AI and robotics, especially from a talent perspective. The U.S., however, lacks a clear awareness of the importance of this competition, has no national priority or spending initiative comparable to China and Russia, has failed to produce adequate number of STEM graduates, and maintains an immigration policy that threatens to erode the talent advantage; (2) Western privacy concerns, especially in biometrics, has slowed development compared to nations such as China, where over half of the country's 1.38 billion population is now in the national facial identification system. Privacy and individualism, however, are key values and would not preclude competitiveness if it became a national priority; and (3) U.S. military leaders know of this challenge and are responding without compromising deeply held ethical mandates, such as keeping the decision to kill under human control.

Participants strongly support the establishment and continuation of ethical standards for AI and robotics in the workplace. Brief reference was made to the Asilomai 23 AI principles sponsored by The Future of Life Institute, which are a set of principles intended to promote the safe and beneficial development of artificial intelligence. The State of California adopted these principles — which include research issues, ethics and values, and longer-term issues — in 2017. One of the Littler-participating attorneys contributed to the development.

During the Roundtable, a new term was advanced: "algorithmic workplace governance." This term evolves from the phrase "algorithmic governance." Essentially, under this form of governance, algorithms are used to make key decisions that enforce processes and values of the society. For example, in Russia and China, the form of central government and government control can be enhanced by algorithms programed to enforce established government policies. With digital identification, this technology has the potential to be a complete police force. Through cameras and other data sources, regulations and laws can be enforced without human involvement. This places great power in the hands of the few who make and program the rules.

Applying this principle to the workforce, algorithms could decide who is hired, where the worker is assigned, monitor worker performance, identify any infractions of workplace rules, decide who deserves promotion, establish and administer compensation levels, and identify who is to be laid off or terminated. While some fairness advantages come from such a world, it removes human decision-making and maximizes worker control. Participants viewed our workplaces as primarily remaining under human control; this was more consistent with a form of democratic workplace governance. Reserved for a future Roundtable is whether the workforces of 2020 and beyond would benefit from some elements of objective AI-tested selection, such as for promoting diversity, while continuing to benefit from human, outside-the-box decision-making.

Littler®

ABOUT LITTLER: Littler is the largest global employment and labor law practice, representing management in all aspects of employment and labor law and serving as a single-source solution provider to the global employer community. Consistently recognized in the industry as a leading and innovative law practice, Littler has been litigating, mediating and negotiating some of the most influential employment law cases and labor contracts on record for more than 75 years. Littler Global is the collective trade name for an international legal practice, the practicing member entities of which are separate and distinct professional firms. For more information visit littler.com.