June 28, 2023

Mr. Alan Mislove
Assistant Director for Data and Democracy
Office of Science and Technology Policy
Washington, DC 20500

RE: **Request for Information: Automated Worker Surveillance and Management (88 FR 27932; Document ID OSTP-TECH-2023-0004-0001)**

Dear Mr. Mislove:

HR Policy Association submits these comments in response to the request for information (RFI) from the White House Office of Science and Technology Policy (OSTP), regarding the use of automated tools in the workplace[1].

HR Policy Association is the lead public policy association of chief human resource officers (CHROs) representing nearly 400 of the largest employers doing business in the United States and globally. Our member companies employ more than 10 million individuals in the United States and are committed to maintaining a culture of trust in the workplace, especially as it relates to workforce data. Our organization and our members provide a unique perspective on the current and future role of automation in the workplace and the potential of automated systems, including those using artificial intelligence (AI) to assist companies in making employment decisions and communicating with their workforce.

The swift growth of automation technology raises substantial questions about how laws and regulations can promote the advancement of trustworthy AI technology and maximize its benefits while mitigating risks. Association members are committed to using technology in the workplace in a transparent and nondiscriminatory fashion. It is imperative, therefore, that prior to making consequential regulatory decisions about the use of automated systems in the workplace, policymakers engage regulated entities and other stakeholders to ensure that any future decisions are based upon the most current, accurate information possible about the current and anticipated state of AI technology and its societal implications.

The Request focuses specifically on the use of automated tools by employers to "surveil, monitor, evaluate, and manage" workers. While the Request acknowledges that automation may be used for a wide range of purposes in the workplace, it focuses on those tools which "pose risks to workers and may even violate labor and employment laws."

HR Policy Association members do not condone unreasonable and intrusive surveillance that serves no business purpose and does nothing to improve the workplace experience for employees. Employers are not seeking to create an environment where every employee action is tracked, and

[1] Request for Information; Automated Worker Surveillance and Management, 88 Fed. Reg. 27932-27936 (May 3, 2023)

where worker privacy is not valued. Rather, our members are committed to reasonable and ethical use of AI that can assist companies with ensuring a safe workplace, mitigate risks to workers and the business, and assist in compliance efforts with various local, state, federal laws, and regulations, and promote legitimate employer production and quality goals. Additionally, AI tools can be used to help companies boost workforce diversity and build a more inclusive workplace.

Background

The capabilities of AI and the pace at which AI is being developed present considerable opportunities and challenges for employers and workers. If properly incorporated into the workplace, AI has the potential to improve the employee experience for all employees and expand opportunities for job candidates who may not otherwise be on the radar of hiring managers. For example, AI can be used to analyze the demographic composition of a workforce and compare that data across industries and regional statistics. These insights allow companies to detect any disparities across race, ethnicity, age, gender, disability, veteran status, and many other factors. Other AI tools may help companies identify additional qualified applicants for employment, better track employee attrition rates, and enhance employee feedback mechanisms which can improve retention, professional development and hiring processes.

In the context of human resources, AI is most effective when it is used to augment, not replace, the core responsibilities of recruiters and hiring managers and the processes that they go through to source job candidates, analyze candidate profiles, and ultimately make hiring decisions. Companies are already incentivized to hire good candidates and to use AI tools appropriately to inform those decisions. A recent assessment by Accenture found that a poor hire can cost companies up to 5x the annual salary of that hire.[2] AI tools can help expand the talent pool for employers, making it more likely that companies can hire individuals that will be successful and contribute positively to the organization.

However, the complex nature of AI technology and the potential for its misuse also raise a number of risks for companies. For example, a failure to guard against harmful biases in talent identification algorithms, or biases in the datasets that train AI, could undermine efforts to create a skilled and diverse workforce. HR professionals are acutely aware of these risks, given their longstanding responsibilities to prioritize employee safety and privacy and to ensure that any employment decisions are in compliance with labor and employment laws.

To build trust and support worker recruitment and retention, employers are committed to preventing bias in the workplace. Companies are fully aware that any instances of harmful bias in the hiring process can undermine worker confidence and damage the reputation of the business. Reputational damage alone may negatively impact a company's efforts to assemble and retain a competitive workforce and, according to past studies, may cost companies as much as 10% in additional costs per hire.[3] The use of AI, or any other technology, does not inherently diminish or change the commitment of employers to eliminate bias and use AI tools appropriately within their organization. Indeed, use of automated tools can help to reduce bias in recruitment and hiring.

As AI tools further permeate business and society, employers will proactively take steps to ensure that AI algorithms are acting as intended and not creating harmful outcomes. Companies know that their reputation and public trust could be irrevocably damaged if AI tools were

[2] Chambliss, Corey; Vaughan, Kristen. "Next generation talent assessment." Accenture.
[3] Burgess, Wade. "A Bad Reputation Costs a Company at Least 10% More per Hire." Harvard Business Review, March 29, 2016. https://hbr.org/2016/03/a-bad-reputation-costs-company-at-least-10-more-per-hire

deployed in a manner that caused harm to employees or discriminated against workers and job candidates. Such a loss of trust would set back a company's ability to use AI, which could make the company less competitive and dynamic in the future.

Reasonable Use of Automated Workplace Monitoring Tools

HR Policy Association recently surveyed our members to assist policymakers in understanding how automation is used in the workforce management and surveillance context.

According to the Association's member survey, conducted in June, most respondents use AI and automated tools in the workplace that are tailored to their respective company's needs. The tools are mainly used for HR purposes such as to source and screen job candidates and enable employee self-services such as looking up company policies or benefits.

While the majority of respondents indicate that they plan to increase usage of AI and automation in the next year, they do not anticipate freezing hiring for AI-impacted roles. Of significance, companies that utilize AI and automated tools do not use automated tools to make decisions without human input.

Of relevance to the OSTP's request for comment, most respondents indicate that they do not use data from monitoring tools to inform employment decisions. The information is used to provide constructive feedback to employees regarding general performance. Furthermore, most companies provide notice to employees who are being monitored using automated tools, contrary to what this request for comment purports.[4] Finally, a majority of respondents indicated that they only review monitoring data for performance assessment purposes, and that they do not otherwise monitor available information on a continuous or ongoing basis.

Automation can assist employers in achieving several key priorities, including:

Ensuring Safe Workplaces

Creating a safe environment for employees and customers is a necessity for any company. Automated monitoring tools can assist businesses with this fundamental responsibility in a much more efficient and effective manner than manual approaches. Indeed, most of our survey respondents indicate that they use automated monitoring tools to track employee movement and location (e.g., staff badges, facial recognition, vehicle monitoring) for safety purposes. For example, a security camera system that utilizes AI technology can be deployed to ensure that no unauthorized personnel enter certain premises, and that the company is able to respond in real time to suspicious behavior. In transportation related or adjacent industries, monitoring tools are essential for tracking employer-owned vehicles operated by employees, both for employee safety and performance purposes. The Request itself cites several ways in which AI may be appropriately used to enhance worker, customer, and community safety. For example, monitoring the speed and acceleration habits of delivery or rideshare drivers can help encourage safer driving habits and lead to fewer accidents or traffic violations. In general, it is essential that employers are aware of whether an employee is endangering themselves or others while on the job. Such information can also be used to rebut improper claims by third parties against companies and their employees in traffic accident matters and provide necessary safety/quality feedback.

[4] Quote the relevant text.

Identifying patterns of potential misbehavior, including harassment or other abusive behavior, can also be enhanced by automated systems. In certain industries, AI can also be used to monitor and maintain oversight of controlled substances that the organization may manufacture or distribute, thereby lowering the chances that powerful drugs may end up in the wrong hands. For example, automated monitoring tools are essential in healthcare settings, where employees are often charged with handling significant amounts of controlled substances. Losing track of such substances can create significant safety issues for the employer, their employees, their consumers, and the general public. Even something as simple as tracking and ensuring patients are receiving the right drugs and the right doses of such drugs can be better accomplished with the help of automated monitoring tools.

Ensuring and Measuring Productivity

Tracking and measuring productivity is not a new concept for employers, and companies have been using technology to assess productivity long before AI became a focus of policymakers. Employers understand, however, that measuring worker performance must be done within reason and not improperly surveil the daily activities of individuals.

As workplaces have increasingly become more digital and employers are adopting hybrid or fully remote long-term work plans, it is essential that employers be able to use automated systems to measure worker performance. New regulations that prohibit or severely disincentivize the use of such tools could prevent employers from tracking progress in a supply chain or from various workstreams that involve multiple departments within an organization.

As noted above, our survey indicates that our member companies do not – at least for productivity and performance measuring purposes – use such tools to constantly and continuously monitor or surveil employees. Instead, data is primarily only reviewed for periodic performance assessments, and generally used to provide constructive feedback and coaching as necessary. Our survey indicates that our member companies generally do not use data from monitoring tools to inform any employment decisions. When this data is used in that fashion, it is generally only used to supplement human input and decision-making, and not as the sole basis for any employment decision. Finally, and perhaps most importantly, those member companies that do use automated systems for monitoring purposes overwhelmingly provide their employees with advance notice of such monitoring.

Risk Mitigation and Ensuring Compliance with Legal Requirements

Employers are subject to a host of federal and state laws regarding safety requirements, labor practices, anti-discrimination statutes, and other standards that require companies to have robust compliance systems. Companies must regularly monitor legal and regulatory developments that impact their organization and industry in order to consistently maintain compliance with these laws and regulations.

Employers – particularly larger companies – must regularly collect and analyze vast amounts of data for either recordkeeping or purposes of reporting to a government agency. Automated tools can make these processes more efficient, reduce human error, and improve compliance for companies in every industry. As one law review article from 2010 stated: “Given the scale and complexity of contemporary business institutions and the massive amount of information involved in corporate operations, the types of risk controls that regulation demands simply

cannot function without the data collection, analyzing, and monitoring capacities of integrated computer technology."[5] The automated tools that exist today will only help make risk monitoring and compliance more efficient and effective for employers.

HR Policy Association Principles

In 2020, HR Policy Association recommended to our members a set of principles on the use of employee data and AI as a framework and starting point for companies to leverage in their own work environments. Companies understand the need to be open and responsive to their employees and customers regarding AI and any automated tools which a business may use. Given heightened public anxiety over the use and growth of AI, businesses recognize the opportunity they have to lead and ensure that AI can be a force for good in the economy and which can help create a better future for employers and workers.

We encourage OSTP to consider these principles as they develop any final policy recommendations:

- **Privacy and Security:** Most companies maintain privacy policies applicable to current and prospective employees and tailor such policies to comply with jurisdiction-specific privacy regulations in the U.S. and abroad (e.g., the European Union's General Data Protection Regulation). Principles for the use of data and AI should include a statement specific to employee privacy and security and may explicitly state that data may not be used for the purpose incompatible with the specific purpose for which it was collected without employee consent.
- **Transparency:** The intended uses of data should be able to be clearly understood, explained, and shared, including the impact on decision-making and the processes for raising and resolving any issues. In some cases, this may include an explanation of the algorithms involved in machine learning assisted analysis and how those algorithms are developed and "trained" to analyze employee data.
- **Integrity:** The principle of integrity is interpreted in a variety of different ways by companies according to their culture but is rooted in the concept of "positive intent." In addition to committing to the use of data in a highly responsible way, companies may also specify that the purpose of all automation and AI is to augment and elevate humans rather than replace or diminish them, and that data usage should be sensitive to cultural norms and customs and aligned with company values.
- **Bias:** Although AI has been touted as the solution to unintended bias in many people-related processes, such as hiring, performance management and promotion, there is inherent risk of unintentional bias occurring within AI algorithms or the datasets used to train them. Principles around data and ethics should commit to continuous monitoring and correction for unintended bias in machine learning.

[5] Bamberger, Kenneth A. Technologies of Compliance: Risk and Regulation in a Digital Age. Texas Law Review, March 2010.

- **Accountability:** Companies should be accountable for the proper functioning of automation and AI systems and for unintended foreseeable consequences arising out of its use. Companies should ensure that everyone involved in the lifecycle of the technology is trained in ethics and that ethics is part of the product development and operation of an automated system. This may include the coders and developers responsible for creating the software, the data scientists responsible for training it, or the management of the company. Further, companies should develop governance and training mechanisms to ensure that automated systems and AI are developed responsibly.

Substantial Existing Law Already Applies to the Use of AI in the Workplace

The use of technology in the employment context is already subject to extensive regulation which should be taken into consideration when developing any additional protections. In the United States alone, federal and state laws dealing with anti-discrimination, labor policy, data privacy, and AI-specific issues affect the use of AI in the employment context.

These areas of law include:

- **Anti-Discrimination:** Title VII of the Civil Rights Act prohibits discrimination in the employment context on the basis of race, color, religion, national origin, or sex. An employer can violate Title VII for disparate treatment or disparate impact. Disparate treatment occurs when similarly situated people are treated differently based on a protected class. Disparate impact occurs when facially neutral policies or practices have a disproportionately adverse impact on protected classes. Discriminatory intent is relevant to establish a claim of disparate treatment, but intent is not necessary for claims of disparate impact. Employers are also prohibited from unlawfully discriminating in the employment context based on age or disability due to the Age Discrimination in Employment Act and the Americans with Disabilities Act.

  Liability for discrimination may arise under anti-discrimination laws when employers use artificial intelligence systems that are trained on biased datasets or that infer or otherwise uncover protected class information and adversely impact members of the protected class. With respect to anti-discrimination measures, any new government guidelines should be co-extensive with existing anti-discrimination laws instead of imposing novel obligations that exceed existing law.

  In fact, the U.S. Equal Employment Opportunity Commission (EEOC) recently released a technical assistance document explaining the application of Title VII of the Civil Rights of 1964 in preventing employer discrimination when using automated systems.[6] As that document explains, the 1978 EEOC Uniform Guidelines on Employee Selection Procedures "would apply to algorithmic decision-making tools when they are used to make or inform decisions about whether to hire, promote, terminate, or take similar actions toward applicants or current employees."

[6] "Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964." Equal Employment Opportunity Commission (May 18, 2023)

In other words, existing law can in many instances be applied to the use of AI in the workplace. Any new guidelines or policy proposals from OSTP or other government bodies should be fully aligned with guidance from the EEOC and other agencies that promulgate AI workplace-related proposals.

- **Labor Laws:** The National Labor Relations Act (NLRA), enforced by the National Labor Relations Board (NLRB), is the cornerstone of American federal labor law and guarantees the right of private sector employees "to organize, engage with one another to seek better working conditions, choose whether or not to have a collective bargaining representative negotiate on their behalf with their employer, or refrain from doing so.[7]" The National Labor Relations Act prohibits employers from interfering with, restraining, or coercing employees' exercise of Section 7 rights, including spying (i.e., doing something out of the ordinary to observe the activity) or giving the appearance of spying on employees' union activities.[8]

  On October 31, 2022, NLRB General Counsel Jennifer Abruzzo issued a memorandum addressing Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights. In the memorandum, the General Counsel announced she will urge the NLRB to adopt a new framework to protect employees from intrusive or abusive electronic monitoring and automated management practices that would tend to interfere with an employee's protected activity by vigorously enforcing current law and applying settled labor law principles in a new framework[9]. The General Counsel has also made clear that the NLRB is committed to an interagency approach to these electronic monitoring and automated management practices issues. To that end, the General Counsel signed agreements with the Federal Trade Commission, the Department of Justice, and the Department of Labor which will facilitate information sharing and coordinated enforcement on these issues.

  The NLRB has taken the General Counsel's instruction seriously. On April 11, 2023, the NLRB found that an employer violated the NLRA by creating an unlawful impression of spying when it viewed camera footage of an employee who was on his lunch break, even though the employee was not engaged in protected concerted activity[10].

  While it is important to recognize and monitor these developments, care should be taken by regulators to balance the rights of employers to monitor their workplace for legitimate non-discriminatory reasons with the rights of employees under Section 7 of the NLRA. Specifically, employers should not have to establish any "special circumstances" to implement carefully tailored necessary workplace monitoring policies.

- **Data Privacy Laws:** Data privacy laws at the federal and state level directly affect the use of technology in the employment context. Federally, the Fair Credit Reporting Act (FCRA) regulates, among other things, how consumer reporting agencies use and share consumer information. A "consumer report" is defined as information bearing on a consumer's credit worthiness, including information related to a consumer's credit standing, credit capacity,

---

[7] https://www.nlrb.gov/about-nlrb/who-we-are
[8] https://www.nlrb.gov/about-nlrb/rights-we-protect/the-law/interfering-with-employee-rights-section-7-8a1
[9] https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and
[10] Stern Produce Company, Inc., 372 NLRB No. 74 (2023)

character, general reputation, personal characteristics, or mode of living. The FCRA requires consumer reports to be used for only permissible purposes, such as for employment. Employers must provide disclosures and obtain consents if using consumer reports.

In addition to the FCRA, employers must also navigate biometric information privacy laws in numerous states. For example, the Illinois Biometric Information Privacy Act (BIPA) prohibits organizations, including employers, from collecting and using biometric information unless they have provided notice and obtained written consent.

Policymakers must be careful to consider these existing laws that can be applied to the use of AI and automated tools, just as they apply to other technologies employers may use in connection with their workforce. Regulators should not rush forward with sweeping, overly prescriptive, one-size-fits-all new rules that will impede investment and innovation in AI, and disincentivize employers from leading efforts to promote responsible uses of automated tools.

Conclusion

While automation and AI has generated a number of important and difficult questions regarding its role in the workplace, policymakers should avoid rushing new regulations into place that could stifle investment in such tools and limit the ways the technology can be used to improve the work experience and livelihood of millions of workers. While employers recognize the opportunity that creates for them to operate better workplaces, they also recognize the responsibility that comes with automation deployment and the importance of employee safety and privacy. Employers will continue to lead the way when it comes to developing appropriate automation standards and ethical practices.

Finally, from a public policy perspective, any new regulations considered by federal agencies must be subject to a robust formal notice-and-comment procedure under the Administrative Procedure Act and take the views of all stakeholders into account. Rules based upon unproven theories or insufficient evidence and data would be counterproductive and undermine many of the private sector initiatives currently underway to promote the responsible use of automation. Careful balancing should occur to ensure that employer rights are considered on an equal basis with employee rights.

HR Policy Association appreciates this opportunity to comment and looks forward to serving as a resource on these critical issues. If you have any questions about the Association's comments, please feel free to contact me at Cbirbal@hrpolicy.org.

Sincerely,

Chatrane Birbal

Chatrane Birbal
Vice President, Policy and Government Relations
HR Policy Association
cbirbal@hrpolicy.org