HRPA HR POLICY ASSOCIATION®

June 12, 2023

VIA Electronic Delivery

Mr. Travis Hall
Deputy Associate Administrator
National Telecommunications and Information Administration
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: AI Accountability Policy Request for Comment (NTIA-2023-0005)

Dear Mr. Hall:

HR Policy Association appreciates this opportunity to provide our views in response to the National Telecommunications and Information Administration's request for comment on Artificial Intelligence (AI) system accountability measures and policies (Request).

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 about the current and future potential of AI in the workplace to further assist companies in making employment decisions and interacting with their workforce.

Background

The capabilities of AI and the pace at which AI is being developed present considerable opportunities for employers and workers. If properly incorporated into the workplace, AI has the potential to improve the work experience for all employees and expand opportunities for job candidates who may not otherwise be on the radar of hiring managers. For example, there have been cases of AI being used to analyze the demographic composition of a workforce and compare that data with regional demographic data across industries. These insights allow companies to detect any disparities across race, ethnicity, age, gender, disability, veteran status, and many other factors compared to the local market. Other AI tools may help companies 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 will be most effective when it is used to augment, not replace, the core responsibilities and processes that recruiters and hiring managers go through to source job candidates, analyze candidate profiles, and ultimately make hiring decisions. Companies already have a major incentive 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.[1] 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 bias in talent identification algorithms 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 employment decisions companies make comply 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 a competitive workforce and, according to past studies, may cost companies as much as 10% in additional costs per hire.[2] The use of AI, or any other technology, does not diminish or change the commitment of employers to eliminate bias within their organization.

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

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. We encourage the NTIA to consider these principles, and the proactive steps companies are taking with regard to AI, as NTIA develops any final policy recommendations:

- o **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.,* EU'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 a purpose incompatible with the specific purpose for which it was collected without employee consent.

- o **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

---

[1] Chambliss, Corey; Vaughan, Kristen. "Next generation talent assessment." Accenture.
[2] 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

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 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.

- **Accountability:** Companies should be accountable for the proper functioning of 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 AI 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 AI is developed responsibly.

HR Policy Association recently surveyed our members to assist policymakers in understanding how AI tools are used in the workplace.

According to an HR Policy Association member survey conducted in June 2023, most respondents use AI and automated tools in the workplace that are tailored to their respective company's needs. The tools are used for legitimate business and HR purposes, including to source and screen job candidates and enable employee self-service such as looking up company policies or benefits.

Of significance to NTIA's request for comments, the majority of our survey respondents indicate that ensuring accountability for the use of AI faces obstacles primarily due to a lack of generally accepted standards to audit/assess against; third party vendors that lack adequate data or are unwilling to share information that would enable independent review; lack of a federal law focused on AI systems; and the absence of a safe harbor for employers to protect themselves when acting in good faith.

AI Accountability Policies (Questions 30-34 of the Request)

The Request seeks input regarding the role of government policy and regulation in overseeing AI and what types of accountability measures should be mandated by government agencies. As a threshold matter, it is important to consider that AI is being used in markedly different ways by companies with regard to workplace matters and hiring practices. Each of the different ways in which AI may be used in the workplace presents different levels of risk which should be reflected in any future efforts by regulators.

For example, using facial recognition technology during interviews or deploying GPS tracking features on a company-owned vehicle present different levels of risk to employee privacy and security than AI-powered predictive text tools, or using AI to compare workforce statistics across different regions of the country. Regulations that treat every use of AI the same from a risk standpoint would be counterproductive and limit the ability of companies to use AI effectively.

Policymakers should also consider the rapid growth of AI when developing rules or guidance to oversee the use of AI in the economy. According to a recent report, the number of businesses using AI has more than doubled since 2017. The average number of AI capabilities that organizations use has also doubled over the last four years.[3] Regulations should promote innovation in AI technology and must be able to adapt to the evolution of AI use and not become stale over time.

Accordingly, regulators should avoid adopting a one-size-fits-all, rigid approach towards overseeing and regulating AI, particularly those aspects of AI which are used by employers to improve the productivity and diversity of their workforce. Instead, policymakers should adopt a more risk-based approach towards regulation. AI applications that involve little risk to personal privacy or safety should not be subjected to heightened standards that may be more appropriate for other applications.

Harmonization Between Federal and State Regulations

Question 34 of the Request also raises several important topics regarding regulatory harmonization and the possibility of state, federal, and international regulations conflicting with one another. We believe that this should be a major area of focus for regulators, as businesses could eventually find themselves in a situation where being in compliance with one set of standards or regulations (*e.g.,* those adopted by the federal government) may mean they are out of compliance with standards or regulations of another jurisdiction (*e.g.,* laws adopted by an individual state). New regulations may also conflict significantly with widely accepted employer best practices regarding the use of AI applications.

HR Policy Association urges policymakers to align, when possible, any new guidelines or standards for AI with existing government policies and commonly adopted employer best practices. Any government guidelines on the use of AI in the employment context should be aligned with regulatory expectations across the federal government.

---

[3] "The state of AI in 2022 – and a half decade in review" McKinsey (December 6, 2022)

Government guidelines should also be compatible with existing processes, procedures, and policies that employers have established to comply with the patchwork of state, federal, and international laws affecting the use of innovative technologies in the employment context. Companies have invested significant resources to develop compliance policies and procedures, and employers should be able to leverage these governance structures when aligning with the recommendations of the NTIA.

<u>Substantial Existing Law Already Applies to the Use of AI in the Workplace</u>

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 AI applications.[4] 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."

  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 NTIA or other government

---

[4] "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)

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.[5]". 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. Consequently, employers subject to the NLRA must already ensure that workforce surveillance and management tools, including those using automation, do not interfere with, restrain, or coerce employees in the exercise of their labor rights. Any new government guidelines should therefore be compatible with the NLRA.

Moreover, 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.[6] 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.[7]

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.

- **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, character, general reputation, personal characteristics, or mode

---

[5] https://www.nlrb.gov/about-nlrb/who-we-are
[6] https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and
[7] Stern Produce Company, Inc., 372 NLRB No. 74 (2023)

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.

<u>State Law</u>

An increasing number of state and local laws are also directly regulating the use of artificial intelligence in the employment context. The Artificial Intelligence Video Interview Act (AIVIA) in Illinois, for example, requires transparency, consent, and certain government reporting from employers who require candidates to record an interview and use artificial intelligence to analyze the submitted videos.

In December 2021, the New York City Council enacted a law requiring companies to obtain independent audits of certain algorithms used in the employment context. The New York law also prohibits the use of "biased" algorithms, although the law does not define the term. The new law raises several significant unaddressed concerns, including that immature technical standards may not be robust enough to address concerns around bias and therefore may deepen rather than address mistrust, and mandating third-party assessments will infringe on the privacy and security of personal information and potentially on confidential business information and IP rights.

We believe that the federal government should coordinate its efforts to promulgate guidelines and requirements on artificial intelligence in the employment context. Where possible, we encourage NTIA to look for ways to promote consistency between federal and state efforts.

Third Party Audits/Assessments

The Request seeks input as to whether audits or assessments – including those conducted by an external organization – should be "folded into" accountability mechanisms for AI systems.

At this time, guidelines on the use of artificial intelligence in the employment context should not require employers to undertake third party assessments or audits. Mature, auditable, and accepted standards to evaluate bias and fairness of AI systems do not yet exist despite ongoing efforts at the National Institute of Standards and Technology, the International Organization for Standardization, and industry associations. In fact, the Request itself notes that "for some features of trustworthy AI, consensus standards may be difficult or impossible to create."[8]

Until such standards are matured and accepted, assessment and audit outputs may be inconsistent (and thus ineffective at promoting fairness) cause companies to forgo innovative technologies in

---

[8] 88 Fed. Reg. 22437

the employment context despite their clear benefits, or inadvertently deepen rather than alleviate distrust in such systems. Moreover, there are concerns that mandating third-party assessments will infringe on the privacy and security of personal information and potentially on confidential business information and IP rights.

Conclusion

HR Policy Association appreciates this opportunity to comment and provide our perspective regarding AI accountability. While AI creates substantial opportunities for employers to improve the daily experience of workers, employers are also well aware of the responsibilities and potential risks that come with the growing use of AI. Accordingly, employers will continue to lead the way when it comes to developing appropriate AI standards and ethical practices.

From a public policy perspective, any new regulations considered by federal agencies must be subject to a robust notice-and-comment period and take the views of all stakeholders into account. Rules based upon 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 AI.

HR Policy Association looks forward to serving as a resource for the National Telecommunications and Information Administration and to policymakers on the critical and ever evolving issue of AI. If you have any questions about the Association's comments, please do not hesitate to contact us at www.HRPolicy.org.