

Federal Register Notice 86 FR 56300, <https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies>, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

COMMENTS BY HR POLICY ASSOCIATION

TO THE

WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

REQUEST FOR INFORMATION ON

PUBLIC AND PRIVATE SECTOR USES OF BIOMETRIC TECHNOLOGIES

Docket No. 2021-21975

JANUARY 14, 2022

Introduction: Thank you for the opportunity to lend our perspective in this critical area. HR Policy Association is the lead public policy organization of chief human resource officers (CHROs) representing more than 400 of the largest employers doing business in the United States and globally. The Association convenes these executives not simply to discuss how human resource practices and policies should be improved, but also to help create and promote HR strategies and initiatives for diverse and inclusive workforces. Collectively our members employ more than 20 million employees worldwide and have a market capitalization of more than \$7.5 trillion. In the United States, Association members employ over 9 percent of the U.S. private sector workforce.

In these comments we will seek to provide insights on employer activities related to topic 6 of the RFI: “Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case.” We will focus our comments on subitem A: “stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies,” though our comments will have implications for several other areas noted in topic 6, including in subitems C, D, E, and F. We will also provide background on employer motivations for ensuring the ethical and responsible use of AI, including biometric technologies.

There is a premium on talent during the economic recovery from COVID. At the time of writing, the labor force participation rate is 61.8%, with the difference from the February 2020 rate of 63.3% representing the absence of millions of workers. Much of this loss reflects the impact of COVID on women and workers over 55 who have largely been pulled out of work by childcare responsibilities and early retirement, respectively. Black and Latino or Hispanic individuals have experienced unemployment rates much higher than other demographic groups throughout the pandemic, with Black women especially dropping out of the labor force at a much higher rate than any other group since schools reopened in August of 2021.¹ Also hard hit were workers without a college degree, whose labor force participation rate is far below even the current average while those with a bachelor’s degree is much higher. In the U.S. alone there are 11 million job openings, with only 6.9 million unemployed Americans to fill them.

Consumers feel these shortages in terms of empty store shelves and rising prices. For example, longshoremen and truck drivers needed to move consumer goods are in short supply in many places in the world as record numbers of container ships have become stuck along Los Angeles, Long Beach, and other key U.S. ports in 2021. Over the last 12 months, the Producer Price Index has soared above an also rising Consumer Price Index as consumer demand has remained

¹ Barr, Anthony, Makada Henry-Nickie, and Kristen E. Broady. “The November Jobs Report Shows Black Women Are Leaving the Labor Force.” Brookings, December 9, 2021. <https://www.brookings.edu/blog/the-avenue/2021/12/08/the-november-jobs-report-shows-black-women-are-leaving-the-labor-force/>.

strong among worker shortages. According to a recent survey of local chamber of commerce leaders, more than 90% reported that lack of available workers is holding back the economy in their area and less than 1% reported it is easy to fill jobs.²

For large companies, attracting and retaining diverse talent and achieving the right culture is a core component of their business strategies and the economic recovery. Even as the labor shortage persists, large companies are seeking to attract, train, advance and retain diverse talent and cultivate inclusive workplace cultures. In the most recent HR Policy survey of CHRO priorities, diversity and inclusion ranked as the top concern. The three priorities that followed are related: cultural transformation in anticipation of the post-COVID work environment; executive development, including critical role succession; and talent management, including recruitment and retention. Digitization of the workplace followed as the fifth highest concern out of 20 total possible responses.

Large employers' commitment to Diversity, Equity and Inclusion (DE&I) goes beyond numerical requirements imposed by federal policy—companies are implementing workforce strategies to create respectful work environments that foster a vibrant diversity of perspectives represented at every level of the organization. Such a balance leads to a more productive workforce and better business outcomes.

DE&I has also increasingly come to be seen as material to business performance by outside stakeholders, including institutional investors. Investors are considering environmental, social, and governance (ESG) disclosures as a potential information source for extracting a competitive advantage, especially over the long term. Companies are integrating ESG as a remunerative facet of their business models—and as a risk management strategy.

Finally, it is worth noting that for large companies with operations throughout the U.S. and globally, DE&I efforts are also designed to ensure that the workforce reflects the company's diverse geographical footprint and customer base. Not surprisingly, companies operating on a global level face a more complex challenge in promoting diversity and inclusion. The challenge manifests on two levels—one within the country where operations exist and the other involving the company's global employee population. With regard to the first, there are varying legal requirements in the jurisdictions within which companies may operate. In fact, diversity-related legal requirements in most countries outside the U.S. often focus exclusively on disability and gender, with little or no attention paid, for example, to ethnicity or nationality. Yet, for all the reasons stated previously, the absence of legal requirements typically does not stop companies from working to apply their own cultural diversity and inclusion imperatives wherever they have employees.

² "The America Works Report: Quantifying the Nation's Workforce Crisis." U.S. Chamber of Commerce, October 25, 2021. <https://www.uschamber.com/workforce/education/the-america-works-report-quantifying-the-nations-workforce-crisis>.

Artificial intelligence has the potential to further enhance the employee experience and expand employment opportunities to underrepresented populations. For example, AI solutions to analyze demographic composition of a given workforce, comparing against industry or regional demographic statistics, are beginning to emerge. Such insights can help companies detect disparities across race, ethnicity, age, gender, disability, veteran status, and other identities, while also diving deeper into intersectional indices. Other platforms may track employee attrition rates and enhance employee feedback mechanisms to detect areas where a company may have an opportunity to implement diversity and inclusion initiatives.

Many employers utilize AI-powered tools to augment recruiters and hiring managers' efforts in sourcing job candidates, increasing efficiency significantly while helping ensure diverse slates of qualified candidates for consideration. (According to an Accenture study, a poor hire can cost up to five times the annual salary of that person.³ A good hire, on the other hand, increases productivity, improves morale, and enhances a company's image as a good employer.) In other cases, employers are using AI-powered tools to identify and remove language on job descriptions that appears to reflect unconscious bias or requirements that are not necessary for the job. The use of such capabilities allow employers to access wider talent pools and begin building talent pipelines of underrepresented populations in ways not previously accessible.

Nevertheless, AI is an evolving technology and therefore careful attention must be paid to weigh benefits against potential risks. Use cases for AI in the workplace vary widely, with risk profiles that vary considerably both in scope and in kind. In addition, the types of data used are different—indeed there are many uses of AI in the workplace that do not rely on biometric data, and many HR tech vendors do not work on biometric information at all.

HR Policy members are aware that, if not implemented and used responsibly, artificial intelligence has the potential to produce adverse outcomes. In the HR context, this particularly means a focus on fairness, privacy, and safety. Even companies with a record of successes in terms of diversity and inclusion within their workplaces must wage a continuing battle against unconscious bias, which can be a barrier among hiring managers during sourcing and talent acquisition processes and can negatively impact diversity efforts.

There is legitimate concern that inaccurate, incomplete, or unrepresentative data potentially can amplify, rather than minimize, bias. Other seemingly objective data may prove misleading—for example, metrics on who leaves the workforce may not take into account that the cause could be a hostile work environment. Moreover, the manner in which certain technologies are deployed, and the practices surrounding use of such technologies, may propagate or create patterns of bias, even in circumstances where the technology is deployed in order to help eliminate bias and while giving the illusion of objectivity.

³ Chambliss, Corey; Vaughan, Kristen. "[Next generation talent assessment](#)." Accenture.

AI-enabled tools powered by biometric data could carry their own set of serious risks. Programs to track facial movements and speaking patterns in interview settings may score a candidate inaccurately due to demographic differences. Facial recognition tools have often scored poorly in accuracy tests for those with darker skin, and particularly darker-skinned females.⁴ Recently, a Facebook algorithm prompted viewers of a video featuring Black men in confrontation with white individuals, including law enforcement, to “Keep seeing videos about Primates.”⁵

In order to build trust and support worker attraction and retention, large employers are committed to the prevention of bias in the workplace. Reputational damage alone may detrimentally impact a company’s efforts to assemble a competitive workforce, and may cost employers as much as 10% in additional cost per hire.⁶ Other potential negative outcomes may be produced by the misapplication of AI in the work context, which could undermine efforts to establish an inclusive corporate culture. Notwithstanding regulatory concerns, in practice the impact of poorly used AI affects both employers as well as current and potential employees. With a loss of trust, companies would face significant challenges deploying even responsible uses of AI to increase efficiency, enhance the worker experience, and support their DE&I efforts.

Regulatory activity and the consideration of such in this area is beginning to emerge. In addition to the White House’s initiative to create an AI Bill of Rights, last November the Equal Employment Opportunity Commission launched an initiative to ensure that artificial intelligence and algorithmic decision-making tools “do not become a high-tech pathway to discrimination,” according to Chair Charlotte Burrows. Meanwhile, the Federal Trade Commission is considering rulemaking to “ensure that algorithmic decision-making does not result in unlawful discrimination.” At the state and federal level, legislation is being considered to provide worker protections against discrimination through the use of AI, with several noteworthy measures already having passed at the state level.

Examples of employer-driven efforts to promote ethical and responsible use of AI: Business leaders and NGOs recognize the importance of building trust regarding the use of AI, and more importantly of avoiding deploying artificial intelligence in ways that discriminate or otherwise undermine corporate business objectives. There are many current examples of employer-driven efforts to ensure AI is used ethically and responsibly, several of which HR Policy Association has led or participated in. Below are examples of just some of these initiatives.

- **HR Policy Association AI principles for company adoption:** In 2020, HR Policy Association recommended to our members a set of principles on the use of employee

⁴ Najibi, Alex. “Racial Discrimination in Face Recognition Technology.” Science in the News, October 26, 2020. <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>.

⁵ Mac, Ryan. “Facebook Apologizes after A.I. Puts 'Primates' Label on Video of Black Men.” The New York Times, September 3, 2021. <https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html>.

⁶ 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>.

data and AI as a framework and starting point for companies to leverage in their own work environments. These principles include:

- **Privacy and Security:** Although most companies currently have an existing data privacy policy, such policies are often broad in scope or geared toward customers and consumers. 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 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, the risk of unintentional bias occurring within AI algorithms or the datasets used to train them is concerning. Principles around data and ethics should commit to continuous monitoring and correction for unintended bias in machine learning.
 - **Accountability:** Individuals should be accountable for the proper functioning of AI systems and for unintended consequences arising out of its use. Companies should ensure that everyone involved in the lifecycle of an AI system is trained in AI 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.
- **World Economic Forum “Human-Centred Artificial Intelligence for Human Resources Toolkit”⁷:** In cooperation with a task force of AI and HR experts including HR Policy Association, the World Economic Forum developed a framework that aims to equip HR professionals with a basic understanding of how AI works in the context of HR, guide

⁷ “Human-Centred Artificial Intelligence for Human Resources.” World Economic Forum. December 2021. <https://www.weforum.org/reports/human-centred-ai-for-hr-state-of-play-and-the-path-ahead>.

companies on the responsible and ethical use of AI, and help companies use AI-based HR tools effectively. The toolkit includes two useful checklists: one for assessing new AI tools before making the critical decision to implement them in a company and one for strategic planning regarding how to responsibly use AI in general.

- **The Data & Trust Alliance** is a not-for-profit consortium bringing together leading businesses and institutions to learn, develop and adopt responsible data and AI practices. Participating HR Policy Association members include American Express, CVS Health, General Motors, Humana, IBM, Johnson & Johnson, MasterCard, the Nielson Company, Pfizer, Under Armour, and UPS. The Alliance has released its Algorithmic Bias Safeguards for Workforce—criteria and education for HR teams to evaluate vendors on their ability to detect, mitigate and monitor algorithmic bias in workforce decisions.⁸

In addition to collaborative efforts, many employers have developed principles and best practices to build safeguards against potential harms in using AI and build trust both within and external to their company. It is important to note that many HR Policy companies do not use or produce biometric technologies, but nevertheless are leaders in developing robust AI oversight policies and practices. The following are just a small sample of such efforts.

- **Accenture’s AI ethics and governance framework** takes an interdisciplinary approach that supports agile innovation and ensures governance of AI systems. Accenture emphasizes the need for organizations to put into practice well-defined AI principles, minimizing unintended bias, ensuring transparency, creating opportunities for employees, and protecting the privacy and security of data.
- **Microsoft’s AI principles** – Fairness, Inclusiveness, Reliability & Safety, Transparency, Privacy & Security, and Accountability – are put into practice throughout the organization largely through the work of its Office of Responsible AI (ORA); the AI, Ethics, and Effects in Engineering and Research (Aether) Committee; and Responsible AI Strategy in Engineering (RAISE). The Aether Committee advises Microsoft’s leadership on the challenges and opportunities presented by AI innovations. ORA sets AI rules and governance processes, working closely with teams across the company to enable the effort. RAISE, meanwhile, enables the implementation of Microsoft responsible AI rules across engineering groups.⁹
- **IBM’s AI Ethics** features a robust, multidisciplinary, multidimensional approach to trustworthy AI, with three principles and five foundational pillars for ethical AI. IBM’s AI

⁸ “Algorithmic Bias Safeguards for Workforce Overview.” The Data & Trust Alliance. December 2021. https://dataandtrustalliance.org/Algorithmic_Bias_Safeguards_for_Workforce_Overview.pdf

⁹ “Responsible AI Principles from Microsoft.” Microsoft. Accessed January 6, 2022. <https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3Aprimaryr6>.

Ethics Board, a central, cross-disciplinary body to support a culture of ethical, responsible, and trustworthy AI throughout IBM, supports a centralized governance, review, and decision-making process for IBM ethics policies, practices, communications, research, products and services.¹⁰

AI, including that which uses biometric information, is not a monolithic concept, and therefore a “one-size-fits-all” approach to oversight may inadvertently expose workers to risk. AI use cases among HR Policy members vary considerably, depending on a wide variety of factors. The risk profiles of different uses of artificial intelligence vary considerably both in scope and in kind (i.e., safety, privacy, autonomy, or fairness). For example, using facial recognition technology during interviews presents a different degree of risk than an AI-powered predictive text tool, and raises different types of risks than GPS tracking features on a company-owned vehicle.

A “one-size-fits-all” model of oversight may inadvertently expose workers to risk, even while providing protections in the cases for which the oversight was aimed. Companies build these considerations into their technology oversight process, seeking to apply their principles on AI in a nimble manner as innovation accelerates. Any AI policy promoting ethics and trust without these characteristics will prove both insufficient and unviable.

New guidelines or standards should align 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. For example, the U.S. Equal Employment Opportunity Commission (EEOC) recently announced an “Artificial Intelligence and Algorithmic Fairness” initiative, part of which will involve the “issuance of technical assistance to provide guidance on algorithmic fairness and the use of AI in employment decisions.”¹¹ Any guidelines should be fully aligned with forthcoming guidance from the EEOC and any other agencies that promulgate AI workplace-related proposals.

Further, any government guidelines should 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. Employers have invested significant resources to develop compliance processes, procedures, and policies, and employers should be able to leverage these governance structures when aligning with the OSTP guidelines.

The use of technology in the employment context is regulated by many frameworks. In the United States alone, federal and state laws relating to anti-discrimination, labor laws, data

¹⁰ “Ai Ethics.” IBM. Accessed January 6, 2022. <https://www.ibm.com/artificial-intelligence/ethics>.

¹¹ “EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness.” U.S. Equal Employment Opportunity Commission. October 28, 2021. <https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness>.

privacy, and AI-specific laws affect the use of technology in the employment context. A brief overview of these laws is below.

- **Anti-Discrimination:** Title VII of the Civil Rights Act (Title VII) 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, any new government guidelines should be co-extensive with existing anti-discrimination laws instead of imposing novel obligations that exceed existing law.

- **Labor Laws:** The National Labor Relations Act, 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 and engage in collective bargaining. The National Labor Relations Act prohibits employers from interfering with employees' exercise of rights to engage in protected "concerted activity." The NLRB has determined that the NLRA prohibits employers from unlawfully surveilling employees' protected activity, which can occur when an employer acts in a way that is out of the ordinary to observe protected activity. Systems that automatically monitor employee activity, whether physical or digital, could be considered unlawful surveillance depending on the facts.

Employers using artificial intelligence in the employment context, such as for workforce management, are already subject to the NLRA's obligations regardless of whether they are unionized. Any new government guidelines should therefore be compatible with the NLRA.

- **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 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.

Meanwhile, congressional lawmakers are actively deliberating on comprehensive consumer privacy reform that may impact the use of technology in the employment context.

- **AI-specific requirements:** An increasing number of state and local laws are 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 of 2021, the New York City Council enacted a law requiring companies to obtain independent audits of certain algorithms used in the employment context. The law also prohibits the use of "biased" algorithms, although the law does not define the term. The new law poses 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 OSTP to look for ways to promote consistency between federal and state efforts.

- **International efforts:** OSTP should also take note of international developments. In Europe, the EU General Data Protection Regulation (GDPR) prohibits solely automated decision-making that has legal or similarly significant effects unless the decision is made pursuant to an individual's consent or another exception applies. Decisions relating to employment may be similarly significant effects, and employers have taken steps to ensure humans remain in the decision-making process for employment accordingly.

In addition, the European Union is considering an EU-wide regulation of artificial intelligence systems under the proposed Artificial Intelligence Act (AI Act). Though the

text remains under deliberation, the AI Act as introduced involves a risk-based classification system for artificial intelligence systems. AI systems in the employment context may be considered “high-risk,” requiring employers using these systems to implement risk management processes, adopt governance structures, provide transparency, register the AI systems, and maintain documentation about the AI systems.

AI specific requirements are being discussed in many other jurisdictions, including in China. OSTP should track those discussions so that any promulgated guidance does not produce unnecessary compliance challenges, if possible, with forthcoming frameworks.

Concerns over third party assessment/audits before standards mature: 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.

Until such standards are matured and accepted, assessment and audit outputs may be inconsistent, and thus ineffective at promoting fairness, may cause companies to forgo innovative technologies in the employment context despite their clear benefits, or may 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.

Final product should be subject to notice and comment and stakeholder meetings: Finally, we believe that any guidelines prepared by OSTP in response to this proceeding should be presented for public comments through a notice and comment process prior to being finalized. Furthermore, we encourage OSTP to hold stakeholder meetings prior to the development and issuance of proposed guidance to solicit input from HR and the regulated community.

We appreciate the opportunity to provide our view and look forward to further lending any assistance we can to this important initiative by the U.S. Office of Science & Technology Policy.