White House Sends Message to Companies Employing Artificial Intelligence: 5 Key Principles You Should Incorporate

Insights
12.05.22

Artificial intelligence impacts Americans on a daily basis in their personal lives and in the workplace. And yet while federal and state governments have made relatively minimal efforts to govern its development, design, and usage, this appears to be changing. The White House Office of Science and Technology Policy recently released its "Blueprint for an AI Bill of Rights," a non-binding whitepaper intended to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems. This blueprint includes five key principles to help protect Americans in the age of artificial intelligence, and employers would be wise to consider them when developing their own policies and practices.

1. Safe and Effective Systems

"You should be protected from unsafe or ineffective systems."

The OSTP recommends that automated systems should be developed in consultation with diverse communities, stakeholders, and domain experts to identify concerns, risks, and potential impacts of the system. Automated systems should not be designed with an intent or reasonably foreseeable possibility of endangering safety. Rather, they should be designed to proactively protect individuals from harms stemming from unintended, yet foreseeable, uses or impacts of automated systems.

This is an important principle, as the OSTP explained, because of unfortunate situations that have occurred in the past, including:

- An algorithm deployed police to neighborhoods they routinely visited, even if those neighborhoods did not have the highest crime rates. The incorrect crime predictions resulted from a feedback loop generated from the reuse of data from prior arrests and algorithm predictions.
- A company installed AI-powered cameras in its delivery vans to evaluate road safety habits of its drivers. However, the system incorrectly penalized drivers when other cars cut them off or when other events beyond their control occurred. This resulted in drivers being ineligible for bonuses.

2. Algorithmic Discrimination Protections

"You should not face discrimination by algorithms and systems should be used and designed in an equitable way."

The White House recommends that designers, developers, and deployers of automated systems take proactive and continuous measures to protect individuals and communities from algorithmic discrimination – when automated systems contribute to unjustified treatment or impact people based on race, color, ethnicity, sex, or other classifications protected by law. It recommends they should use and design automated systems in an equitable way. This should include proactive equity assessments, use of representative data and protection against proxies for demographic features, ensuring accessibility for people with disabilities, disparity testing, and organizational oversight.

This principle was developed by the OSTP based on historical situations such as:

- A hiring tool learned the features of company employees who were predominantly men. It then rejected female job applicants. If an applicant's resume had the word "women's" (e.g., "women's chess club captain"), the applicant would be penalized in the candidate ranking.
- Advertisement delivery systems that predict who is most likely to click on a job advertisement delivered job advertisements that reinforced racial and gender stereotypes, such as directing job advertisements for supermarket cashiers to women.

3. Data Privacy

"You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used."

The report recommends that individuals should be protected from privacy violations through design choices that ensure that protections are included by default in automated systems. This specifically includes ensuring that data collection confirms to reasonable expectations and that only the data strictly necessary for the specific context is collected.

Designers, developers, and deployers of automated systems should seek permission from individuals and respect their decisions regarding the collection, use, access, transfer, and deletion of data in appropriate ways. Requests for consent should be brief, understandable, and provide an individual with agency over their data collection and its use. In addition, continuous surveillance and monitoring should not be used in work or in other contexts where the use of surveillance is likely to limit rights, opportunities, or access.

The OSTP cited to specific situations that have occurred in the past, and which warrant the need for this principle:

- Companies used surveillance software to track employee discussions about union activity and used the data to surveil individual employees and intervene in discussions.

- A data broker harvested significant amounts of personal data and then suffered a breach, exposing hundreds of thousands of people to potential identity theft.

4. Notice and Explanation

"You should know that an automated system is being used, and understand how and why it contributes to outcomes that impact you."

The OSTP advises designers, developers, and deployers of automated systems to provide accessible, plain-language documentation that includes descriptions of the overall system functioning and the role automation plays, notice that such systems are being used, the entity responsible for the system, and explanations of outcomes that are clear, timely, and accessible.

The "Notice and Explanation" principle stems from prior situations, including:

- A system that awarded benefits changed its criteria invisibly. Individuals were then denied benefits due to data entry errors and other flaws in the system. The flaws were only exposed when an explanation of the system was demanded and produced. The lack of an explanation made it more difficult for errors to be corrected in a timely fashion.
- A predictive policing system claimed to identify individuals at greatest risk to commit or become the victim of gun violence and resulted in individuals being placed on a watch list without any explanation or public transparency regarding how the system came to its conclusions. The police and the public were deprived of information showing why and how the system was making its determinations.

5. Human Alternatives, Consideration, and Fallback

"You should be able to opt out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter."

Finally, the White House recommends that individuals should be able to opt out from automated systems in favor of a human alternative, where appropriate. They should also have access to timely human consideration and remedy by a fallback and escalation process if an automated system fails, produces an error, or if the individual would like to appeal or contest its impact.

The OSTP finds this principle necessary, given instances that have occurred in the past:

- A corporation automated human resources functions, which led to employees being fired by an automated system without the possibility of human review, appeal, or other recourse.
- A benefits system required, as a condition of accessing benefits, that applicants have a smartphone in order to verify their identity. Since no alternative human option was readily available, many people were denied access to benefits.

The OSTP advises that independent evaluation and/or reporting should be used to ensure the protections afforded by these five principles.

Next Steps for Businesses

The Blueprint for an AI Bill of Rights is designed to support policies and practices to protect individuals' rights in the development and use of automated systems. For businesses, however, this is a strong sign from the White House that it is taking artificial intelligence seriously. It is also an indication that future – and significant – legislation surrounding artificial intelligence will likely be proposed at the federal and state levels. Businesses should stay abreast of these developments to ensure that their practices are in compliance with applicable rules and regulations governing artificial intelligence.

We will continue to monitor developments with the regulation of artificial intelligence, so make sure you are subscribed to Fisher Phillips' Insight system to keep up with the most up-to-date information. Please contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our Privacy and Cyber Practice Group should you have any questions.

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159
Email

Service Focus

AI, Data, and Analytics

Counseling and Advice

Privacy and Cyber

Employment Discrimination and Harassment