Federal Agencies Concerns with AI:

Why Many Agencies Are Banning the Technology and the Future of AI in Federal Governments

Areeva Solutions
Simplifying Technology for All!

Artificial Intelligence (AI) has remained a big technological storm across industries over the past few years. Government agencies, including the Department of Health and Human Services (HHS), the US Department of Defense (DOD), and the US Department of Agriculture (USDA), have been using AI-powered technologies to increase efficiency and accuracy in their operations.

However, waves are quickly changing, and most government agencies have reconsidered using the new technology. The Federal Communications Commission (FCC), the Department of Energy (DOE), and the Department of Veteran Affairs (VA) are among the latest federal agencies to announce a ban on AI-powered technologies like ChatGPT, though temporarily.

What implications does the new trend hold for the use of AI in the federal government, and where does the future of this new technology lie, given the recent bans across agencies? Keep scrolling for a comprehensive look into the topic.

Why Are Some Federal Agencies Choosing to Ban or Restrict Access to AI Tools Like ChatGPT?

Artificial Intelligence has been carrying the technological airwaves by storm since its introduction. Companies worldwide quickly adopted the technology and leveraged the advantages of incorporating it into their operations.

However, most of these companies have raised concerns regarding probable loopholes in the functionality of AI technology. Data privacy and security are the most significant reasons most agencies have reconsidered their technology usage. Most of these agencies have banned the use of AI, while others have restricted their employees from using it until they develop secure ways to work with the technology.

Here are the top concerns of generative AI and how they threaten the agencies.

DATA PRIVACY CONCERNS

Data leakage poses a significant risk for agencies using generative AI, which depends on large data volumes for learning and efficient operation. The training process involves extensive internet data use, allowing AI trainers potential access to any user-provided data, including confidential and sensitive information. This could violate data protection policies and risk unauthorized data exposure. Moreover, chatbots record inputted information, potentially using sensitive data in responses to other users, creating a data leakage pathway that could harm an agency's reputation.

CYBERSECURITY CONCERNS

AI offers both the capability to enhance cybercrime detection and prevention and the risk of facilitating cybercriminal activities. While AI's role in exposing agencies to cybersecurity threats is debated, criminals could potentially exploit its vulnerabilities. For example, incorporating ChatGPT into operations might allow attackers to embed malware undetectably, and its ability to generate human-like responses could enable phishing attacks to convincingly impersonate legitimate users, tricking employees into divulging sensitive information.

WORKFORCE ROLES AND MORALE

Artificial Intelligence can perform several daily tasks that workers mostly do, including analysis, coding, writing, content creation, and more. This is an efficient way to reduce the workload for the employees and cut down on what a company spends on hiring and onboarding staff.

However, the need to equip employees with generative AI skills has accelerated, demanding more resources and time. Also, employees have grown so dependent on the capabilities of AI, gradually killing individual competence, skills, and creativity in performing these tasks.

UNAVAILABILITY OF EXPLAINABILITY AND INTERPRETABILITY OF RESPONSES

Generative AI systems like ChatGPT operate by grouping the facts they learn and using these clusters of information to give responses. Thus, most of the bots' answers are based on probability and lack elements of explainability and interpretability. Therefore, the information isn't typically trustworthy.

Most agencies feel it's essential to halt the use of this technology until a high percentage of trustworthiness is possible with its responses.

WHAT MEASURES ARE AGENCIES LIKE DOE TAKING TO ENSURE A SECURE EXPLORATION OF AI TECHNOLOGIES?

Numerous agencies have taken measures to build new AI oversight frameworks to ensure secure exploration of the technology. The National Institute of Standards and Technology (NIST) and GrantSolutions are encouraged to develop risk management frameworks that secure operations.

For instance, the Department of Energy AI Risk Management Playbook provides guidelines for risk identification and recommended actionable pathways to attain responsible AI use. It's a comprehensive reference outlining some of the common risks associated with AI, plus steps different agency teams, AI leaders, and practitioners can take to mitigate the threats. Here are some recommendations from the AI Risk Management Playbook.

Create a comprehensive checklist containing precise risks and recommended solutions	Encourage and provide education and upskilling for the staff on AI risk management	Explain why responsible and trustworthy AI use is necessary

WHAT IMPLICATIONS DOES THE CONDITIONAL APPROVAL OF AI TECHNOLOGIES HAVE FOR FUTURE FEDERAL USE OF AI?

Many agencies initially adopted generative AI to enhance efficiency and public service. This phase allowed them to discover the technology's potential and limitations. However, recent widespread AI restrictions by federal agencies, such as the DOE's temporary ban, signal a cautious approach towards its future use, aiming to establish a groundwork for responsible deployment. While DOE views this as a chance to refine their AI strategy, other agencies with permanent bans might position themselves differently regarding AI's role in their operations.

FINAL THOUGHTS

Generative AI introduced a new era in the professional landscape, offering endless opportunities and technological advantages across numerous industries. However, it carried its share of weaknesses into the scene as well. The lack of trustworthiness in its responses, data safety and security concerns, and the laxity it introduced in the agencies made it less desirable to most organizations. That led to a temporary ban on the use of AI in most agencies. While AI's future is still uncertain, it's sufficient to believe that most agencies will ultimately embrace the technology from experience and better preparation, enhancing its productivity in the federal government.