BROOKINGS

COMMENTARY

How AI can enable public surveillance

Darrell M. West

April 15, 2025

- → AI surveillance may no longer just be a foreign government threat, as there are troubling stories about possible abuses within the United States.
- → With major agencies, law enforcement, and intelligence services now in the hands of Trump loyalists, AI-based monitoring capability is a particular concern.
- → It is a risky time for AI surveillance due to a combination of advanced digital technologies, abundant unsecured data, and a political environment that endangers people's freedoms.

Artificial intelligence (AI) offers many promising applications. Algorithms and machine learning can help develop new drugs ↗ and target treatment in effective ways. AI also plays a role in tracking climate change by monitoring weather patterns ↗. Wildlife experts have coupled AI with satellite imagery to monitor how endangered species ↗ are faring and where threats are appearing.

But there is a dark side to AI as well, given its potential for nefarious purposes. Concerns ↗ around privacy, safety and security have grown as the technology is used to analyze confidential material and amplify false narratives as part of disinformation campaigns ↗. Due to its scalability and capacity to examine large data sets, it can study people's behavior ↗ and act on that information.

Perhaps the starkest example is in China, where AI enables surveillance ↗ on a widespread scale. Coupled with social media monitoring, cameras, and facial

recognition, the technology enables authorities to track dissidents and government critics and identify their statements and locations. There is infrastructure in place that can integrate information from a variety of sources and analyze it in real time for government authorities.

Concerns over AI surveillance echo the fears surrounding TikTok's ↗ data-sharing practices with Chinese authorities, including the collection of users' personal details and content interactions. U.S. officials have flagged this as a national security threat, contributing to Congress' decision to ban ↗ TikTok in 2024.

However, AI surveillance may no longer be just a foreign government threat. Reports have surfaced about potential abuses in the U.S., including government contracts that may enable the Department of Homeland Security (DHS) to monitor social media. According to the Politico Digital Future newsletter ↗, "the contractors advertise their ability to scan through millions of posts and use AI to summarize their findings" for their clients. With major agencies, law enforcement, and intelligence services now in the hands of Trump loyalists, this monitoring capability is a particular concern right now when the administration is going after its critics ↗.

DHS later confirmed it is using digital tools to analyze social media posts ↗ from individuals applying for visas or green cards. The surveillance software would search for any signs of "extremist" rhetoric or "antisemitic activity." The announcement raised questions about how these terms would be defined and whether public criticism of certain countries could be used to label applicants as "terrorist sympathizers."

Other reports suggest that surveillance has already occurred within the Environmental Protection Agency (EPA). According to sources quoted by Reuters ↗, "some EPA managers were told by Trump appointees that Musk's team is rolling out AI to monitor workers, including looking for language in communications considered hostile to Trump or Musk." The EPA has denied the report, calling it "categorically false ↗."

It is not just the American government that is getting into the monitoring act. Some U.S. companies already engage in workplace surveillance ↗ of their employees for business purposes. In the absence of a national privacy bill, there are few legal safeguards ↗ to limit workplace computer or network surveillance—or even to require

that such monitoring be disclosed. Employers can track what workers do ↗ on their computers, even if they are using their equipment at home as part of hybrid work. Some firms even go as far as monitoring keystrokes or facial expressions to see what people are doing, who may be underperforming, and whether they are obeying company policies. These digital practices (https://www.brookings.edu/articles/how-employers-use-technology-to-surveil-employees/) are perfectly legal in many states.

Overall, it is a risky time for AI-based surveillance because we have a combination of advanced digital technologies, high-level computing power, abundant and non-secured data ↗, data brokers who buy and sell information, and a risky political environment. It is the confluence of each of these factors that endanger people's freedoms and ability to express themselves in an open manner. As AI surveillance grows, individual freedom diminishes, and the risks of government and corporate overreach rise.

A national privacy bill could help mitigate some of these threats by establishing privacy standards and blocking some of the most dangerous practices, but it would not be a comprehensive solution.

Further, U.S. government agencies should be barred from using AI or facial recognition software to spy on individuals or monitor their public statements on social media. Using such tools to track what people say about public officials could cross into undemocratic territory for the United States.

AUTHOR

Darrell M. West Senior Fellow - Governance Studies, Center for Technology Innovation, Center for Effective Public Management, **Douglas Dillon Chair in Governmental Studies** 𝕏 @