Opinion

Congress must prevent AI surveillance. The Anthropic feud proves it

Ashley Gorski and Patrick Toomey

The company's clash with the Pentagon is a fight over the future of American privacy

Mon 9 Mar 2026 10.00 GMT
Last modified on Mon 9 Mar 2026 10.17 GMT

The US military wants to use its state-of-the-art AI tools to supercharge surveillance against Americans, making it easier than ever to monitor our movements, our search history, and our private associations. That's one of the major takeaways from a dramatic dispute between the Department of Defense and some of the leading AI companies in America. What this clash highlights most of all, however, is just how easily AI surveillance systems can be turned against the people in this country, and the urgent need for Congress to intervene.

Last week, the Pentagon and Donald Trump announced that the government would cease using Anthropic's AI products, asserting that the safety guardrails proposed by the company - no mass domestic surveillance or fully autonomous weapons - were unacceptable. The Trump administration went even further, claiming that these positions render Anthropic a "supply chain risk", and prohibited anyone doing business with the US military from conducting commercial activity with Anthropic in their military work.

But this is no ordinary contract dispute. This is a fight over the future of American privacy, and it will ultimately affect all of us.

At the heart of the dispute is the government's assertion that it should be able to use AI for any "lawful" purpose. The problem is that the law is running decades behind the technology. The law doesn't account for a world where cellphones are tracking devices; our internet browsing is as revelatory as our personal diary; our data can be bought on the open market; and where AI would let the government seamlessly integrate this data it buys into the most comprehensive and largest set of domestic dossiers ever created.

Compounding this problem, as we saw with some of the worst surveillance abuses after September 11, the executive branch often secretly decides what is "lawful". Without clear and specific rules from Congress, the Trump administration could rubberstamp a domestic spying program and deem it lawful because they said so. Given what we already know about the government's quenchless thirst for our data-and how willing it has already been to sidestep our fourth amendment rights against unreasonable searches and seizures - this prospect is chilling to say the least.

The defense department and other federal agencies already take the position that they can "lawfully" purchase Americans' private data - including location history and web-browsing records - and search that data without a court order. Although bipartisan coalitions in Congress have long criticized these warrantless searches, they've so far failed to end them.

But the problem is poised to become far worse with AI. According to New York Times reporting on the contract negotiations, the Pentagon wanted to apply AI to "the collection and analysis of unclassified, commercial bulk data on Americans

the collection and analysis of unclassified, commercial bulk data on Americans, such as geolocation and web browsing data". Not only does the reporting confirm that the government is, in fact, collecting Americans' private data in bulk, but it shows that the Pentagon wants to deploy the world's most powerful tools to exploit this immense and controversial pool of data.

> *These tools promise to combine data from disparate sources, find patterns, and distill the results into a detailed picture of someone's movements, political views or associations*

AI tools could allow the government, at the touch of a button, to extract information and inferences about a person that previously might have taken an agent or analyst days or weeks to develop. These tools promise to combine data from disparate sources, find patterns, and distill the results into a detailed picture of someone's movements, political views or associations. As just one example: the government may purchase a large dataset containing the movements of thousands of cellphones, but often those trails of digital data don't have names assigned to them, requiring additional analysis. AI can conduct that kind of analysis faster than any human, while integrating other data streams for an even more comprehensive picture of a person's life. And it can do this work at scale. That's especially alarming when one considers the Trump administration's race to access voting data, health records, and tax information.

Anthropic's fight might be with the Pentagon, but other government agencies purchase commercial data in bulk too. As the ACLU's Freedom of Information Act work has confirmed, ICE has repeatedly bought cellphone location data and information from license plate databases to go after immigrant communities. And over the past few months, federal agents have also been collecting license plate data and faceprints from some of the people protesting and documenting their activities in public. Against this backdrop, there is every reason to be concerned about the powers that these agencies are amassing via AI.

As in other contexts, AI tools remove human friction from the work of surveillance, magnifying the dangers of digital spying by making it cheaper, faster and more detailed. If Congress fails to step in, the application of AI to "lawfully" acquired data could quickly lead to a dystopian government database filled with the most telling details about all of us. The consequences of an AI-powered mass domestic database would be devastating: large-scale invasions of privacy, an extreme chill on the freedoms of speech and association, and the targeting of vulnerable or unpopular populations for further scrutiny or worse.

For society as a whole, these effects are corrosive. And as we know firsthand from our clients at the ACLU, government surveillance can feed into discriminatory profiling and watchlists. It can result in unwarranted investigations and prosecutions. And it leaves people looking over their shoulders for decades.

On Monday night, OpenAI – which had announced an agreement with the Pentagon after Anthropic's fell through – said it was amending its deal to add language protecting the civil liberties of US citizens and permanent residents. While this is a welcome development, the new language is riddled with loopholes. And it underscores a bigger problem: our rights shouldn't rise or fall with the whims of one CEO. Whether government agencies should be buying Americans' private data, and whether they should be applying AI tools to analyze that data, are immensely consequential questions. The answers to these questions shouldn't depend on contracts that can change at any time (and in secret); nor should they depend on the individual viewpoints or market motives of tech executives. People in the United States deserve a real and lasting legislative solution to protect their privacy. Congress must step in.

Congress can start by passing the bipartisan Fourth Amendment Is Not For Sale Act, a commonsense reform bill that bans the government from buying data that it would otherwise need a warrant to obtain. Congress must also impose basic guardrails on the government's use of novel AI tools: safeguards that protect against warrantless invasions of our privacy and prohibit uses that threaten our ability to speak out and associate freely online and off.

Ashley Gorski is senior staff attorney with ACLU's National Security Project. Patrick Toomey is its deputy director

Most viewed