How ICE Already Knows Who Minneapolis Protesters Are

Agents use facial recognition, social media monitoring and other tech tools not only to identify undocumented immigrants but also to track protesters, current and former officials said.

▶ Listen to this article · 7:56 min   Learn more

By Sheera Frenkel and Aaron Krolik

Sheera Frenkel reports on defense technology and Silicon Valley. Aaron Krolik reports on data and technology.

Published Jan. 30, 2026   Updated Jan. 31, 2026

> **Sign up for the On Tech newsletter.**   Get our best tech reporting from the week. Get it sent to your inbox.

On the morning of Jan. 10, Nicole Cleland was in her car trailing an Immigration and Customs Enforcement agent through Richfield, Minn., her hometown.

Suddenly, the agent turned into a series of one-way streets and stopped, getting out of his white Dodge Ram, said Ms. Cleland, who volunteers with a local watchdog group that observes the activity of immigration officers. The agent then walked over to Ms. Cleland's car and surprised her by addressing her as Nicole.

"He said he had facial recognition and that his body camera was on," said Ms. Cleland, 56, who had not met the agent before.

Ms. Cleland was one of at least seven American citizens told by ICE agents this month that they were being recorded with facial recognition technology in and around Minneapolis, according to local activists and videos posted to social media, which were verified by The New York Times. None had given consent for their faces to be recorded.

Facial recognition is just one technology tool that ICE has deployed in Minneapolis, where thousands of agents are conducting a crackdown. The technologies are being used not only to identify undocumented immigrants but also to track citizens who have protested ICE's presence, said three current and former officials of the Department of Homeland Security who were not authorized to discuss confidential matters.

ICE is using two facial recognition programs in Minnesota, they said, including one made by the tech company Clearview AI and a newer program, Mobile Fortify. The agency is also using cellphone and social media tools to monitor people's online activity and potentially hack into phones. And agents are tapping into a database, built by the data analytics company Palantir, that combines government and commercial data to identify real-time locations for individuals they are pursuing, the current and former officials said.

"The technologies are being deployed, or appear to be deployed, in a much more aggressive way than we have seen in the past," said Nathan Freed Wessler, a lawyer at the American Civil Liberties Union, which has sued the Homeland Security Department over the immigration operation in Minneapolis. "The conglomeration of all these technologies together is giving the government unprecedented abilities."

The Homeland Security Department has not disclosed which technologies immigration agents are using in Minneapolis. A spokeswoman said the agency would not detail its methods, adding: "For years law enforcement across the nation has leveraged technological innovation to fight crime. ICE is no different."

The reach of the technologies has raised concerns. In November, Democratic senators including Edward J. Markey of Massachusetts, Chris Van Hollen of Maryland and Adam B. Schiff of California asked ICE for more information on its facial recognition software, and asked that it suspend use of the technology in U.S. cities.

ICE has vastly expanded its tech tools over the last year after an influx of cash. In July, President Trump signed a bill increasing ICE's annual budget to roughly $28 billion from $8 billion, making it the most richly funded law enforcement agency in the federal government.

In April, the Homeland Security Department awarded Palantir a nearly $30 million contract to build a system backed by artificial intelligence that would help find and track individuals for deportation. Palantir was due to deliver a prototype by Sept. 25, according to public tenders issued by the agency. The agency has started using the system, two current Homeland Security officials said.

A person familiar with Palantir said the company works with ICE on a database that integrates different information to help agents identify only noncitizens.

In September, the Homeland Security Department also spent nearly $10 million acquiring at least three social media monitoring tools and services that allow it to delve into people's cellphones, according to procurement records and public contracts for the project.

One of the tools, which was built by Paragon, an Israeli technology company, lets

people take control of phones or remotely hack into them to read messages or track locations. The others were built by Penlink, a Nebraska-based software company. They use social media data scraped from the web and information from data brokers to help build dossiers of anyone with a social media account.

Some details of these tools were reported earlier by 404 Media. Paragon and Penlink did not respond to requests for comment.

ICE's use of facial recognition software was documented in videos and photos from local activist groups in Minnesota this month and reviewed by The Times. Two photos captured fatigue-clad agents using cellphones to scan the faces of protesters in Minneapolis, while in one video, agents could be heard telling people that they were being recorded with facial recognition technology and that their faces would be added to a database.

The technology visible in the photographs was Mobile Fortify. The app was built on technology that had been created for Customs and Border Protection, the current and former Homeland Security officials said.

A department spokeswoman said Mobile Fortify was a "lawful law enforcement tool" and "lawfully used nationwide in accordance with all applicable legal authorities."

In a 2024 agency report, the Homeland Security Department said it used a facial recognition tool from Clearview AI for child exploitation investigations. But in a $3.75 million contract with the company in September, the agency said the tool would also be used to investigate attacks on law enforcement.

A Clearview AI spokeswoman said the focus of its contract with the department was supporting investigations into child exploitation and cybercrimes.

ICE is continuing to seek more technology. Last week, the agency published a request for information for ways to better acquire and integrate so-called big data and advertising tech into its operations, saying it was "working with increasing volumes of criminal, civil and regulatory administrative documentation from numerous internal and external sources."

The questionnaire asked vendors to describe the types of data they could provide on "people, businesses, devices, locations, transactions, public records." It also asked vendors how their systems could help "identify subjects, entities or locations of interest" and whether people could be searched by identifiers including "name, phone, device, account, location."

Justin Sherman, a distinguished fellow at Georgetown Law's Center on Privacy and Technology, said the request showed ICE was "doubling down" on buying sensitive data.

Ms. Cleland, the Richfield resident, said that three days after the encounter with the ICE agent, she received an email from the Department of Homeland Security saying her Global Entry and Transportation Security Administration travel privileges had been revoked. No explanation was provided.

Ms. Cleland said she had swung from anger to fear. "I don't know how far-reaching ICE can be," she said. "I'm struggling to figure out what I can do, without putting myself at greater risk or putting other people at risk."

Last week, Ms. Cleland signed a declaration joining a lawsuit against the Homeland Security Department in U.S. District Court in Minnesota. The lawsuit challenges ICE's treatment of observers. In her declaration, Ms. Cleland asked why her traveler status had been revoked.

"I am a totally average American, and I cannot abide by what is happening right now," she said.

Daniel Wood and Kashmir Hill contributed reporting.

Sheera Frenkel is a reporter based in the San Francisco Bay Area, covering the ways technology impacts everyday lives with a focus on social media companies, including Facebook, Instagram, Twitter, TikTok, YouTube, Telegram and WhatsApp.