Always watching: How ICE’s plan to monitor social media 24/7 threatens privacy and civic participation

Nicole M. Bennett, Ph.D. Candidate in Geography and Assistant Director at the Center for Refugee Studies, Indiana University

Published: November 7, 2025 8:18am EDT

ICE's surveillance gaze is likely to sweep across millions of people's social media posts.
Westend61/Westend61 via Getty Images

When most people think about immigration enforcement, they picture border crossings and airport checkpoints. But the new front line may be your social media feed.

U.S. Immigration and Customs Enforcement has published a request for information for private-sector contractors to launch a round-the-clock social media monitoring program. The request states that private contractors will be paid to comb through “Facebook, Google+, LinkedIn, Pinterest, Tumblr, Instagram, VK, Flickr, Myspace, X (formerly Twitter), TikTok, Reddit, WhatsApp, YouTube, etc.,” turning public posts into enforcement leads that feed directly into ICE’s databases.

The request for information reads like something out of a cyber thriller: dozens of analysts working in shifts, strict deadlines measured in minutes, a tiered system of prioritizing high-risk individuals, and the latest software keeping constant watch.

I am a researcher who studies the intersection of data governance, digital technologies and the U.S. federal government. I believe that the ICE request for information also signals a concerning if logical next step in a longer trend, one that moves the U.S. border from the physical world into the digital.

A new structure of surveillance

ICE already searches social media using a service called SocialNet that monitors most major online platforms. The agency has also contracted with Zignal Labs for its AI-powered social media monitoring system.

The Customs and Border Protection agency also searches social media posts on the devices of some travelers at ports of entry, and the U.S. State Department reviews social media posts when foreigners seek visas to enter the United States.

What would change isn't only the scale of monitoring but its structure. Instead of government agents gathering evidence case by case, ICE is building a public-private surveillance loop that transforms everyday online activity into potential evidence.

Private contractors would be tasked with scraping publicly available data to collecting messages, including posts and other media and data. The contractors would be able to correlate those findings with data in commercial datasets from brokers such as LexisNexis Accurint and Thomson Reuters CLEAR along with government-owned databases. Analysts would be required to produce dossiers for ICE field offices within tight deadlines – sometimes just 30 minutes for a high-priority case.

Those files don't exist in isolation. They feed directly into Palantir Technologies' Investigative Case Management system, the digital backbone of modern immigration enforcement. There, this social media data would join a growing web of license plate scans, utility records, property data and biometrics, creating what is effectively a searchable portrait of a person's life.

Who gets caught in the net?

Officially, ICE says its data collection would focus on people who are already linked to ongoing cases or potential threats. In practice, the net is far wider.

The danger here is that when one person is flagged, their friends, relatives, fellow organizers or any of their acquaintances can also become subjects of scrutiny. Previous contracts for facial recognition tools and location tracking have shown how easily these systems expand beyond their original scope. What starts as enforcement can turn into surveillance of entire communities.

What ICE says and what history shows

ICE frames the project as modernization: a way to identify a target's location by identifying aliases and detecting patterns that traditional methods might miss. Planning documents say contractors cannot create fake profiles and must store all analysis on ICE servers.

But history suggests these kinds of guardrails often fail. Investigations have revealed how informal data-sharing between local police and federal agents allowed ICE to access systems it wasn't authorized to use. The agency has repeatedly purchased massive datasets from brokers to sidestep warrant requirements. And despite a White House freeze on spyware procurement, ICE quietly revived a contract with Paragon's Graphite tool, software reportedly capable of infiltrating encrypted apps such as WhatsApp and Signal.

Meanwhile, ICE's vendor ecosystem keeps expanding: Clearview AI for face matching, ShadowDragon's SocialNet for mapping networks, Babel Street's location history service Locate X, and LexisNexis for looking up people. ICE is also purchasing tools from surveillance firm PenLink that combine location data with social media data. Together, these platforms make continuous, automated monitoring not only possible but routine.

Lessons from abroad

The United States isn't alone in government monitoring of social media. In the United Kingdom, a new police unit tasked with scanning online discussions about immigration and civil unrest has drawn criticism for blurring the line between public safety and political policing.

Across the globe, spyware scandals have shown how lawful access tools that were initially justified for counterterrorism were later used against journalists and activists. Once these systems exist, mission creep, also known as function creep, becomes the rule rather than the exception.

The social cost of being watched

Around-the-clock surveillance doesn't just gather information – it also changes behavior.

Research found that visits to Wikipedia articles on terrorism dropped sharply immediately after revelations about the National Security Agency's global surveillance in June 2013.

For immigrants and activists, the stakes are higher. A post about a protest or a joke can be reinterpreted as "intelligence." Knowing that federal contractors may be watching in real time encourages self-censorship and discourages civic participation. In this environment, the digital self, an identity composed of biometric markers, algorithmic classifications, risk scores and digital traces, becomes a risk that follows you across platforms and databases.

What's new and why it matters now

What is genuinely new is the privatization of interpretation. ICE isn't just collecting more data, it is outsourcing judgment to private contractors. Private analysts, aided by artificial intelligence, are likely to decide what online behavior signals danger and what doesn't. That decision-making happens rapidly and across large numbers of people, for the most part beyond public oversight.

At the same time, the consolidation of data means social media content can now sit beside location and biometric information inside Palantir's hub. Enforcement increasingly happens through data correlations, raising questions about due process.

ICE's request for information is likely to evolve into a full procurement contract within months, and recent litigation from the League of Women Voters and the Electronic Privacy Information Center against the Department of Homeland Security suggests that the oversight is likely to lag far behind the technology. ICE's plan to maintain permanent watch floors, open indoor spaces equipped with video and computer monitors, that are staffed 24 hours a day, 365 days a year signals that this likely isn't a temporary experiment and instead is a new operational norm.

What accountability looks like

Transparency starts with public disclosure of the algorithms and scoring systems ICE uses. Advocacy groups such as the American Civil Liberties Union argue that law enforcement agencies should meet the same warrant standards online that they do in physical spaces. The Brennan Center for Justice and the ACLU argue that there should be independent oversight of surveillance systems for accuracy and bias. And several U.S. senators have introduced legislation to limit bulk purchases from data brokers.

Without checks like these, I believe that the boundary between border control and everyday life is likely to keep dissolving. As the digital border expands, it risks ensnaring anyone whose online presence becomes legible to the system.

Nicole M. Bennett is affiliated with the Center for Refugee Studies at Indiana University.