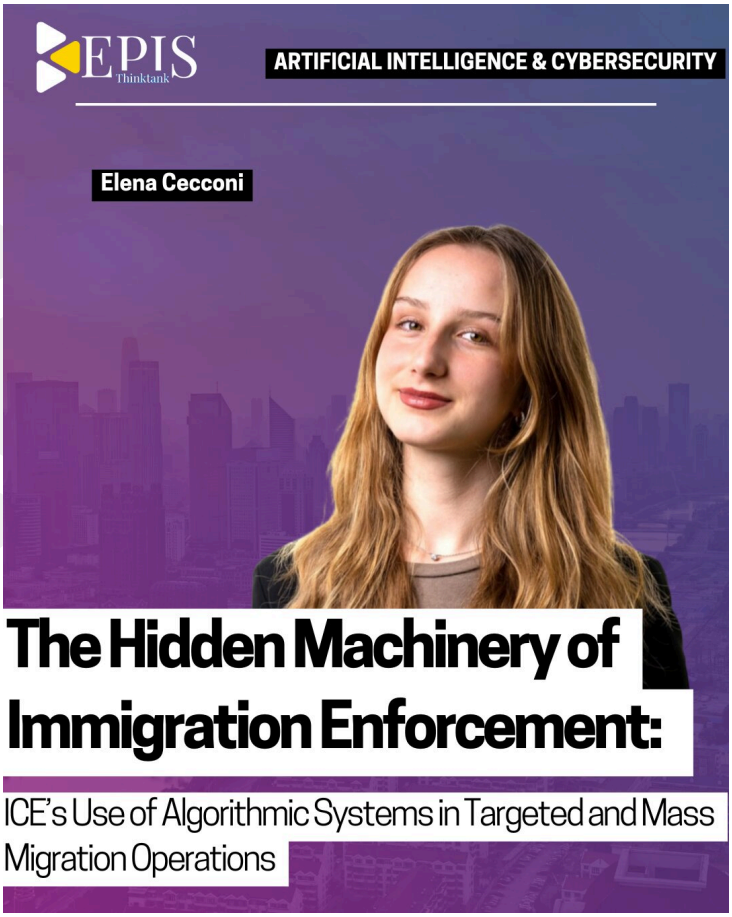
The Hidden Machinery of Immigration Enforcement:

29 DECEMBER 2025

Elena Cecconi



In September, U.S. Immigration and Customs Enforcement (ICE) quietly entered into a five-year, $5.7 million contract with Zignal Labs, an AI-driven social media monitoring platform, a move that exemplifies what has been described as a "political panopticon" (Chayka, 2025; Schwenk, 2025). The agreement marks more than a routine procurement decision: it signals the further entrenchment of algorithmic surveillance at the core of U.S. immigration enforcement. Zignal Labs performs large-scale Open Source Intelligence (OSINT) and social media scraping, leveraging artificial intelligence and machine learning to analyze over eight billion posts

per day across more than 100 languages (Schwenk, 2025). According to the company's materials, this process generates "curated detection feeds" designed to enable law enforcement to identify and respond to perceived threats with "greater clarity and speed" (The Tech Buzz, 2025).

Within ICE, Zignal Labs licences are used by Homeland Security Investigations (HSI), the agency's intelligence arm, for real-time data analysis in criminal investigations and to generate operational leads for enforcement actions (The Tech Buzz, 2025). The system, already employed by the Pentagon and the Israeli military, is capable of extracting precise geolocation data from video metadata and identifying individuals through partial visual markers in photographs, such as their irises or posture patterns, effectively converting online activity into raid-ready intelligence files (The Tech Buzz, 2025). In doing so, it facilitates continuous, population-level monitoring, in which everyday digital expression becomes a potential trigger for investigation.

Crucially, Zignal Labs should not be understood as a novel or isolated innovation. Rather, it represents the latest layer in an expanding digital surveillance infrastructure that ICE has developed over time. Its integration feeds into a broader technological ecosystem oriented toward highly automated enforcement (Dou, 2025). Central to this system is ImmigrationOS, a Palantir-developed platform that manages the enforcement lifecycle, from approving raids and booking arrests to routing individuals through detention and deportation processes (Angélica Franganillo Díaz, 2025). Algorithmic risk assessment is further institutionalized through tools such as the "Hurricane Score", which assigns individuals in the Alternatives to Detention program a numerical rating intended to predict the likelihood of absconding (Parvini et al., 2024).

These systems are complemented by biometric databases like Clearview AI, which scrapes billions of images from the web, and by phone tracking technologies that layer financial data and social networks onto Palantir's centralized hub (Cameron, 2025). Taken together, this dragnet reflects a decisive shift away from tools designed to improve administrative efficiency toward a technology-driven enforcement apparatus in which AI, predictive analytics, and algorithmic judgment automate targeting, risk scoring, and enforcement, rendering pervasive surveillance institutionalized rather than experimental and enabling a qualitative, arguably unprecedented, expansion of state control.

Migration Securitization as a Political Enabler of Exceptional Measures

The rapid expansion of ICE's digital surveillance capacity in the United States is politically enabled and rooted in the long-standing securitization of migration. As the Copenhagen School (Buzan et al., 1998) famously argued, security is not determined by objective threats but emerges through

discursive processes in which political actors construct specific issues as existential dangers, thereby justifying extraordinary measures.

In U.S. migration politics, this securitizing logic has been particularly pronounced. A substantial body of scholarship documents how Donald Trump, beginning with his 2016 presidential campaign, advanced a mystifying and alarmist depiction of immigration, which intensified during his second mandate's campaign (Giagnoni, 2019; Slocum, 2024; Ward, 2024). Through the strategic use of isolated tragedies and overtly xenophobic rhetoric, migrants were portrayed as culturally corrosive outsiders, "rapists" and "drug lords" imported from the "dungeons of the third world", whose presence allegedly threatened the nation's social and political fabric (Ward, 2024). Building on this rhetoric, Trump openly claimed credit for inventing the term "migrant crime", presenting it as a distinct and uniquely dangerous category, thereby mobilizing fear as a political resource (Giagnoni, 2019; Slocum, 2024).

Immigration was increasingly cast as an "invasion", involving an "army of illegal alien gang members" allegedly "destroying the country from inside its borders" (Ramirez Uribe & Briceño, 2025; Slocum, 2024). Such alarming discourse provided the justificatory foundation for exceptional policies, including mass deportations and the invocation of the Alien Enemies Act of 1789, which enables the executive to bypass ordinary judicial procedures under the guise of wartime authority (Ramirez Uribe & Briceño, 2025). This narrative functioned as a master frame that collapsed migration, criminality, and terrorism into a single security threat, relying heavily on misinformation and racialized stereotypes to elevate perceived risk (de Paula Moreira et al., 2025).

Seen Raids, Unseen Routes

Turning specifically to ICE, the agency's operational mandate under the current administration has shifted decisively from targeted enforcement, often summarized as a "worst first" approach, toward broad, high-volume operations designed to maximize arrests and generate visibility, deterrence, and fear (Misra, 2025). This strategic reorientation helps explain the proliferation of social media footage depicting military-style raids and mass arrests. Acting ICE Director Todd Lyons has explicitly framed enforcement efficiency through a logistical metaphor, describing the goal of deportation operations as resembling "Amazon delivery routes—like Prime, but with human beings" (Franganillo Díaz, 2025). Rather than prioritizing individuals' criminal histories, enforcement now emphasizes the sheer quantity of apprehensions, effectively repurposing ICE to "go out and get as many people as possible", with operations increasingly resembling area sweeps rather than individualized investigations (Misra, 2025).

These operations frequently involve stopping individuals in public spaces, coordinating with local law enforcement during traffic stops, or tar-

geting apartment buildings where undocumented residents are suspected to live (Misra, 2025). Such enforcement actions are characterized by militarized tactics, aggressive conduct, and the conspicuous use of force, including agents wearing tactical gear and masks, smashing car windows, and using pepper balls or smoke bombs, often prompting public backlash and widespread media attention (Misra, 2025). Importantly, ICE's aggressiveness is not merely instrumental but also performative and politically communicative, as the agency has become a primary symbol of the administration's core priorities.

Yet this visible theatre of enforcement represents only part of the story. Kelley-Widmer (2021) introduces the concept of "unseen policies" to describe low-visibility executive rules and bureaucratic adjustments that quietly reshape U.S. immigration governance without new legislation. Unlike headline-grabbing initiatives, these technical changes, procedural barriers, data-sharing arrangements, and restrictive reinterpretations of existing law expand executive power while largely escaping public scrutiny, despite their profound impact on migrants' daily lives (Kelley-Widmer 2021).

Building on this framework, the same notion of the "unseen" can be extended to the digital systems that enable contemporary immigration enforcement. The enforcement regime can be conceptualized through an iceberg metaphor. The visible tip consists of highly publicized raids, militarized operations, and mass deportations on cargo flights that dominate public debate. Beneath the surface lies the hidden structure: a vast technological infrastructure of algorithmic risk scoring, biometric databases, and integrated analytics platforms, which silently coordinate and scale enforcement capacity.

Beyond Migration: Democratic Stakes of Digital Enforcement

While immigration enforcement directly targets migrants, the expansion of ICE's digital surveillance infrastructure has implications for democracy as a whole, which can be understood through two interrelated lines of reasoning.

First, practices often described as "digital authoritarianism", "the use of digital technologies by state and non-state actors to 'surveil, repress, and manipulate domestic and foreign populations'" (Polyakova & Meserole, 2019), are no longer limited to overtly authoritarian regimes and are increasingly present within democratic systems as well (Glasius, 2018; Roberts & Oosterom, 2025). The deployment of AI-powered monitoring tools such as Zignal Labs demonstrates how technologies initially justified for migration control can normalize pervasive surveillance across society. According to Stewart et al. (2025), the State Department now uses AI to monitor the public speech of foreign nationals, including students and visitors, revoking visas for those who display "hostile attitudes" toward U.S. institutions or "celebrate" events deemed contrary to national interest. In line with this

approach, ICE has deployed elite investigative officers to probe "anti-ICE protester networks" and "professional agitators", employing Zignal Labs and remote-controlled drones to track individuals (Dou, 2025). This development has raised growing concern that ICE now wields the authority to surveil not only immigrant communities but also U.S. citizens exercising their First Amendment right to protest (Dou, 2025).

As David Greene of the Electronic Frontier Foundation has warned, AI-driven social media surveillance risks producing a "massive chilling effect on free speech", commensurate with the unprecedented scale of monitoring itself (The Tech Buzz, 2025). Similar concerns were raised by a coalition of labour unions in a lawsuit against the Trump administration, which argued that AI-based, viewpoint-driven online surveillance "exacerbate[s] the chilling impact of that surveillance" (Schwenk, 2025). Notably, this complaint, highlighting the role of Zignal Labs, was prepared with the involvement of attorneys from the Electronic Frontier Foundation and Yale Law School's Media Freedom and Information Access Clinic (Schwenk, 2025). Echoing these concerns, Patrick Toomey, deputy director of the ACLU's National Security Project, has warned that the Department of Homeland Security should not be scrutinizing online speech using opaque "black box" technologies that lack meaningful accountability or oversight (Schwenk, 2025). Importantly, these systems should not be understood as static: the more they are used, the more they are trained, refined, and expanded, accumulating vast repositories of behavioural data. In this process, the boundary between targeting migrants and monitoring dissent becomes increasingly porous.

Unlike conventional surveillance, digital monitoring functions silently, persistently, and automatically, making it difficult to contest either legally or politically. Its most consequential effects lie not in overt coercion, but in the quiet, algorithmic decisions that reshape governance while remaining largely invisible to public scrutiny and democratic accountability.

References

Bermeo, N. (2016). On Democratic Backsliding. Journal of Democracy, 27(1), 5–19. https://doi.org/10.1353/jod.2016.0012

Buzan, B., Wæver, O., & De Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner Publishers.

Chayka, K. (2025, October 29). ICE and the Smartphone Panopticon. The New Yorker. https://www.newyorker.com/culture/infinite-scroll/ice-and-the-smartphone-panopticon

de Paula Moreira, N., Hassan, M., Kim, Y., Zhang, M., Floyd, B., & Franklin Fowler, E. (2025). The One-Sided Narrative on Immigration and Its Consequences – COMM. Commhsp.org. https://commhsp.org/the-one-sided-narrative-on-immigration-and-its-consequences/

Dell, C. (2025, October 3). ICE Wants to Build Out a 24/7 Social Media Surveillance Team. WIRED. https://www.wired.com/story/ice-social-media-surveillance-24-7-contract/

Dou, E. (2025, October 17). ICE amps up its surveillance powers, targeting immigrants and antifa. The Washington Post. https://www.washingtonpost.com/technology/2025/10/17/ice-surveillance-immigrants-antifa/

Franganillo Díaz, A. (2025). "Like Prime, but with human beings": How the Trump administration is using AI to ramp up immigration enforcement. CNN. https://edition.cnn.com/2025/09/22/politics/artificial-intelligence-immigration-enforcement

Giagnoni, S. (2019). Fear and Hate in Alabama and Beyond: Narratives of Immigration in the Trump Campaign. Journal of Hate Studies, 14(1), 7. https://doi.org/10.33972/jhs.122

Glasius, M. (2018). What Authoritarianism Is ... and Is not: a Practice Perspective. International Affairs, 94(3), 515–533. https://doi.org/10.1093/ia/iiy060

Levinson-Waldman, R., Panduranga, H., & Patel, F. (2022, January 7). Social Media Surveillance by the U.S. Government. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government

Misra, R. (2025, October 14). Why Is ICE So Aggressive Now? A Former ICE Chief Explains. POLITICO. https://www.politico.com/news/magazine/2025/10/14/former-ice-director-q-a-00603916

Parvini, S., Burke, G., & Bedayn, J. (2024, November 26). Surveillance tech advances by Biden could aid in Trump's promised crackdown on immigration. AP News. https://apnews.com/article/artificial-intelligence-ai-deportation-biden-trump-immigration-0a0c2387762a7342af5668660f0391b5

Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

Ramirez Uribe, M., & Briceño, M. (2025). How falsehoods drove Trump's immigration crackdown in his first 100 days. Al Jazeera. https://www.aljazeera.com/news/2025/4/29/how-falsehoods-drove-trumps-immigration-crackdown-in-his-first-100-days

Roberts, T., & Oosterom, M. (2024). Digital authoritarianism: a systematic literature review. Information Technology for Development, 31(4), 860–884. https://doi.org/10.1080/02681102.2024.2425352

Schwenk, K. (2025, October 23). ICE Just Bought A Social Media Surveillance Bot. The Lever. https://www.levernews.com/ice-just-bought-a-social-media-surveillance-botice-just-bought-a-social-media-surveillance-bot/?utm_source=newsletter-email&utm_medium=link&utm_campaign=newsletter-article-read-more

Slocum, J. (2024). Immigration in the 2024 US presidential election campaign: policy stalemate, disinformation, and a call for mass deportation. Cidob.org. https://doi.org/10.24241/NotesInt.2024/311/enAll

Stewart, J., Lee, N. T., & DU, M. (2025, October 6). How tech powers immigration enforcement. Brookings. https://www.brookings.edu/articles/how-tech-powers-immigration-enforcement/

The Tech Buzz. (2025, October 25). ICE Deploys $5.7M AI Surveillance System to Track Millions. https://www.techbuzz.ai/articles/ice-deploys-5-7m-ai-surveillance-system-to-track-millions

Ward, M. (2024, October 12). We Watched 20 Trump rallies. His racist, anti-immigrant Messaging Is Getting darker. Politico. https://www.politico.com/news/2024/10/12/trump-racist-rhetoric-immigrants-00183537

EPIS