Science & technology | Frontier AI

How ICE's new software tools could speed up deportations

The risk of overreach is high

February 19th 2026

GOVERNMENT NOTICES on software contracts rarely make for intriguing reading. Yet one published on April 17th 2025 by America's Immigration and Customs Enforcement (ICE), the muscle behind President Donald Trump's crackdown on undocumented immigrants, stood out. The agency was urgently seeking a powerful new artificial-intelligence model to find and prioritise individuals eligible for deportation—ranging from those who overstayed their visas to violent criminals. A prototype of the "streamlined end-to-end immigration lifecycle" software, called ImmigrationOS, was to be delivered by Palantir, an American data-analysis giant, by the end of September.

The White House seeks a million deportations annually, so ICE is under pressure to get people out. But such technological moves to speed up immigration enforcement have troubled many observers. A lawsuit filed on January 15th by the American Civil Liberties Union described ICE's recent operations in Minnesota as a "crude dragnet" that had led to scores of

unlawful detentions, many carried out with excessive force. Recent rulings suggest judicial discontent is growing.

"I understand why people would be scared to death of these tools," says John Sandweg, an acting director of ICE during Barack Obama's second term. He fears they will sweep up large numbers of undocumented but otherwise law-abiding people, who leave brighter paper trails than hardened criminals. Some are disturbed that AI models contributing to what ICE agents call "targeting packages" have their origins in military and intelligence software developed to fight terrorism. Courts have begun to question the legality of domestic mass surveillance. If ImmigrationOS proves to work as intended, these tensions will only grow.

ImmigrationOS was made possible by the White House's willingness to spend. In the 13 months since Mr Trump's second term began (and before a congressional stand-off over enforcement operations triggered a partial government shutdown on February 14th), ICE's parent Department of Homeland Security (DHS) had awarded, by one tally, $1.2bn in IT contracts. Of that, more than $81m went to Palantir. Officials are tight-lipped about the technology, as is Palantir. But Patrick Lechleitner, who led ICE in the final stretch of Joe Biden's administration, says ImmigrationOS will make information collected for criminal cases also "usable and useful" for civil immigration cases.

ICE has been adding to the types of data it crunches for years. Information on vehicle, phone and utilities usage is now hoovered up, as are data from local police, jails, courts and commercial databases, not to mention social media. But navigating several computer systems—what one former senior ICE official who requested anonymity calls "swivel-chair analytics"—

has slowed things down. AI, he believes, will paint a unified picture on a single screen.

One priority is weeding out falsehoods in visa applications. Simon Hankinson, a former State Department official in charge of technology for vetting visas, says such fraud was still rampant when he left in 2022. Fishy claims for asylum can also be spotted. Mr Hankinson, now an immigration researcher at the Heritage Foundation, a conservative think-tank in Washington, DC, says applicants have often "recycled" stories of political persecution. That will be harder to pull off with AI vetting.

Fed enough data, algorithms could also match names across hitherto-disconnected data sets. In November the Social Security Administration, America's pensions body, said it would comply with DHS requests for data to "identify and locate aliens". Records kept by departments of motor vehicles have also been useful, in part because many states issue drivers' licences regardless of immigration status. Suspicious-activity reports, in which banks flag potential signs of financial crime, offer clues, too. So do records from organisations, like welfare programmes, that interact with people on society's margins.

How well all this works, however, is unclear. Emily Tucker, director of Georgetown Law's Centre on Privacy & Technology and a co-author of reports on ICE, believes accuracy is poor. Last month in St Paul, Minnesota, ICE pulled a man in shorts from his home in freezing weather only to learn that the sex offender they were seeking was in prison. Officials have kept quiet on rates of false positives from AI. A related problem, says Steven Hubbard, a data scientist at the American Immigration Council, an advocacy group,

is that the inner workings of Palantir's AI are so opaque no one seems to know exactly how assessments are made. Palantir did not reply to requests for comment.

Opposition to ICE's methods is, therefore, growing. Courts have restricted access to some data. On February 5th a federal judge ruled that the Internal Revenue Service had illegally shared taxpayer data with DHS, and barred further access. Many government bodies, especially in blue states and "sanctuary" cities opposed to aggressive immigration sweeps, are not sharing. ICE is using two main tactics to get the data anyway.

One is to obtain records via subpoenas and court orders. Preparing the paperwork for a judicial warrant can take an investigator two or three days. With AI, many now get the job done in less than an hour, says Doug Gilmer, a former senior ICE officer who periodically advises DHS on the use of AI for combating human trafficking and other serious crime. The time savings will probably result in more requests for warrants. According to Mr Lechleitner, ImmigrationOS is even being configured to alert agents to the existence and location of potentially helpful information that privacy rules have kept off-limits. The idea is for the software to then advise agents on steps to obtain lawful access.

Another option is to purchase data. Some government bodies that refuse to share records with ICE nevertheless sell them to data aggregators that do. In Illinois, Cook County, home to Chicago, has disallowed data sharing for civil immigration enforcement, for example. But the county's jails sell records, via intermediaries, to LexisNexis Risk Solutions, which does have a contract with ICE. Hannah Lucal of Just Futures Law, a non-profit that files lawsuits to restrict immigration enforcement,

says such arrangements are often murky enough for local officials to be unaware of ICE's "backdoor" access.

Other data sources abound. ICE already buys data from ad firms that track consumer behaviour. Automated licence-plate readers provide additional information. ICE can also request footage from the more than 2,000 local police and fire departments in America that have partnered with Amazon's Ring video-doorbell service, though users can opt out.

ICE agents in the field can also snap and upload pictures for facial recognition. One system developed by Clearview AI, an American firm, contains more than 70bn pictures of people scraped from the public internet. Clearview's chief technologist, Amos Kyler, says ICE's Homeland Security Investigations (HSI) unit uses the database to find matches of priority suspects. Another firm, which has signed a secret contract with HSI, uses images from CCTV or body cams to find other pictures of the same objects, be they online or in other surveillance footage. The system, says the firm's chief technologist, does this by matching distinctive marks, like a dented bumper or a tear in clothing.

Such capabilities may invite mission creep. ICE has already begun to process images and social-media details of activists attempting to hinder arrests. But the effort has also sucked in data on law-abiding protesters, potentially chilling political speech. Moreover, critics fear that these protesters are being targeted by a Trump administration that has called opponents of ICE operations "domestic terrorists".

Thus far, this administration has been largely uninterested in engaging with its critics. The courts have also struggled to keep up with the rapid development of

these technologies, says Georgetown Law's Ms Tucker. The resulting lack of legal clarity has been taken, she believes, as a green light for their use. This also means, however, that legal challenges have plenty of scope to push back. Those in the cross-hairs will hope she is right. ■

Curious about the world? To enjoy our mind-expanding science coverage, sign up to Simply Science, our weekly subscriber-only newsletter.

Science & technology | The nature of nurture

The Human Exposome Project will map how environmental factors shape health

It makes the Human Genome Project look easy

February 19th 2026