FORD SCHOOL
SCIENCE, TECHNOLOGY,
AND PUBLIC POLICY
UNIVERSITY OF MICHIGAN

June 2026

Understanding ICE Surveillance and its Civil Rights Implications

Madeleine Gibbons-Shapiro, Master's in Public Policy '27

EXECUTIVE SUMMARY

Recent operations of U.S. Immigration & Customs Enforcement (ICE) have revealed an extensive web of surveillance technologies and databases of private information that ICE uses to track, arrest, and deport people. ICE contracts with private companies and collects information from other government agencies to amass tremendous quantities of sensitive data including locations and real-time movements, biometrics, and online behaviors. These tactics raise many civil rights concerns including Fourth Amendment violations; the expanded powers of ICE and the U.S. Department of Homeland Security (DHS); and the federally unchecked ability of corporations to access and sell private data, including from government agencies. Congress should defund ICE's budget for surveillance technology, develop formal oversight of DHS's use of said technology, and ban data brokers from amassing and selling personal data. State governments should cease the use of mass surveillance systems and enact privacy protections.

KEY FINDINGS

- Under the second Trump administration, the U.S. Department of Homeland Security (DHS) and U.S. Immigrations & Customs Enforcement (ICE) have created a large-scale, complex surveillance system.
- The surveillance system amasses residents' personal information from disparate government databases; tracks immigrants and allies' locations with tools such as automated license-plate reader (ALPR) cameras; and breaks into people's phones without their knowledge.
- ICE and U.S. Customs & Border Protection (CBP) violate civil rights by collecting and using biometric facial recognition data without reasonable suspicion.
- Federal lawmakers have attempted to challenge these violations through the introduction of bills and open letters but have not made meaningful changes. State lawmakers have made some progress pushing back against the use of ALPR cameras and data sharing with ICE.

BACKGROUND: ICE'S WIDESPREAD SURVEILLANCE TACTICS

Collecting and connecting sensitive government datasets

Over the last several years, ICE has created a large database pooling personal information from federal government agencies, state and local governments, and private companies to track immigrants and their families and allies. The methods and speed with which ICE is building and using this database have expanded rapidly during Trump's second term. The database and its accompanying data-sharing network have facilitated hundreds of thousands of bulk searches for data on driver's licenses and motor vehicles and has recently expanded to include voter registration and Social Security.[1]

Using more than $113 million in federal funding, DHS has paid the private company Palantir to create individual "dashboards" by aggregating information from sources like Medicaid and the IRS. This information was previously separate in order to

protect private data and increase public trust in the federal government over sensitive issues like personal finances and health care.[2] ICE agents access these dashboards using apps like Palantir's Elite, which pinpoints people's addresses, criminal records, and other information to create a "confidence score" based on how recent and accurate the information is likely to be and pays private investigators to verify that data.[3]

Photo credit: Longfin Media - stock.adobe.com

Tracking Immigrants' Real-Time Movements

ICE recently contracted with Flock Safety, which has sold nearly 80,000 cameras to police departments, malls, grocery stores, hospitals, schools, and churches nationwide in order to access real-time license plate tracking data. Flock cameras are automated license plate readers (ALPRs) which have been used by local police departments to feed license plate and location data to the Trump administration. Evidence shows that local police were searching for "illegal immigration" in Flock's database even before any official Flock contracts had been in place, including in states where immigration enforcement by local police is illegal. Flock's ALPR cameras—alongside their drones and "gunshot detection" microphones—not only track and report real-time location information, they also allegedly predict people's "future locations" based on their movement patterns.[4] To further incentivize local police to search and aggregate personal data for immigration enforcement, Flock has partnered with Lexipol, a company with a "License Plate Readers Grant Assistance Program," which funds police who use ALPR cameras by fast-tracking installation and covering all upfront implementation costs.[5] With a growing ability to track immigrants across the U.S., even in self-proclaimed "sanctuary" cities, ICE has created a national surveillance infrastructure.

With a growing ability to track immigrants across the U.S., even in self-proclaimed "sanctuary" cities, ICE has created a national surveillance infrastructure.

Surveillance of Protestors

On top of its tracking of immigrants, ICE also surveils protestors, legal observers, and anyone who attempts to prevent or record ICE arrests. ICE uses software from a company called Paragon to remotely break into people's phones—including end-to-end encrypted chats like Signal or WhatsApp—without that person even clicking a link.[6] Further, ICE employs the company Penlink to scrape web information from data brokers about anyone with a social media account, creates fake social media accounts to track those people, and uses technology developed for use in conflict zones in Iran and Afghanistan to locate protestors' phones without a warrant.[7] ICE agents have also recently been spotted wearing Meta's AI smart glasses, likely to identify people's movement and faces in real time.[8]

PROTECTING YOURSELF FROM SURVEILLANCE

Despite the pervasiveness of ICE surveillance, there are steps you can take to help secure your devices and reduce ICE access to your data. Because the tools and tactics that ICE uses keep changing, we recommend using guidance from organizations committed to regularly updating their resources, such as Activist Checklist or the Electronic Frontier Foundation's Surveillance Self-Defense Toolkit. Keep your phone software up to date, use strong passwords, and enable multifactor authentication wherever possible.

ICE AND CIVIL RIGHTS

ICE's use of private information from government databases, personal devices, and location-tracking cameras to target Americans—documented or undocumented—is a violation of civil rights in the following ways:

- **Groundless biometric arrests**: ICE agents arrest people without warrants, sometimes relying on Mobile Fortify's biometric screening and database as a primary means of identification, rather than any physical documentation of U.S. citizenship the person may have, including a birth certificate.[9]

- **Racially biased biometric tools**: the Mobile Fortify facial recognition software is known to be less accurate at identifying people with darker skin, exacerbating pre-existing concerns about racial profiling.[10]

- **Fourth Amendment violations**: ICE conducts unreasonable searches and seizures of immigrants—and their allies—regardless of their documentation status. They do so using blanket surveillance systems like ALPRs and paying data brokers to amass and sell people's personal information.

Federal and state challenges to civil rights violations

Because of the Republican Majority in Congress, federal lawmakers who oppose these tactics remain relatively unable to make serious change. In October of 2025, Congresswoman Shontel Brown (D-OH), Ranking Member of the Committee on Oversight's Cybersecurity, Information Technology, and Government Innovation Subcommittee, wrote an open letter to DHS demanding regulation and transparency surrounding the "digital dragnet surveillance system."[11] Rep. Bennie G. Thompson (D-MS), Ranking Member of the Committee on Homeland Security, has introduced the Realigning Mobile Phone Biometrics for American Privacy Protection Act (H.R.7124) to limit DHS's unchecked use of Mobile Fortify.[12] Neither effort has made much headway. DHS replied to Congresswoman Brown's letter in April 2026, acknowledging the use of a "specific tool" for surveillance but failing to provide requested documentation of oversight or safeguards; H.R.7124 has not moved past the initial introduction phase in the House.[13]

However, in the absence of federal regulation to curb DHS's unconstitutional technology and surveillance usage, state governments have had some success fighting back. State courts have begun litigating against Fourth Amendment violations posed by local governments' use of ALPR cameras. A U.S. District Court in Virginia has challenged the city of Norfolk's use of Flock ALPR cameras, which gather data on all vehicles without a warrant.[14] Similarly, when Illinois Secretary of State Alexi Giannoulias discovered that Flock had been illegally allowing U.S. Customs & Border Protection (CBP) access to Illinois ALPR cameras to surveil drivers, his office ordered an immediate stop to said data-sharing.[15] With growing state-level pushback on the Trump administration's surveillance tactics, state governments may be able to protect their residents in ways the federal government is currently unable or unwilling to do.

ICE's use of private information from government databases, personal devices, and location-tracking cameras to target Americans—documented or undocumented—is a violation of civil rights.

POLICY RECOMMENDATIONS

Federal

Stop funding for ICE/DHS use of surveillance technology, and develop formal oversight over its current use.

The July 2025 passage of the One Big Beautiful Bill Act (OBBBA) allocated $190 billion in funding to DHS and exploded ICE's budget from $9.8B in FY24 to $85.1B in FY25—with only 13% of that figure obligated for a specific purpose.[16] There has been

little publicly available data regarding ICE's spending and only broad, vague information as to how it was appropriated. In future funding cycles, Congress should remove the $6 billion appropriated to CBP's "Technology, Screening, and Surveillance" program.[17] Congress must also reinstate staff removed from the Office for Civil Rights and Civil Liberties (CRCL) and bolster CRCL's ability to oversee DHS civil rights abuses, including increased transparency, auditing, and funding for staff with surveillance technology expertise.[18]

Ban DHS from amassing bulk data on residents

On June 12, 2026, Section 702 of the Foreign Intelligence Surveillance Act (FISA)—the provision intended to prevent federal agencies from gathering bulk data on U.S. citizens—was up for reauthorization.[19] This act has frequently been cited as the source of a loophole that has allowed data brokers to both buy bulk private data and sell that data to the federal government, violating the Fourth Amendment.[20] Congress should pass reforms to FISA's reauthorization to prevent such purchase and sale of personal data—and to prevent the Trump administration from continuing its unregulated buying of residents' data and their sharing of that data with ICE and CBP.

State & Local

Cease use of mass surveillance systems

Similarly, state and local governments should end the use of ALPR surveillance and AI facial recognition software in their jurisdictions. The best way to protect this information is not to collect it in the first place. Where surveillance systems remain in use, prohibit ICE from tapping into local networks, and prohibit local agencies from sharing data for immigration enforcement.[21] Municipal and state governments should refuse surveillance-driven contracts, pilot programs, surveillance equipment, and donor funding.[22]

Enact data privacy protections

Especially for the 19 states that offer drivers' licenses to state residents regardless of their immigration status, states must restrict DHS access to DMV information. State governments should follow California's lead with its California Values Act, which prohibits all members of the California Law Enforcement Telecommunications System from using information for immigration enforcement if the individual does not have a criminal history.[23] State governments should also model data protections after Montana's law that prevents the government from buying cellphone data via data brokers and the use of other mechanisms that elude the Fourth Amendment.[24] With rigorous state and local data protection practices, states can unite against ICE's invasive surveillance of U.S. residents.

ENDNOTES

1. Jonathan Shorman, "Homeland Security Wants State Driver's License Data for Sweeping Citizenship Program," Stateline, November 25, 2025, https://stateline.org/2025/11/25/homeland-security-wants-state-drivers-license-data-for-sweeping-citizenship-program/.
2. Cindy Cohn and Max Taves, "Cohn: Trump Is Building 'One Interface to Rule Them All.' It's Terrifying," *The Mercury News*, August 25, 2025, https://www.mercurynews.com/2025/08/23/opinion-trumps-plan-for-one-interface-to-rule-them-all-risks-our-privacy-and-security/; William Turton, Christopher Bing, and Avi Asher-Schapiro, "The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE," *ProPublica*, July 15, 2025, https://www.propublica.org/article/trump-irs-share-tax-records-ice-dhs-deportations
3. Joseph Cox, "'ELITE': The Palantir App ICE Uses to Find Neighborhoods to Raid," 404 Media, January 20, 2026. https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid/.
4. Jason Koebler, "Flock Off," 404 Media, February 2, 2026, https://www.404media.co/icezine/.
5. Beryl Lipton and Sarah Hamid, "'Free' Surveillance Tech Still Comes at a High and Dangerous Cost," Electronic Frontier Foundation, February 13, 2026, https://www.eff.org/deeplinks/2026/02/free-surveillance-tech-still-comes-high-and-dangerous-cost.
6. Joseph Cox, "ICE's Silent Exploit," 404 Media, February 2, 2026, https://www.404media.co/icezine/.
7. Sheera Frenkel and Aaron Krolik, "The Tech Arsenal That ICE Has Deployed in Minneapolis," *The New York Times*, January 31, 2026, https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html; "Shubhanjana Das, "ICE Isn't Just Tracking Your Phone. The Surveillance Technology Goes Further Than That," *Sahan Journal*, February 4, 2026, https://sahanjournal.com/immigration/ice-surveillance-technology-facial-recognition-phones-minnesota/.
8. Joseph Cox, "Meta Debate," 404 Media, February 2, 2026, https://www.404media.co/icezine/.
9. "How ICE Went Rogue: Analysis of the Legal Authorities Governing ICE," American Immigration Council, February 11, 2026, https://www.americanimmigrationcouncil.org/fact-sheet/ice-cbp-legal-analysis/.
10. Jay Stanley, "Face Recognition and the 'Trump Terror': A Marriage Made in Hell | ACLU," American Civil Liberties Union, March 17, 2026, https://www.aclu.org/news/privacy-technology/ice-face-recognition.
11. "Brown Leads Oversight Letter to DHS on ICE's Troubling Mass Surveillance Tech | Representative Shontel Brown," Office of Congresswoman Shontel Brown, February 19, 2026, https://shontelbrown.house.gov/media/press-releases/brown-leads-oversight-letter-dhs-ices-troubling-mass-surveillance-tech.
12. "Ranking Member Thompson Introduces Legislation to Curb Unchecked DHS Mobile Biometric Surveillance and Protect Privacy of American Citizens," Committee on Homeland Security, January 15, 2026, https://democrats-homeland.house.gov/news/legislation/ranking-member-thompson-introduces-legislation-to-curb-unchecked-dhs-mobile-biometric-surveillance-and-protect-privacy-of-american-citizens.
13. "Rep. Summer Lee, Colleagues Slam DHS Response on ICE Use of Foreign Spyware, Vow Continued Oversight | Congresswoman Summer Lee," Office of Congresswoman Summer Lee, April 3, 2026, https://summerlee.house.gov/newsroom/press-releases/rep-summer-lee-colleagues-slam-dhs-response-on-ice-use-of-foreign-spyware-vow-continued-oversight; "H.R.7124 - 119th Congress (2025-2026): Realigning Mobile Phone Biometrics For American Privacy Protection Act," Library of Congress, January 15, 2026, https://www.congress.gov/bill/119th-congress/house-bill/7124.
14. Dan King, "Judge Rules Lawsuit Challenging Norfolk's Use of Flock Cameras Can Proceed," Institute for Justice, February 6, 2025, https://ij.org/press-release/judge-rules-lawsuit-challenging-norfolks-use-of-flock-cameras-can-proceed/.
15. "Giannoulias' Audit Finds License Plate Reader Company in Violation of State Law," Illinois Secretary of State, August 25, 2025, https://www.ilsos.gov/news/2025/august-25-2025-giannoulias-audit-finds-license-plate-reader-company-in-violation-of-state-law.html.
16. Bill Chappell, "How ICE Grew to Be the Highest-funded U.S. Law Enforcement Agency," NPR, January 21, 2026, https://www.npr.org/2026/01/21/nx-s1-5674887/ice-budget-funding-congress-trump.
17. Dominik Lett, "Here's How the Administration Plans to Spend the Largest Immigration Enforcement Funding Surge in History," Cato Institute, March 27, 2026, https://www.cato.org/blog/heres-how-administration-plans-spend-largest-immigration-enforcement-funding-surge-history.
18. "Reforms to Curb DHS, ICE, CBP Overreach," Brennan Center for Justice, March 31, 2026, https://www.brennancenter.org/our-work/analysis-opinion/reforms-curb-dhs-ice-cbp-overreach.
19. Hannah James and Elizabeth Gotein, "Section 702 of the Foreign Intelligence Surveillance Act," Brennan Center for Justice, April 10, 2026, https://www.brennancenter.org/our-work/research-reports/section-702-foreign-intelligence-surveillance-act.

ENDNOTES

20. Jude Joffe-Block, "Your Data Is Everywhere. The Government Is Buying It Without a Warrant," NPR, March 25, 2026, https://www.npr.org/2026/03/25/nx-s1-5752369/ice-surveillance-data-brokers-congress-anthropic.
21. Koebler, "Flock Off."
22. Lipton and Hamid, "'Free' Surveillance Tech."
23. "Protecting State Driver's License Information," NILC, March 26, 2026, https://www.nilc.org/resources/protecting-state-drivers-license-information/.
24. Joe Lancaster, "Montana Closes Data Broker Loophole for Government Surveillance," *Reason*, May 16, 2025, https://reason.com/2025/05/16/new-montana-law-blocks-the-state-from-buying-private-data-to-skirt-the-fourth-amendment/.