Immigration, DOGE, and Data Privacy

A resource in collaboration between Center for Democracy & Technology and The Leadership Conference's Center for Civil Rights and Technology

Last updated May 9, 2025

Federal agencies collect personal data about individuals to administer programs and benefits, such as student loans or Social Security. This information, also known as administrative data, can pose a range of potential risks to immigrants (i.e. anyone who is not a U.S. citizen) and their families if it is used for purposes other than public service delivery. Because data collection and surveillance that targets immigrants is often done to find the current location of individuals, even the most seemingly mundane and non-sensitive information (such as current living address, familial associations, and employer) can have immense ramifications.

This explainer summarizes the types of administrative data the federal government holds that could directly or indirectly locate or identify immigrants, the potential impacts of federal immigration authorities and Department of Government Efficiency's (DOGE) access to this information, the use of this information for immigration-related purposes, and unanswered questions.

Federal Administrative Data Background

Federal agencies collect a wide swath of information to administer government services and public benefits. This includes the following data points:

Identifying Information:	***Contact Information:***
• Legal name • Date of birth • Social Security number • Individual taxpayer identification number (ITIN)	• Home and work address • Work and mobile phone numbers • Email address
Demographics:	***Life events:***
• Race • Nationality • Sex • Disability • Citizenship status	• Employment records • Pregnancy and birth • Marriage and divorce • Job loss • Bankruptcy • Family deaths

Repurposing Federal Administrative Data for Immigration Enforcement

While it was at first purported to be an advisory body, DOGE has transformed into an embedded group obtaining expansive access to government databases, enabling the seizure of the most sensitive information about tens of millions of people across the United States. Over the past several months, DOGE representatives have gained access to sensitive information from a large number of federal agencies. There are now **fourteen** lawsuits that allege violations of **six** federal privacy protections across **eight** federal agencies. This information could be repurposed for immigration enforcement; in fact **one of these lawsuits challenges Department of Homeland Security's (DHS) attempt to access Internal Revenue Service (IRS) data for immigration purposes**. Moreover, federal immigration authorities are actively seeking information held by other agencies for enforcement purposes. **Sources:** Just Security Litigation Tracker; New York Times Lawsuit Tracker; DOGE and Government Data Privacy, March 17, 2025

Recent reporting details a new agreement between the IRS and Immigration and Customs Enforcement (ICE) that would provide details on people who have been ordered to leave the U.S. or are being investigated; ICE has expressed a desire to access tax data on as many as seven million people. **Source:** Top I.R.S. Officials Said to Resign After Deal to Give ICE Migrants' Data, April 8, 2025

Likewise, the Department of Housing and Urban Development (HUD) recently entered an agreement with the DHS that enables the two agencies to share information and resources aimed at addressing the "abuse" of federal housing benefits by undocumented immigrants. **Source:** HUD, DHS Seek to Stop Undocumented Immigrants from Using Federal Housing Programs, March 24, 2025

DOGE Access to Data on Immigrants

Recent reporting also indicates that DOGE has been granted access to data held by the U.S. Citizenship and Immigration Services (USCIS), including information about refugees, asylum seekers, naturalized citizens, and immigrants. This database includes an extensive amount of information on individuals who have engaged with the immigration process in the United States. **Sources:** DOGE Granted Access to Naturalization-Related IT Systems, Memo Shows, April 2, 2025

DOGE has gained access to sensitive data of migrant children, including reports of abuse, mental health, and photos. Experts question why DOGE needs access to these highly sensitive records. **Source:** DOGE Gained Access to Sensitive Data of Migrant Children, Including Reports of Abuse, April 3, 2025

Three Immigration-Related Use Cases

Federal administrative data could be used for immigration-related efforts in at least three ways:

1. *Identifying Immigrants*
2. *Locating Immigrants*
3. *Identifying and Acting Upon Entitlement Fraud*

Use Case #1: Identifying Immigrants

Federal administrative data can be repurposed to aid immigration authorities in identifying immigrants for investigation or potential enforcement efforts.

"I [Donald Trump] am also ordering the establishment of an interagency working group to improve access to administrative records, with a goal of making available to the Department [of Commerce] administrative records showing citizenship data for 100 percent of the population."

Donald Trump, President of the United States
Source: Executive Order 13880—Collecting Information About Citizenship Status in Connection With the Decennial Census, July 11, 2019

Federal agencies collect information that directly, or indirectly, identifies immigrants:

Direct Identification	Indirect Identification
Example: The Social Security Administration collects immigration status as some lawfully present non-U.S. citizens are eligible for this public benefit.	***Example***: The U.S. Department of Education collects the Social Security numbers of students' parents who are applying for financial aid. An immigrant parent without a Social Security number would submit 000-00-0000 or N/A.

Use Case #2: Locating Immigrants

Federal administrative data can be repurposed to aid immigration authorities in locating known immigrants for the purposes of deportation or other enforcement actions.

"In a recent video call, DHS officials told IRS officials they needed access to their data to help them locate up to 7 million suspected undocumented immigrants – an eye-popping figure that 'shocked' IRS employees, according to a source with knowledge of the meeting."

Source: IRS Reaches Data-Sharing Deal With DHS to Help Find Undocumented Immigrants for Deportation, April 8, 2025

Federal agencies that administer government services and benefits collect contact information for individuals:

Function	Indirect Identification	Undocumented Immigrants	Contact information
Example: Tax filing (IRS)	Approx. 167 million individual tax returns	Approx. 5.4 million active ITINs (proxy for undocumented filers; includes immigrant visitors with work authorization)	• Mailing Address • Phone Numbers • E-mail Address • Date of Birth

Use Case #3: Identifying and Acting Upon Entitlement Fraud

Combining data that identify immigrants, along with information on how to locate them, can be used to recognize and take action based on potential entitlement fraud, which is knowingly providing false or misleading information to access public benefits for which a person is ineligible. Given that more than 90 percent of individuals who commit this crime are U.S. citizens, it is unlikely that this effort would yield significant cost savings; however, it could become the basis for removal as entitlement fraud is a crime (whereas overstaying a visa and being present in the U.S. without authorization are civil offenses).

"The Social Security Administration is dedicated to protecting the vital benefits that American workers have earned on behalf of themselves and their families. We are committed to working diligently to implement the President's memorandum and to ensure that benefits are paid only to those who should receive them."

Acting Commissioner Leland Dudek

Source: Social Security Statement on President Trump's Memorandum, "Preventing Illegal Aliens from Obtaining Social Security Act Benefits", April, 15, 2025

Federal agencies are entering into data sharing agreements to pursue entitlement fraud, along with immigration enforcement actions.

Federal Agency	Administrative Data Action
Social Security Administration	Based on data provided by DHS, SSA added 6,300 migrants to its death master file, resulting in cutting off individuals from "crucial financial services like bank accounts and credit cards, along with their access to government benefits."

Source: Social Security Lists Thousands of Migrants as Dead to Prompt Them to 'Self-Deport', April 10, 2025

Legal Protections for Federal Administrative Data and Law Enforcement Exceptions

Existing, long-standing legal protections are relevant to whether and how federal administrative data can be used for immigration enforcement purposes. These protections include, but are not limited to:

- **The Privacy Act of 1974:** The Privacy Act generally prohibits sharing of personal data outside of agencies without individual consent, but provides exemptions for: (1) civil or criminal law enforcement activity by another agency; and (2) for "routine uses," as defined by the agency. Routine uses often include law enforcement purposes. Additionally, the Privacy Act only protects the personal data of U.S. citizens, including naturalized citizens and lawful permanent residents. **Source:** 5 U.S. Code § 552a - Records Maintained on Individuals

- **§6103 of the Internal Revenue Code:** The Internal Revenue Code provides additional restrictions beyond the Privacy Act for accessing tax records. This protection applies to all tax records including those shared with other federal agencies like the Department of Education and the Social Security Administration. However, it does permit sharing tax return information for use in investigating potential violations of federal criminal statutes not related to tax administration. Overstaying a visa and being physically present in the U.S. is not a crime, but rather a civil immigration matter under federal law. **Source:** 26 USC 6103: Confidentiality and Disclosure of Returns and Return Information

- **E-Government Act of 2002:** The E-Government Act of 2002 recognized that computers and tech advances have important ramifications for the protection of personal information. Two portions of the E-Government Act set security standards and limitations on the sharing and use of data:

    - **Federal Information Security Modernization Act of 2014 (FISMA):** Requires Privacy Impact Assessments (PIAs) for transferring large amounts of personal data. For example, the IRS would be responsible for publishing a PIA before conducting a data transfer containing the personal information of 7 million individuals to another agency (even if such a transfer was otherwise lawful). **Source**: Federal Information Security Modernization Act of 2014

    - **Confidential Information Protection and Statistical Efficiency Act (CIPSEA):** Requires informed consent to use or disclose information collected exclusively for statistical purposes for non-statistical purposes. There is no exception for law enforcement purposes, so agencies with statistical data (e.g., the Census Bureau) would not be permitted to share that data for immigration enforcement purposes. **Source**: Confidential Information Protection and Statistical Efficiency Act

- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA generally prohibits the disclosure of protected health information (PHI) held by healthcare providers and insurers without informed consent, but provides exceptions for law enforcement purposes, including: (1) to respond to a court order, warrant, or administrative requests; and (2) to respond to requests for PHI to identify/locate a suspect or fugitive. HIPAA can apply to certain public benefits programs where protected health information (PHI) is electronically transmitted in connection with certain transactions (e.g., Medicaid). This would include agencies that administer these programs, such as the Department for Health and Human Services (HHS). **Source:** Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement

Impact of Government Data Access and Use on Immigrants

- **Mass Surveillance and Data Collection Leading to Targeting of Lawful Immigrants and U.S. Citizens:** As the federal government seeks to create a vast repository of data to surveil immigrants—including tax records, Social Security information, and immigration-related data—this will inevitably include information about lawful immigrants and U.S. citizens. Such a database fuels mass surveillance and data collection practices that allow for administrative data to be repurposed to target and deport even individuals with lawful status.

- **Loss of Critical Social Services:** Immigrants and immigrant families, including families that are mixed-status (in which at least one family member is undocumented but others are lawfully present), could face the loss of federal housing support, education assistance, food aid, and health care to which they are otherwise entitled, as a result of the misuse and abuse of federal data. Immigrant families and individuals, no matter their legal immigration status, could also be deterred from obtaining critical social services for fear of having their personal data used to target them or their family members for detention or deportation. **Sources:** Trump Administration 'Villainizes' Immigrant Families with Misleading Directive on Food Aid, March 20, 2025; Weaponizing Immigrant Tax Data: How IRS-DHS Cooperation Would Undermine Tax Compliance, Increase Burdens, and Threaten Data Privacy, March 24, 2025

- **Loss of Revenue and Disincentivization of Participation in Public Infrastructure:** Repurposing federal administrative data for immigration enforcement may also lead to unintended consequences that disincentivize immigrants and U.S. citizens from participating in core public programs. This could undermine tax compliance within immigrant communities out of fear that their tax information could be used against them, leading to significant losses in federal revenue and eroding public trust in government services. **Sources:** Weaponizing Immigrant Tax Data: How IRS-DHS Cooperation Would Undermine Tax Compliance, Increase Burdens, and Threaten Data Privacy, March 24, 2025; The Potential Impact of IRS-ICE Data Sharing on Tax Compliance, April 8, 2025

- **Increased Security Risks and Harm From Pooled Data:** The centralization and combination of multiple data sources from across the federal government creates significant security vulnerabilities. Any centralized database, and especially one at scale, increases the likelihood of data breaches, hacking attempts by malicious actors, and other privacy harms, compromising the privacy and safety of all U.S. residents. **Source:** DOGE Is Building a Master Database to Surveil and Track Immigrants, April 18, 2025

- **Incomplete Data and Decreased Data Quality:** Combining and repurposing federal administrative data for federal immigration enforcement also comes with the risks of incorrect identifications or matches due to incomplete or poor data quality. When large datasets are combined without appropriate measures to ensure the completeness, accessibility, and quality of data sources, the overall utility and accuracy of the combined dataset is significantly diminished and can often lead to harmful outcomes like the misidentification of individuals targeted for deportation. Additionally, similar to disincentives to participate in government services, this may also create a chilling effect in federal data collection efforts including the decennial census, further eroding quality information.

Unanswered Questions

The potential that DOGE and federal immigration authorities may access various federal administrative databases for law enforcement and immigration purposes raises a number of unanswered questions:

- **Legality:** As immigration enforcement authorities seek information held by other agencies, their legal authority to do so is still under question. While laws such as the Internal Revenue Code allow for information sharing with federal law enforcement for non-tax criminal investigations, such actions would run counter to decades of existing precedent. Moreover, some forms of immigration enforcement are civil rather than criminal in nature. **Source:** IRS Nears Deal with ICE to Share Addresses of Suspected Undocumented Immigrants, March 22, 2025

- **Artificial Intelligence (AI):** Both DOGE and federal immigration authorities have indicated that they will seek to expand the use of AI for a variety of purposes. For instance, reports indicate that DOGE is already using AI to make a range of high-stakes decisions across the federal government. Moreover, prior to the inauguration, DHS issued a directive on the agency's acquisition and use of AI, including restrictions on how the technology can be used in immigration enforcement. The status of, and compliance with, this directive is uncertain, raising significant questions about how DHS officials may use AI tools to analyze information accessed across the federal government. **Sources:** 100 Days of DOGE: Assessing Its Use of Data and AI to Reshape Government; April 30, 2025; New DHS AI Directive Sets Prohibited Uses, Expands Acquisition Governance, January 17, 2025

- **Combining Social Media Monitoring with Administrative Data:** DHS recently issued a notice indicating that it will screen social media content and use AI-powered tools to surveil social media data in order to identify and target individuals for deportations. This raises unanswered questions about DHS's intentions to combine information from social media platforms with federal administrative data, and how this may be used to target immigrants. **Sources:** New Collection: Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms, March 5, 2025; DHS to Begin Screening Aliens' Social Media Activity for Antisemitism, April 9, 2025; Automated Tools for Social Media Monitoring Irrevocably Chill Millions of Noncitizens' Expression, April 15, 2025

What to Look for Next

Recent actions by DOGE and federal immigration authorities indicate that there will likely be additional changes to the federal government's approach to data access and sharing in the coming months. These pose new risks to U.S. citizens and noncitizens alike, and continue to undermine public trust and transparency about why, when, and to what extent federal agencies are accessing and using data to make highly consequential decisions about immigration.

- **More Federal Data Sharing:** On March 20, 2025, President Trump signed Executive Order 14243, which directs federal agencies to take significant steps to remove any guardrails that prevent the sharing of unclassified information between federal agencies. While purportedly aimed at addressing fraud, waste, and abuse, the EO lays the groundwork for unprecedented access to highly sensitive information across the entirety of the federal government. **Source:** Trump Order on Information Sharing Appears to Have Implications for DOGE and Beyond, March 21, 2025

- **Public Documentation Updates:** Already, federal agencies like the Office of Personnel Management have quietly updated their public documentation, such as privacy impact assessments and system of record notices, to account for changes in the access and use of federal information. Similar actions are likely to occur to facilitate information sharing for the purposes of immigration enforcement. **Source:** OPM Quietly Swapped Out Privacy Assessment for Governmentwide Email System Central to Ongoing Litigation, March 3, 2025

- **State Administrative Data Collection:** Under the first Trump administration, the federal government actively sought administrative data from states for immigration enforcement. Such efforts are likely to occur again, as EO 14243 directs federal agencies to seek comprehensive access to data from all state programs that receive federal funding. **Source:** 4 States Sharing Data to Help Trump Administration Determine Citizenship Status: Report, July 15, 2020