Federal Efforts to Expand Access to Data from State-Run Programs and Individual Privacy

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

Last updated July 23, 2025

State agencies collect personal data about individuals to administer a range of programs and benefits, such as Medicaid and Unemployment Insurance. Historically, this information, also known as state administrative data, has been safeguarded by states and only shared with federal agencies when necessary to execute federally funded programs and in adherence with privacy and security standards. Recent attempts by the federal government to dramatically expand access to sensitive data that has historically been safeguarded by states run counter to decades of precedent, threatening the privacy and security of millions of state residents' personal information.

This explainer summarizes the types of administrative data held by state governments, the history of and current efforts by the federal government to expand its access to this information, the potential harms of federal agencies' and the Department of Government Efficiency's (DOGE) unprecedented access to state data, unanswered questions about the lasting impacts of these actions, and other sources of state data that may come under threat.

Although this explainer primarily focuses on data that states collect to administer public benefits programs, states also collect and maintain personal data like voting rolls, DMV records, and education data, many of which present the same risks and challenges described in this resource.

State Administrative Data Background

Millions of individuals receive public benefits from programs that are administered by state agencies and are at least partially funded by the federal government, including:

- More than **78 million people** receive health care through **Medicaid** and the **Children's Health Insurance Program (CHIP)**. **Source:** March 2025 Medicaid & CHIP Enrollment Data Highlights, March 2025.

- More than **42 million people** receive food assistance through the **Supplemental Nutrition Assistance Program (SNAP)**. **Source:** SNAP: Monthly Participation, Households, Benefits, June 2025.

State Administrative Data Background (cont.)

- More than **6.7 million women and children** receive food assistance through the **Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)**. **Source:** WIC Annual Participation and Costs, June 2025.

- More than **2 million people** receive cash assistance through the **Temporary Assistance for Needy Families (TANF) program**. **Source:** Temporary Assistance for Needy Families (TANF) Caseload Data - Fiscal Year 2024, January 2025.

- More than **5 million people** receive financial assistance through **Unemployment Insurance**. **Source:** Unemployment Insurance Data, May 2025.

To administer these state-run public benefits programs, state agencies collect a wide swath of information, including the following:

Identifying Information: • Legal name • Date of birth • Social Security number	**Contact Information:** • Home and work address • Work and mobile phone numbers • Email address
Demographics: • Race • Sex • Disability • Citizenship status	**Life events:** • Employment records • Pregnancy and birth • Marriage and divorce • Job loss • Household income and property • Incarceration history • Foster care history

Some of the information collected by state agencies includes sensitive data that may not be captured in existing federal databases. For example:

To administer **Medicaid**, **Virginia** collects:	To administer **TANF**, **Illinois** collects:	To administer **Unemployment Insurance**, **Maryland** collects:
• Alien registration number (if applicable) • Incarceration date, jurisdiction of jail, and expected release date • Foster care history (including what state) **Source:** Virginia Medicaid Standard Application.	• Any unearned income, such as unemployment benefits, child support payments, etc. • Proof of relationship to everyone included on application, like a birth certificate • Documents showing any child or spousal support paid and the names of absent parents **Source**: Disability Benefits 101, Illinois.	• Reason for separation from employer • Union name and local number (if applicable) • Any past or scheduled payments, including severance, vacation, holiday, bonus, or retirement payments, back pay, damages, and special payments **Source:** Maryland Department of Labor, Claimant Most Frequently Asked Questions - Unemployment Insurance.

History of Federal Attempts to Access State Administrative Data

Federal efforts to access sensitive state data that have historically been held and safeguarded at the state-level have accelerated over the last decade. Under the George W. Bush administration and continuing through much of the Obama administration, for example, U.S. Immigration and Customs Enforcement (ICE) sought biometric information like fingerprints from states and cities to aid in immigration enforcement. Further efforts to access state data continued under the first Trump administration. As part of a purported investigation into voter fraud, the Presidential Election Integrity (Pence-Kobach) Commission sought voter registration data from every state, including names, addresses, birthdates, partial Social Security numbers, party affiliation, and history of incarceration — an effort that was later abandoned after significant legal pushback from a bipartisan group of states and fierce opposition from the civil rights and pro-democracy communities.

History of Federal Attempts to Access State Administrative Data (cont.)

Subsequently, the first Trump administration also issued an executive order seeking citizenship data from cities and states as part of the census, but more than a dozen states across the political spectrum refused to share this information. **Sources:** Obama Ends Secure Communities Program That Helped Hike Deportations, November 2014; President Trump Launches Commission on 'Election Integrity', May 2017; Trump Dissolves Controversial Election Commission, January 2018; Census Bureau Asks States For Driver's License Records To Produce Citizenship Data, October 2019; President Trump's Election Commission Has Already Violated Federal Law, October 2017; Letter to Secretaries of State regarding Pence Kobach Commission Data Request, July 2017.

"In the event I were to receive correspondence from the Commission [...] [m]y reply would be: They can go jump in the Gulf of Mexico and Mississippi is a great State to launch from."

Delbert Hosemann, Former Mississippi Secretary of State, on the Presidential Election Integrity Commission's request for state voting records

Source: Secretary Hosemann's Statement on Request for Voter Roll Information, **July 2017.**

Current Federal Attempts to Access and Use State Administrative Data

On March 20, 2025, President Trump signed an executive order directing federal agencies to gain access to all data held by state programs that receive federal funding, including relevant data held by third-party vendors. Following this order, the U.S. Department of Agriculture (USDA) sent a letter on May 6 to state agencies responsible for overseeing SNAP, demanding access to a host of sensitive information about every SNAP applicant and recipient since 2020, including their names, Social Security numbers, and addresses. In the same letter, USDA specified it was already taking steps to seek this information directly from the third-party vendors who serve as SNAP payment processors. **Sources:** Executive Order 14234—Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, March 2025; FNS Data Sharing Guidance, May 2025; Letter to Payment Processors, May 2025.

Current Federal Attempts to Access and Use State Administrative Data (cont.)

On May 22, 2025, Protect Democracy, Student Legal Defense Network, Electronic Privacy Information Center (EPIC), and the National Center for Law and Economic Justice filed a lawsuit challenging USDA's requests under federal privacy statutes. In response, USDA acknowledged in a declaration that it needed to comply with the procedures required by these statutes prior to initiating the data collection and has since published a related System of Record Notice (SORN). SORNs are public notices about federal agencies' collection and use of personally identifiable information required under the Privacy Act of 1974. **Sources:** USDA Sued for Illegally Demanding the Personal Information of Millions of SNAP Recipients From States, May 2025; USDA SORN, June 2025.

The Trump administration's push to amass sensitive personal data from state governments is ongoing and extends far beyond the SNAP program. In early May, ICE subpoenaed California's cash assistance program for low-income, elderly, or disabled legal immigrants who do not qualify for Social Security benefits. Then in June, officials at the Department of Health and Human Services shared highly sensitive data on millions of Medicaid recipients from California, Illinois, Washington, and D.C. with the Department of Homeland Security. And in July, the Centers for Medicare & Medicaid Services (CMS) gave ICE access to the personal information of nearly 80 million Medicaid recipients, including Social Security numbers and ethnicities. These data grabs are being used for immigration enforcement and are part of a broader effort to consolidate data government-wide, threatening the privacy and security of data about people across the country. The Trump administration is already taking rapid steps to combine its data assets — including those it obtains from states — for new use cases, including a searchable national citizenship database with the purported goal of allowing state and local elections officials to verify the citizenship status of voter lists. **Sources:** The Trump Administration is Making an Unprecedented Reach for Data Held by States, June 2025; The Trump Administration is Building a National Citizenship Data System, June 2025; ICE Is Getting Unprecedented Access to Medicaid Data, July 2025.

"Immediately upon execution of this order, Agency Heads shall take all necessary steps, to the maximum extent consistent with law**, to ensure the Federal Government has unfettered access to comprehensive data from all State programs that receive Federal funding,** including, as appropriate, data generated by those programs but maintained in third-party databases."

Source: Executive Order 14234—Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, March 2025.

Legal Protections for Federal Attempts to Access State Administrative Data

A number of long-standing legal protections must be considered to assess the legality of federal attempts to access state administrative data. Federal agencies must comply with the following legal requirements when they **request** state data:

- **The Privacy Act of 1974:** The Privacy Act requires federal agencies initiating a new data collection to publish a SORN, or a public notice, in the Federal Register identifying the purpose for which information about an individual is collected, from whom, what type of information is collected, and how that information will be shared with other agencies. **Source:** DOJ Overview on the Privacy Act, October 2022.

- **The Paperwork Reduction Act of 1980:** Under the Paperwork Reduction Act, federal agencies must conduct an independent review of any proposed collection of information and seek public comment on the proposed collection by publishing a 60-day notice in the Federal Register. **Source:** OPM Paperwork Reduction Act (PRA) Guide, April 2011.

- **The E-Government Act of 2002:** The E-Government Act of 2002 requires federal agencies to conduct a Privacy Impact Assessment (PIA) prior to initiating a new collection of information, which includes detailing what information will be collected, why it is being collected, and how the information will be collected, used, shared, and secured. **Source:** DOJ Overview of the E-Government Act, February 2019.

- **Core Constitutional Principles and the Right to Privacy:** A federal request for state data is subject to the U.S. Constitution, including key federalist principles (especially anti-commandeering and anti-coercion that guard against federal overreach in laying claim to states' resources and powers) and the individual right to privacy under the Fifth and 14th Amendments. That individual right to privacy is violated when the government wrongfully discloses information in which an individual has a "reasonable expectation of privacy" and the government lacks a "compelling governmental interest in disclosure [that] outweighs the individual's privacy interest." **Sources:** Data Federalism, February 2022; Payne v. Taslimi, 998 F.3d 648, 655–56 (4th Cir. 2021).

- **Program-Specific Enabling Statutes and Regulations:** Many of the United States' social programs are by design funded by the federal government, but administered by states. Typically, state-run programs that receive some federal funding are authorized by specific federal statutes. For example, the SNAP program was most recently authorized by the Food and Nutrition Act of 2008. A program's authorizing statute and associated regulations delineate the roles and responsibilities of federal and state actors in program administration, which can include information-sharing. **Source:** Food and Nutrition Act of 2008 (7 U.S.C. § 2011 et seq.).

Legal Protections for Federal Attempts to Access State Administrative Data (cont.)

States must consider the following legal requirements when they **provide access** to state data:

- **State Privacy Laws:** State privacy regimes vary. Twenty states have comprehensive privacy laws, such as the Virginia Consumer Data Protection Act. In addition, states may also have laws that govern specific categories of data, such as California's law on data collected by automatic license plate readers. Only a small portion of state privacy laws apply to government actors, as the majority focus on the private sector's data collection and management. **Sources:** Which States Have Consumer Data Privacy Laws?, April 2025; VA Code § 59.1-580; Calif. Veh. Code § 2413.

- **Sector-Specific Federal Privacy Protections:** States must also comply with applicable legal requirements under federal laws that govern the collection and use of specific types of data, such as personal health information in the case of the Health Insurance Portability and Accountability Act (HIPAA) or education records in the case of the Family Educational Rights and Privacy Act (FERPA). **Sources:** Summary of the HIPAA Privacy Rule, March 2025; Privacy Protection Under FERPA.

- **Program-Specific Federal and State Legal Requirements:** Both federal and state statutes and regulations that govern a program can contain specific requirements regarding handling and sharing of program data. For example, in the context of the SNAP program, federal law requires states to establish "safeguards which prohibit the use or disclosure" of SNAP recipient information for unauthorized purposes, and Massachusetts regulation restricts the use of SNAP applicant information to only "persons directly connected with the administration or enforcement of the Food Stamp Act" with limited exceptions. **Sources**: Food and Nutrition Act of 2008, 7 U.S.C. § 2020(e)(8); 106 C.M.R. 360.400(c).

- **State Contracts and Data Sharing Agreements (with both vendors and federal agencies):** States must also account for information-sharing provisions, especially in the context of joint federal-state programs, in any contracts they have entered into. These contracts typically fall into one of two categories: (1) data-sharing agreements between state and federal agencies, and (2) contracts between states and third-party vendors responsible for program data management or processing. These contracts are typically not publicly available, but frequently have provisions that have implications on whether and how a state or its vendors can comply with a federal data request. **Source:** Letter to Payment Processors, May 2025.

Impact of State Data Access and Use by the Federal Government

Recent efforts by the federal government to gain access to and use of an unprecedented range of sensitive state data without proper oversight or respect for transparency rules has broad and wide-ranging impacts on state governments and individuals across the country, including:

- **Expanded Access to Sensitive Information Fueling Mass Surveillance:** Administrative data collected from state agencies will significantly expand what the federal government knows about people present in the United States as states have data that are more extensive and sensitive than what the federal government alone holds. The federal government's access to state administrative data that includes information on residents' welfare use, immigration status, and health records could fuel mass surveillance and disproportionately affect marginalized groups such as non-citizens, families with lower incomes, or people with disabilities. **Source:** Immigration, DOGE, and Data Privacy, May 2025.

- **Chilling Effect on Public Services:** People may avoid accessing essential services, like health care or food assistance, that are made available by statutes if they fear their data could be used against them in contexts such as immigration enforcement, especially if safety net programs like SNAP, TANF, and housing assistance are turned into surveillance tools. This could deter lawful participation in public services, deepen poverty, and exacerbate housing and food insecurity. **Source:** Living in an Undocumented Immigrant Family Under the Second Trump Administration: Fear, Uncertainty, and Impacts on Health and Well-Being, May 2025.

- **Increased Risks of Large-Scale Algorithmic Profiling and Targeting:** Access to state data, together with data already held by federal agencies, could expand over time and be used for AI-driven surveillance and decision-making without individual or public knowledge or consent. With such access, the federal government could exploit state data for harmful practices such as algorithmic profiling, which has historically led to racial and socioeconomic discrimination. Like in China, compiling state data alongside federal data sources could be used for social scoring and to deny benefits or restrict behavior. **Sources:** DOGE's Growing Reach into Personal Data: What it Means for Human Rights, April, 2025; How China Is Using Big Data to Create a Social Credit Score, 2019.

- **Decreased Trust in Government:** Unless transparency and oversight requirements are respected, people will not know how their information, including data held by state agencies, is collected, processed, used, stored, or protected. This can result in information being shared or disclosed without individuals' explicit knowledge or consent and would prevent people from challenging inaccuracies or seeking redress if harm occurs. This in turn undermines democratic accountability and may lead to decreased trust in federal and state governments. **Source**: Understanding Government Transparency vs. National Security Confidentiality.

Impact of State Data Access and Use by the Federal Government (cont.)

- **Cybersecurity and Breach Risks:** Centralizing sensitive data, including from state databases, increases the risk of large-scale breaches. This puts the safety and security of both individuals' information as well as the sound and efficient functioning of state public services at risk, especially given that federal agencies notoriously struggle to protect information without appending tens of millions of records. **Source:** 75% of U.S. Government Websites Experienced Data Breaches, March 2025.

What To Look For Next

Should unprecedented data collection, consolidation, and analysis by the federal government continue, there will likely be implications for federal procedures governing data, technical changes to government data management, and increased privacy and civil liberties risks.

- **Potential Changes to Federal and State Data Norms and Technical Infrastructure:** Efforts to consolidate data across state and federal agencies signal a significant change in decades-long practices to securely store and share data between government agencies. As the federal government expands its efforts to access state data, this could institute longstanding changes to the underlying technical infrastructure of the federal government — like new methods of data transfer across government entities, additional data systems to house consolidated information, and fewer safeguards that limit data access. **Source:** DOGE Aims to Pool Federal Data, Putting Personal Information at Risk, May 2025.

- **Forthcoming Internal and External Documentation Updates:** As part of their effort to consolidate federal and state data, the Trump administration directed all federal agencies to catalogue and document all regulations governing unclassified data, including documentation requirements like SORNs, that pose "barrier(s) to the inter- or intra-agency sharing" of data. This could lead to significant changes in how federal agencies internally and externally document changes to their data practices. **Source:** Executive Order 14234—Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, March 2025.

What to Look for Next (cont.)

- **Increased Rhetoric Aligning Fraud, Waste, and Abuse with Immigration Enforcement:** While rates of beneficiary fraud in public benefits programs remain exceedingly low, the federal government is increasingly using claims of fraud, waste, and abuse to target information held by states for the purposes of immigration enforcement. As "anti-fraud" and immigration enforcement efforts become increasingly intertwined, this opens the potential for state data to be weaponized in new and expansive ways to target and further criminalize immigrant communities and surveil all of us. **Sources:** The Trump Administration is Making an Unprecedented Reach for Data Held by States, June 2025; Immigration, DOGE, and Data Privacy, May 2025.

- **Possible Targeting of Other High-Risk State Data Sources and Combination with Additional Government Data:** While initial reporting indicates that the federal government is seeking access to state SNAP and Medicaid data, these efforts are unlikely to stop here. Other high-risk state data sources like voter rolls, statistical information, arrest records, and child welfare information may also be targeted by federal agencies. Already, the Trump administration has requested copies of voter rolls from at least nine states. The Trump administration has also already begun efforts to aggregate federal data sources, and combining these highly sensitive state datasets with other governmental data could accelerate these efforts and further threaten the privacy and security of individuals' personal information. **Sources:** DOJ Demands Access to Minnesota's Voter Rolls, July 2025; DOGE Is Building a Master Database to Surveil and Track Immigrants, April 2025; Trump Taps Palantir to Compile Data on Americans, May 2025; DOJ Hits States with Broad Requests for Voter Rolls, Election Data, July 2025.

Questions? Contact civictech@cdt.org, techcenter@civilrights.org, or techanddata@protectdemocracy.org.