CENTER FOR DEMOCRACY & TECHNOLOGY

Vectors for Federal Access to Personal Data

From Data Brokers to State Administrative Data

Tom Bowman, *Policy Counsel, Security & Surveillance*
Maddy Dwyer, *Policy Analyst, Equity in Civic Technology*

April 30, 2026

About CDT

The **Center for Democracy & Technology** (CDT) is the leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. We shape technology policy, governance, and design with a focus on equity and democratic values. Established in 1994, CDT has been a trusted advocate for digital rights since the earliest days of the internet. The organization is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

Federal Access to Commercially-Available Information (CAI) through Data Brokers

01. Data Brokers and Commercially Available Information (CAI)

- Delete Act: "**Data Broker**" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Civ. Code § 1798.99.80(c)
- **Commercially Available Information (CAI)** refers to data sold, leased, or licensed to the general public or government entities, often sourced from data brokers, apps, or social media. It includes, but is not limited to, cell phone location, personal, financial, and consumer data.

Scale: global industry valued at over $280 billion in 2024, projected to exceed $500 billion by 2033. *Source:* https://www.grandviewresearch.com/industry-analysis/data-broker-market-report

CDT resource: Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers Shenkman, C., Franklin, S.B., Nojeim, G., and Thakur, D. (2021)

ODNI resource: Report to the Director of National Intelligence 27 January 2022

02. Data Broker Landscape

- **Global Giants:** like Acxiom, CoreLogic, Experian, Equifax, and Oracle, especially for financial information.
- **Specialized Firms:** that often focus on particular categories of data, especially for government and intelligence clients.
  - **Location Brokers** (e.g., Venntel, Babel Street): geolocation data
  - **Identity Brokers** (e.g., LexisNexis, Thomson Reuters): “public record” data
  - **Health Brokers** (e.g., Optum): “health risk” profiles (more for insurance companies)

Structured data is highly-organized, machine-readable data.
Unstructured data does not have a predefined format; it is messy.

The market is rapidly pivoting toward ***unstructured*** and ***custom-structured*** data, which could offer stronger signals unlocked through natural language processing and machine learning.

03. How Data Brokers Get Your Data

Data brokers act as the "middlemen" of the digital economy, operating a massive supply chain that feeds on three primary streams: **surreptitious harvesting** via Software Development Kits (SDKs) embedded in ordinary mobile apps (like weather or gaming tools), **automated leakage** from Real-Time Bidding (RTB) advertising auctions that broadcast your location and device ID thousands of times a day, and **mass aggregation** of public records, social media scraping, and commercial purchase histories.

Data supply chains: A data broker is unlikely to be the entity that initially collected the data that it makes available commercially. In fact, data may often pass through several different providers before it finds its way to a data broker. Data may be purchased for one purpose, but ultimately repurposed for another, making preserving legal protections and accountability difficult.

How AI can transform the data: Data brokers can use machine learning to combine fragments of your digital life into comprehensive profiles. AI identifies patterns across different datasets to reveal real-world identities (for example, linking a device ID to a specific home address).

04. How the Government Gets Your Data from Data Brokers

Government agencies obtain sensitive data by acting as commercial customers rather than legal authorities. They use **Commercial Off-the-Shelf (COTS)** contracts to purchase access to massive databases. This allows them to treat your personal information like office supplies or software subscriptions.

Agencies often hide these purchases under vague budget categories. They use terms like **Open Source Intelligence (OSINT)** or **"publicly available information"** to describe the data. These contracts frequently provide "all-you-can-eat" subscription access to global tracking tools. Law enforcement then integrates this commercial data into internal systems. This allows them to track individuals across different platforms without ever filing a single legal motion in court.

Data brokers themselves may not contract directly with federal agencies, but may provide databases through different vendors.

05. Data Broker Loophole

Two protections that generally restrict federal access to personal data:

- *Fourth Amendment*: generally requires a warrant supported by probable cause for law enforcement to obtain sensitive data that would otherwise be an invasion of a reasonable expectation of privacy (e.g., historical cell-site location data).
- *Electronic Communications Privacy Act of 1986 (ECPA) / Stored Communications Act (SCA)*: defines categories of electronic service providers and restricts their ability to disclose information to law enforcement absent a warrant or other legal process.

The "Data Broker Loophole" allows law enforcement to bypass the Fourth Amendment and ECPA by purchasing CAI that would otherwise require a warrant or other legal process.

06. How Often the Federal Goverment Exploits the Loophole

In March 2026, FBI Director Kash Patel told lawmakers during a congressional hearing that the DOJ is purchasing commercially available information that is then used in law enforcement operations.

Our best estimate is that the federal government spends **hundreds of millions (if not billions) of dollars annually** on purchasing data from data brokers. In 2021, CDT reported on 30 publicly-available awards that totalled **approximately $86 million dollars** across various federal agencies, which we believe is a **very small proportion of the total awards and total value**.

Closing the Data Broker Loophole

01. The Fourth Amendment Is Not For Sale Act (4ANFS)

The Road to Closing the Loophole

The 4ANFS was first introduced in 2021 by a **bipartisan coalition** (Sens. Wyden and Paul; Reps. Lofgren and Davidson). In April 2024, the House passed the Act (H.R. 4639) with a 219–199 vote, before it stalled in the Senate (after being narrowly defeated in a 212–212 vote during the 2024 FISA reauthorization).

States pick up the mantle: In 2025, Montana became the first state to pass a version of the 4ANFS (SB-282).

02. The Fourth Amendment Is Not For Sale Act (4ANFS)

Closing the Loophole

- **Expands covered entities** under the Stored Communications Act to include “intermediary service providers” (i.e., data brokers).
- **Adds a general prohibition** on law enforcement agencies and elements of intelligence community **purchasing covered records** and any “illegitimately obtained information” from any “third parties” (i.e., data brokers).
- **Introduces an exclusionary rule** that prohibits the use in court of any information (or evidence derived therefrom) obtained in violation of the statute.
- **Prohibits dissemination** of information obtained in violation of the statute to other federal agencies.

Federal Attempts to Access and Consolidate State-Level Administrative Data

01. What is Administrative Data?

Administrative Data is information collected by federal, state, local, tribal, or territorial governments used to administer programs and deliver services and benefits.

Administrative data **can include** sensitive, personal information that spans a variety of aspects of someone's identity and life (e.g., Social Security Number, employment history, address).

Information held by public agencies is often times **more sensitive** than what private companies have access to.

02. Past Attempts to Access State Administrative Data

Federal efforts to access sensitive state data, which has **historically been held and safeguarded at the state level**, have accelerated over the last decades. 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.

Such attempts continued under the first Trump administration, including:

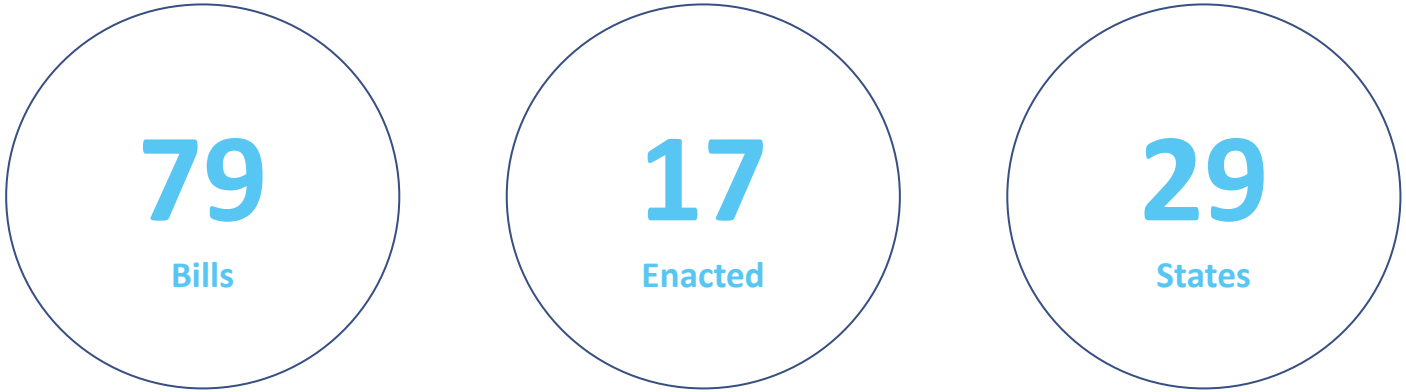
- Seeking voter registration data from every state under the Presidential Election Integrity (Pence-Kobach) Commission.
- Issuing an executive order that directed the U.S. Department of Commerce to seek State administrative records concerning citizenship in connection with the census.

03. Brief Overview of the Issue Since January 2025

- Following on the heels of DOGE's efforts to dramatically change how information is collected and shared at the federal level, the Trump administration expanded such efforts to include **state administrative data**.
    - This effort began in full on March 20, 2025, as President Trump signed an executive order directing federal agencies to gain access to data held by state programs that receive federal funding, including relevant data held by third-party vendors.
- From May to August 2025, the Administration has requested state **SNAP** data from USDA, gave ICE access to state **Medicaid** data via HHS, and issued a Notice of Proposed Rulemaking that would require states to provide sensitive **unemployment insurance** information to the federal government.
    - In the SNAP case, USDA sent a letter to all states demanding access to a host of sensitive information about beneficiaries including names, Social Security numbers, and addresses, and specified it was already taking steps to seek this information directly from SNAP payment processors.

04. State Legislative Efforts to Address the Issue

In the 2025 legislative session, 79 bills were introduced across 29 states, with 17 being enacted, that either **strengthen or weaken existing privacy protections** for administrative data, some which directly respond to the federal government's attempts to access state data.



05. Common Themes Across Bills Strengthening Protections

Across the bills introduced in states this session, several common topics emerged among bills aimed at **strengthening protections** for administrative data:

- Increasing **general privacy and cybersecurity protections** for information held by government agencies, including public benefits programs
  - Ex: New Mexico's SB 36
- Safeguarding **immigration-related information** by prohibiting voluntary sharing with federal immigration authorities and/or prohibiting the collection of such information
  - Ex: New York's SB 3657 and Connecticut's HB 7212
- Responding to **DOGE's threats** to government data privacy in states and across the federal government
  - Ex: Montana's H.Res. 3
- Protecting **education-related data** and instituting safeguards around data requests to schools
  - Ex: Nevada's AB 217 and Hawaii's SB 856

05. Common Themes Across Bills Strengthening Protections

- Safeguarding **disability-status information** from being shared with the federal government, particularly autism-related data
  - Ex. New York's AB 8716 and Nevada's AB 589
- Increasing privacy protections for **tax-related information** from being shared with unauthorized parties
  - Ex. New Jersey's SR 130
- Addressing **additional areas of concerns** related to public benefits data
  - California's SB 59 increases protections for **sexual orientation and gender identity data** by making court records related to name and/or gender marker changes confidential
  - New Jersey's AB 1905 would increase **public awareness** of immigration-related data privacy by launching a campaign about privacy laws that prevent the disclosure of health care enrollment information to immigration enforcement authorities

06. Five Policy Priorities for State Lawmakers

- **Data Governance**: Establishing baseline procedures and protections for the handling and oversight of personal data can mitigate privacy and security harms.
- **Data Minimization and Disclosure**: Limiting the amount of personal information collected and disclosed to only that which is necessary to achieve the intended purpose minimizes security risks and threats of misuse.
- **Notice, Access, and Correction:** Providing individuals with notice about when their information is used and the ability to access and correct their personal data increases public trust and transparency around government data practices.
- **Data Retention and Deletion:** Limiting the time period for which information is retained and using best practices to delete personal data reduces the overall amount of sensitive information held by the government.
- **Enforcement:** Creating strong enforcement mechanisms for government data privacy protections, including penalties for violating individuals' rights, holds bad actors accountable and prevents future harms.

Thank you!

Center for Democracy & Technology

Security & Surveillance, Equity in Civic Technology

Tom Bowman
Policy Counsel, Security & Surveillance

> *tbowman@cdt.org*

Maddy Dwyer
Policy Analyst, Equity in Civic Technology

> *mdwyer@cdt.org*

Find out more about CDT's work at *cdt.org*.

@cdt.org

Center for Democracy & Technology

techpolicy.social/@CenDemTech

@CenDemTech

CENTER FOR DEMOCRACY & TECHNOLOGY