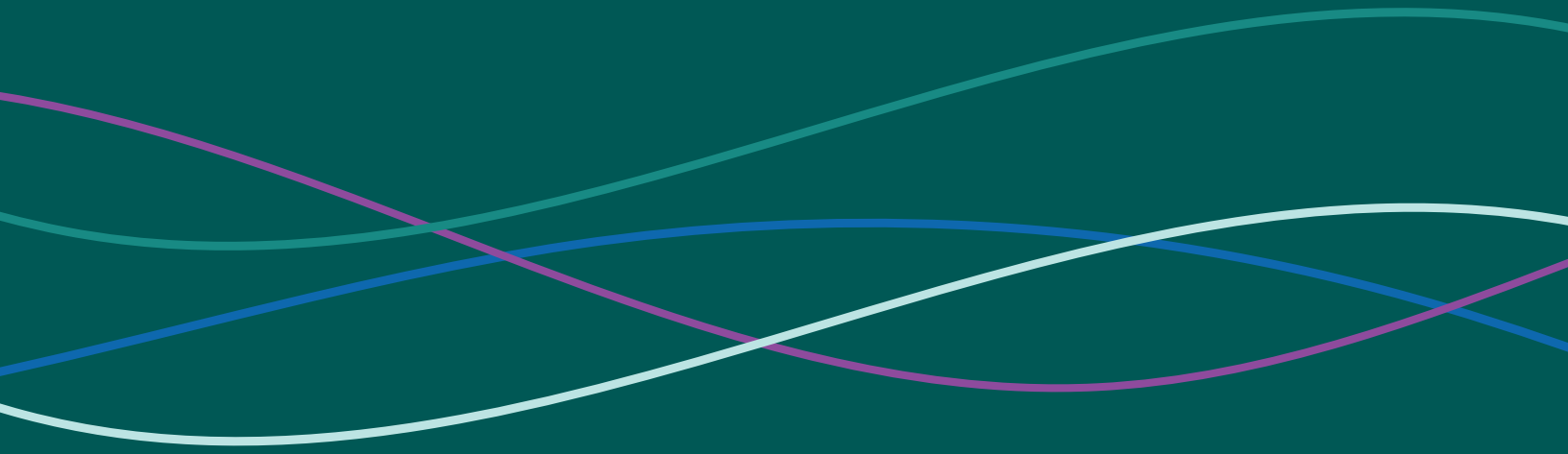
NEW AMERICA

OPEN TECHNOLOGY INSTITUTE



Data Matters

Power, Democracy, and Our Data One Year In

2025

A year into the current administration, it has become clearer than ever that we cannot separate questions about data from questions about power. Decisions about what information is collected, how it is interpreted, and who bears the consequences show up in everyday encounters with government, technology, and public institutions. Data moves through society—sometimes subtly, sometimes overtly—shaping the services people encounter, the risks they face, and the sense of security and agency they feel in daily life.

Over the past year, our work at the Open Technology Institute (OTI) treated data not merely as a technical input for policy, but also as a force that simultaneously shapes democracy and serves as a mirror that reveals society's values. Across different projects and issue areas, the same tensions kept resurfacing. Who has access? Who is exposed? Who gets to define what is true? What emerges is a picture of data as part of the architecture of public life—shaping not only how systems function but also how democracy is experienced.

Four threads run through the work:

01 Pushing Back on Surveillance and the Erosion of Public Trust

02 Shedding Light on the Power Dynamics of Data

03 Underscoring the Battle Over Evidence

04 Building A Better Future For Our Data in the Age of AI

01

Pushing Back on Surveillance and the Erosion of Public Trust

Surveillance expanded this year with little public debate or oversight. Government agencies and their contractors continue to collect massive amounts of personal information, often without clear limits on how it can be reused or combined with other systems. Early in 2024, we raised concerns about the Department of Homeland Security's use of data-driven systems, which can disproportionately impact communities already under heavy monitoring. The same dynamics showed up in the so-called Department of Government Efficiency's (DOGE) data practices, where mishandling sensitive information put millions of Americans at risk and demonstrated how weak governance turns surveillance into real harm. As we feared, these examples were early harbingers of continuing trends.

The effects are not always dramatic, but they are cumulative. When people are unsure how their information might be shared or repurposed, they adjust their behavior. They speak less freely. They hesitate before engaging with institutions. Over time, that hesitation develops into a mistrust that undergirds public life.

These effects are not evenly distributed. Communities that have long been disproportionately surveilled experience these risks more acutely, reinforcing existing gaps in who feels protected by democratic institutions and who does not.

Partnerships That Protect People by Strengthening Systems

Partnerships with organizations, including the National Institute for Reproductive Health (NIRH) and state agencies, helped OTI translate these principles into practice. This work focuses on how sensitive personal information moves through complex administrative systems and how to protect individuals at a collective level, not only through legal safeguards but also through better data practices.

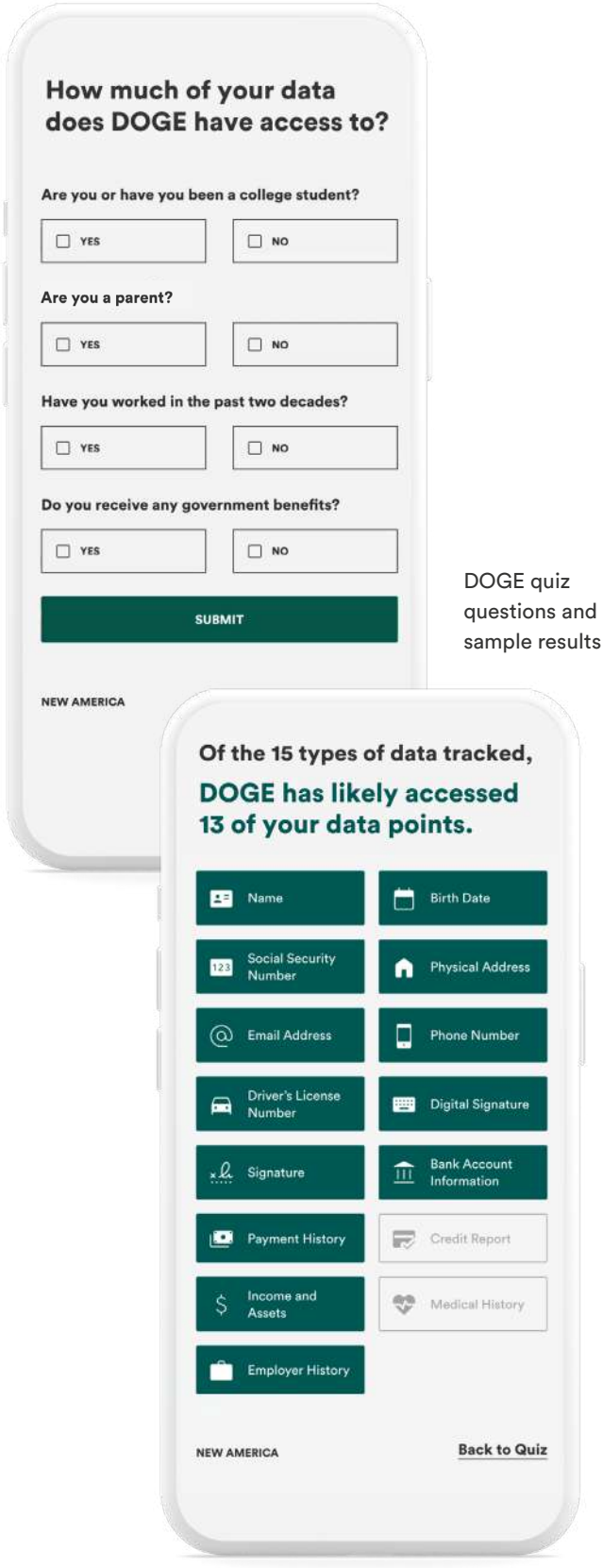
With NIRH, we will continue to focus on maternal mortality data and the barriers that make it difficult to see how reproductive restrictions affect care while helping partner organizations strengthen how they collect, store, and share sensitive information. Better data practices are not only a public health necessity; they allow families, providers, and policymakers to understand what is happening in real time and respond before harms deepen.

We also worked with a state agency confronting federal demands for expanded data access, helping them clarify and standardize processes to protect residents' information, uphold legal and ethical safeguards, and preserve public trust in state data systems. Our outputs included practical handouts for staff and more detailed guidance for long-term implementation designed to ensure that sensitive data is only used for its intended purpose.

Our work examining DOGE's data practices made these dynamics concrete. DOGE's handling of sensitive personal information placed millions of Americans at risk, revealing how easily bad data governance can translate into real harm. To make those risks easier to grasp, we built an interactive quiz that allowed people to see which parts of their own personal data could be exposed. More than 5,000 people took the quiz, and many shared their results publicly. What could have remained a narrow policy concern instead became a shared point of discussion about consent, accountability, and trust.

5,400+ Quiz Completions

Over 5,000 people explored their own data risk in real time, making it the top-performing piece of content at OTI.



DOGE quiz questions and sample results

We also examined the rapid proliferation of online age-verification requirements. While framed as child safety measures, many proposals would require users to submit government IDs or biometric data simply to access lawful content. These systems create new stores of sensitive personal information, introduce security risks, and can deter people from seeking information or participating in online spaces. Age verification expands the infrastructure of online monitoring in ways that are difficult to unwind once established, so it must be judiciously implemented at the right intervention points with technological architectures that ensure both safety *and* privacy.

02

Shedding Light on the Power Dynamics of Data

One reason harmful data practices persist is that they are difficult to recognize while they are happening. They sit inside technical systems, procurement decisions, and administrative processes that rarely invite public scrutiny.

Our work consistently found ways to make those systems easier to see. The response to the DOGE quiz underscored something we return to often.

Quick Engagement

It only took the average person 90 seconds to find out how the government misused their personal data.

People are more willing to engage when they can connect data practices to their own experiences. Seeing how a system touches your life changes the tone of the conversation. It becomes less abstract and harder to dismiss.

People are more willing to engage when they can connect data practices to their own experiences. Seeing how a system touches your life changes the tone of the conversation. It becomes less abstract and harder to dismiss.

Digital spaces also reveal the stakes for individuals. They can provide access, community, and resources, but they can also magnify offline harms: harassment, stalking, and gender-based abuse disproportionately affect women and gender minorities. Encryption has become a critical tool, safeguarding communication and sensitive information so people can seek care, report abuse, and organize safely. With reproductive care increasingly criminalized, personal data—like searches, GPS logs, and health app records—can be used as evidence against people seeking care. To address these risks, we've developed practical guidance for organizations and individuals, showing how protections like encryption can be applied in real-world contexts and how to navigate the complex tradeoffs between data use and privacy.

Zine for Real-World Impact

In collaboration with NIRH, we turned maternal health data safety into a digital zine—because "Don't Get Phished" practically demanded an illustration.

This kind of visibility matters because democratic oversight depends on more than formal transparency. Information can be public and still be inaccessible. When data governance remains opaque, accountability erodes. When people can understand what is happening and talk about it with others, pressure begins to build in more familiar ways.

03

Underscoring the Battle over Evidence

Alongside surveillance, we spent much of the year confronting a different problem—the growing use of data to distort, rather than clarify reality. Democratic decision-making depends upon a shared willingness to engage with evidence, even when it is inconvenient. That willingness is rapidly eroding.

In several policy areas, we saw efforts to selectively present statistics, suppress findings that complicate official narratives, or exaggerate uncertainty where evidence exists. We coined the term "data theater" to describe this practice, which reflects a deeper discomfort with evidence we're seeing in the United States. Data theater manipulates evidence to serve power instead of shared understanding, thus eroding the public's trust in institutional legitimacy.

ARGUMENT *An expert's point of view on a current event.*

When U.S. Data Lies, the World Listens

The Trump administration's manipulation of statistics is exporting uncertainty into the international system.

By Sydney Saubestre, a senior policy analyst at New America's Open Technology Institute, and Prem M. Trivedi, the director of New America's Open Technology Institute.

FOREIGN POLICY ILLUSTRATION/GETTY IMAGES

OTI's Sydney Saubestre and Prem Trivedi stress the consequences of "data theater" in *Foreign Policy*.

That tension over evidence also shaped our work on maternal mortality data. In a *Ms. Magazine* article, we examined how maternal mortality review committees have recently been delayed, defunded, or dissolved in several states. These committees are tasked with reviewing deaths that occur during pregnancy or within one year postpartum, and their goal is to lower the high U.S. maternal mortality rate. At the same time, gaps in federal reporting on reproductive health data make it difficult to see how federal and state policy changes are affecting care. Early warning signs are critical to identify and curtail emerging risks, but inconsistent reporting and political interference fragment the evidence needed for an effective response.

> **When the systems meant to document information are weakened or obstructed, harmful outcomes become harder to count, harder to understand, and harder to prevent.**

When the systems meant to document information are weakened or obstructed, harmful outcomes become harder to count, harder to understand, and harder to prevent. Over time, this narrows the range of acceptable debate and erodes accountability. Our work pushed back against these trends and insisted that evidence remains central to any meaningful democratic process.

Global Reach

We reached participants outside of the Washington, D.C. policy bubble; users came from across the United States and beyond.

04

Building a Better Future for Our Data in the Age of AI

Resisting harm is only part of the work. Throughout the year, we also focused on what responsible data governance can and should look like in practice.

We produced guidance to help governments share data in ways that support public outcomes while reducing privacy risks through privacy-enhancing technologies. This guidance was cited in a report on a bipartisan approach to modernizing the Privacy Act of 1974 prepared by Representative Lori Trahan's office. We also published a blueprintfor how data can move among agencies and other stakeholders without sacrificing oversight or public trust. Additionally, we shared guidance with state agencies on how to best protect their residents' data. These efforts were grounded in the same concerns that shaped our work on data weaponization but applied toward building systems that work better, rather than simply exposing those that do not.

Policy in Action

Analysts nationwide referenced OTI's privacy-enhancing technology guide while drafting new government data policies. In fact, staff reported keeping our guidance open in a browser tab while working on real-world government policies.

This approach also shaped how we engaged with artificial intelligence. In practice, AI governance begins long before a system is deployed. Decisions about what data is collected, whose experiences are represented, and how information is structured shape outcomes in ways that are difficult to reverse later, especially when that data is being used to power AI. Already, we are seeing AI introduced into institutions that matter deeply for democratic life, including universities and federal agencies, even while safeguards are removed.

To unpack the importance of what are often treated as technocratic issues, we examined how new technical developments impact transparency, privacy, and power. We paired that analysis with more practical guidance—including recommendations to universities on AI adoption—that preserves student and educator agency.

Across these efforts, our work supports a shift away from collecting data first and managing risk later. Rapid advances in AI make it more essential than ever to design systems with clear limits on data use, meaningful stakeholder input, and accountability from the outset. The choices institutions make today about data are inseparable from how AI will function tomorrow—shaping who benefits, who is overlooked, and whether institutions can correct course when necessary.

The choices institutions make today about data are inseparable from how AI will function tomorrow—shaping who benefits, who is overlooked, and whether institutions can correct course when necessary.

Where This Leaves Us

Taken together, these threads point to a simple reality. Data has become one of the main ways power operates in modern democracy. It can be used quietly, through systems that feel distant from everyday life, or openly, through policies that reshape who is protected, who is served, and who is not.

One year into the current presidency, the direction is still being set. The choices being made now about data will shape public life long after individual policies fade from view. Our work this year focused on making those choices easier to see, harder to abuse, and more firmly grounded in the public interest.

Explore our work
newamerica.org/open-technology-institute