Why people don’t demand data privacy – even as governments and corporations collect more personal information

Rohan Grover, Assistant Professor of AI and Media, American University

Published: November 5, 2025 8:27am EDT

People feeling that their data is being collected at every turn leaves many numb to the issue of data privacy.

J Studios/DigitalVision via Getty Images

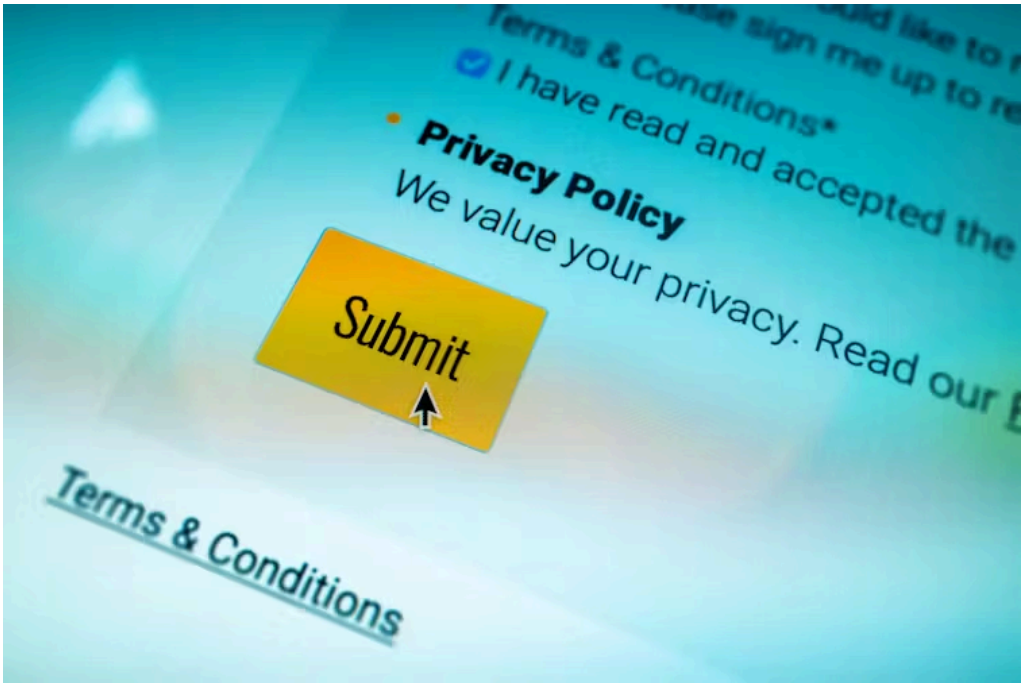
When the Trump administration gave Immigration and Customs Enforcement access to a massive database of information about Medicaid recipients in June 2025, privacy and medical justice advocates sounded the alarm. They warned that the move could trigger all kinds of public health and human rights harms.

But most people likely shrugged and moved on with their day. Why is that? It’s not that people don’t care. According to a 2023 Pew Research Center survey, 81% of American adults said they were concerned about how companies use their data, and 71% said they were concerned about how the government uses their data.

At the same time, though, 61% expressed skepticism that anything they do makes much difference. This is because people have come to expect that their data will be captured, shared and misused by state and corporate entities alike. For example, many people are now accustomed to instinctively hitting “accept” on terms of service agreements, privacy policies and cookie banners regardless of what the policies actually say.

At the same time, data breaches have become a regular occurrence, and private digital conversations exposing everything from infidelity to military attacks have become the stuff of public scrutiny. The cumulative effect is that people are loath to change their behaviors to better protect their data − not because they don’t care, but because they’ve been conditioned to think that they can’t make a difference.

As scholars of data, technology and culture, we find that when people are made to feel as if data collection and abuse are inevitable, they are more likely to accept it – even if it jeopardizes their safety or basic rights.



How often do you give your consent to have your data collected?

Sean Gladwell/Moment via Getty Images

Where regulation falls short

Policy reforms could help to change this perception, but they haven’t yet. In contrast to a growing number of countries that have comprehensive data protection or privacy laws, the United States offers only a patchwork of policies covering the issue.

At the federal level, the most comprehensive data privacy laws are nearly 40 years old. The Privacy Act of 1974, passed in the wake of federal wiretapping in the Watergate and the Counterintelligence Program scandals, limited how federal agencies collected and shared data. At the time government surveillance was unexpected and unpopular.

But it also left open a number of exceptions – including for law enforcement – and did not affect private companies. These gaps mean that data collected by private companies can end up in the hands of the government, and there is no good regulation protecting people from this loophole.

The Electronic Communications Privacy Act of 1986 extended protections against telephone wire tapping to include electronic communications, which included services such as email. But the law did not account for the possibility that most digital data would one day be stored on cloud servers.

Since 2018, 19 U.S. states have passed data privacy laws that limit companies' data collection activities and enshrine new privacy rights for individuals. However, many of these laws also include exceptions for law enforcement access.

These laws predominantly take a consent-based approach – think of the pesky banner beckoning you to "accept all cookies" – that encourages you to give up your personal information even when it's not necessary. These laws put the onus on individuals to protect their privacy, rather than simply barring companies from collecting certain kinds of information from their customers.

The privacy paradox

For years, studies have shown that people claim to care about privacy but do not take steps to actively protect it. Researchers call this the privacy paradox. It shows up when people use products that track them in invasive ways, or when they consent to data collection, even when they could opt out. The privacy paradox often elicits appeals to transparency: If only people knew that they had a choice, or how the data would be used, or how the technology works, they would opt out.

But this logic downplays the fact that options for limiting data collection are often intentionally designed to be convoluted, confusing and inconvenient, and they can leave users feeling discouraged about making these choices, as communication scholars Nora Draper and Joseph Turow have shown. This suggests that the discrepancy between users' opinions on data privacy and their actions is hardly a contradiction at all. When people are conditioned to feel helpless, nudging them into different decisions isn't likely to be as effective as tackling what makes them feel helpless in the first place.

U.S. adults' attitudes about data privacy

Americans have high levels of concern about data privacy – but also high levels of resignation, according to a 2023 survey.

Chart: The Conversation CC-BY-ND • Source: Pew Research Center • Get the data • Embed • Download image • Created with Datawrapper

Resisting data disaffection

The experience of feeling helpless in the face of data collection is a condition we call data disaffection. Disaffection is not the same as apathy. It is not a lack of feeling but rather an unfeeling – an intentional numbness. People manifest this numbness to sustain themselves in the face of seemingly inevitable datafication, the process of turning human behavior into data by monitoring and measuring it.

It is similar to how people choose to avoid the news, disengage from politics or ignore the effects of climate change. They turn away because data collection makes them feel overwhelmed and anxious – not because they don't care.

Taking data disaffection into consideration, digital privacy is a cultural issue – not an individual responsibility – and one that cannot be addressed with personal choice and consent. To be clear, comprehensive data privacy law and changing behavior are both important. But storytelling can also play a powerful role in shaping how people think and feel about the world around them.

We believe that a change in popular narratives about privacy could go a long way toward changing people's behavior around their data. Talk of "the end of privacy" helps create the world the phrase describes. Philosopher of language J.L. Austin called those sorts of expressions performative utterances. This kind of language confirms that data collection, surveillance and abuse are inevitable so that people feel like they have no choice

Cultural institutions have a role to play here, too. Narratives reinforcing the idea of data collection as being inevitable come not only from tech companies' PR machines but also mass media and entertainment, including journalists. The regular cadence of stories about the federal government accessing personal data, with no mention of recourse or justice, contributes to the sense of helplessness.

Alternatively, it's possible to tell stories that highlight the alarming growth of digital surveillance and frame data governance practices as controversial and political rather than innocuous and technocratic. The way stories are told affects people's capacity to act on the information that the stories convey. It shapes people's expectations and demands of the world around them.

The ICE-Medicaid data-sharing agreement is hardly the last threat to data privacy. But the way people talk and feel about it can make it easier – or more difficult – to ignore data abuses the next time around.

The authors do not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and have disclosed no relevant affiliations beyond their academic appointment.