Free Press Action

What Happens to Our Data Online Is a Civil-Rights Issue

A Free Press Action Guide

Internet use is essential to full participation in modern society. Even the most careful internet users have their personal data circulating in the hands of social-media companies, internet service providers, government agencies and others. This guide explains what happens to our data when we go online and examines the civil-rights issues this presents.

I. What's really happening with our data?

No matter how innocuous it may appear in isolation, everything we do online generates data — and private companies and governments can track and use every bit of that data. Corporate privacy policies are cumbersome to opt out of and are not designed to minimize the data companies gather and store about us. Rather, these policies act as our consent form so companies can collect untold amounts of information about us, including our browsing histories, our locations, our social-media profiles, our biometric data and inferences other platforms make about our identities. Companies create specific online profiles about each of us, feeding powerful algorithms and other machine-learning tools to deliver hyper-personalized content, easier shopping experiences, accurate rideshare pickup locations and tailored streaming entertainment suggestions.

II. Who has access to our data?

Many different kinds of companies have access to our data. Platforms like Google and TikTok and even companies like Target or your local coffee shop maintain websites and other digital services, like mobile apps, which gather information about us. And it's not just private companies like social-media platforms that have access to our data. Government agencies are also buying up personal information from private data brokers that profit from collecting as much about people as possible, which allows governments to engage in mass surveillance *without* a warrant.

III. The ability to gather & use our data can lead to discrimination.

Surveillance advertising can feel efficient — even beneficial. Some people, understandably, aren't worried about tailored ads for the shoes they recently searched for. But other consequences flow from data collected and analyzed about us when companies exclude specific users from the same information and opportunities as others, resulting in discriminatory outcomes.

An algorithm widely used in U.S. hospitals to allocate health care to patients systematically discriminated against Black people, who were less likely than their equally sick white counterparts to be referred to hospitals. Meta settled a lawsuit with the Department of Justice regarding its housing advertising scheme, which resulted in Black users seeing fewer or no ads for affected housing on Facebook. And during the 2020 elections, Black, Indigenous and Latinx users were subjected to sophisticated microtargeting efforts based on data collected about them — and targeted with deceptive content on social media about the voting process. These are just a few examples of discrimination flowing from data that companies collected about users.

IV. Solutions:

Companies won't simply stop gathering or selling our data — their business models are built on these practices. And governments have been getting around constitutional requirements that they secure warrants before surveilling us.

One powerful way to disrupt use of our data to surveil and discriminate is to limit the amount of data these companies can collect and store. Private companies should collect less data about us, retain information for shorter periods of time, and limit sales they otherwise make to third parties and government entities. Lawmakers should advance policies — such as civil-rights protections around our data privacy — to give us control of our data. How Tech Companies & Policymakers Can Safeguard Digital Civil Rights offers more detailed solutions. Another great resource is our Disinfo Defense League Policy Platform.