

<u>After Dobbs</u>, Warrantless Purchase of Data Threatens People Seeking Reproductive Healthcare

Consumer Data Contains Highly Sensitive Information; Buying It Sidesteps Constitutional Protections

In *Dobbs*, the Supreme Court overruled *Roe v. Wade* and opened the door to restricting abortion rights, leading to a sharp spike in Google searches for "abortion" and related terms. Beginning in July, searches for "abortion near me" <u>dropped below pre-Dobbs</u> levels and have remained low as people avoid leaving a digital paper trail in their search for reproductive healthcare.

By exploiting gaps in privacy laws, state and federal agencies can gather information that would otherwise require a court order to obtain, including data on racial and ethnic identity, political affiliation, sexual orientation, medical information, location, internet activity, and more. Agencies can even Parenthood, threatening our civil liberties and endangering the most vulnerable among us.

As the <u>Congressional Research Service found</u>, "federal data privacy law provides relatively limited constraints upon law enforcement's ability to acquire privacy data relating to criminal activity, potentially including abortion activity proscribed under the state laws of the requesting law enforcement agency."

Government Purchase of Data Threatens Constitutional Protections:

- <u>Law enforcement regularly buys information that would otherwise require a court order to obtain.</u>

 Purchasing private data without a warrant deliberately circumvents Fourth Amendment protections.
- Purchased data can be used to identify and target individuals based on their First Amendment protected activities, which is exacerbated by several states' enactment of financial bounties for private actors.
- Information on religious communities and political parties is available to anyone, including law enforcement, (e.g. a US military contractor purchased data from a Muslim prayer app)

Government Purchase of Data Poses Acute Dangers to Vulnerable Populations

- Data purchases are a harmful tool that <u>anti-abortion activists are already using</u>. Access to sensitive information, <u>including locations that can identify protected classes</u>, is a critical threat as citizens are encouraged to track and report suspected abortions, <u>even where legally obtained in another state</u>.
- For abortion-seekers, queer people, parents seeking gender-affirming care for their children, and others, privacy can be lifesaving. Increased state surveillance through bought data endangers vulnerable groups.

Abortion Bans Enforced by Purchased Data Criminalize Marginalized Peoples

- <u>Purchased data can track someone's location to an abortion clinic</u> or a pharmacy, identify people as abortion advocates, or connect an abortion seeker to the support network that helped them obtain care.
- Purchased data is a warrantless way to disproportionately target Black and poor persons for surveillance and criminalization. Poor people and people of color particularly Black people are less likely to have adequate access to care and resources they need to prevent pregnancy. They are more likely to need and seek abortion care, and therefore more likely to be impacted by this practice.
- Online resources are essential for navigating the intricacies of states' laws and accessing reproductive healthcare. Fears about government access to internet activity and location records are causing painful chilling effects for people who need reproductive healthcare and those who provide it.