FOR LEGISLATORS

USER ERROR: REPRODUCTIVE HEALTH, RIGHTS, & JUSTICE

BY KAIROS ACTION. IN COLLABORATION WITH STATE INNOVATION EXCHANGE

KAIROS

SiX
STATE INNOVATION EXCHANGE

ACKNOWLEDGMENTS

Our deepest appreciation to the researchers and organizers who contributed their expertise to this report, including Cynthia Conti-Cook of Surveillance Resistance Lab; and the State Innovation Exchange (SiX) Reproductive Rights team and SiX State Directors.

DEFINITIONS USED IN THIS DOCUMENT

Big Tech: Umbrella term for the companies that make tech — hardware and software — and have an outsized impact on technology development, the internet, and the economy as a whole. Big Tech often refers to Meta, Microsoft, Google, Apple, and Amazon.

BACKGROUND

People seeking abortion care, abortion clinics and providers, and people who help facilitate abortion care, such as abortion funds and practical support networks, are being surveilled by both state agencies and private actors. The corporations that govern our digital spaces act as a significant, largely unregulated arm for these surveillance systems, constantly collecting and sharing intimate data about our behaviors, movements, and communications that are easily weaponized. And while some medical information that flows through Big Tech is protected by expanded HIPAA protections, anti-abortion lawmakers are already suing to remove those safeguards.

Big Tech companies and data brokers have supplied anti-abortion groups and law enforcement agencies with the information they need to surveil, criminalize, stalk, doxx, and harass abortion seekers or anyone connected to them. These companies have:

- Collected personal information and communications including private Facebook messages and shared them with law enforcement in states that have criminalized abortion.
- Sold location data of people visiting reproductive healthcare clinics to anyone willing to pay.
- Platformed dangerous disinformation on social media and in paid search results and ads.

POLICY EXAMPLES

In states where abortion care remains legal, protections have not been restricted and abortion seekers travel to these states , protection must go beyond enshrining abortion rights in legislation or state constitutions. It is also important to conduct comprehensive auditing to show how data sharing weakens state protections through the use of commercial database systems (license plate readers, electronic health record marketplaces, Clearview AI, etc.) and interjurisdictional agreements. Without these reviews, laws focused on one data type or use remain vulnerable to being undermined.

The following policy examples target multiple aspects of data protection so that people can be protected before they begin an online search and beyond.

In Massachusetts, the Location Shield Act (2023 MA HB 357/SB 148) was introduced to protect people who need to cross state lines to access reproductive care. The act prohibits companies from selling cell phone location data, making it harder to prosecute users based on their digital data trail.

Legislation enacted in Nevada (2023 NV SB 370) and Washington (2023 WA HB 1155) creates new requirements for collecting, selling, and using consumer health data, including prohibiting the sale of health data without the consumer's authorization. These 2023 laws, as well as bills introduced in states such as Hawaii (2024 HI SB 2696) and Vermont (2024 VT SB 173), also prohibit the use of a "geofence" to identify individuals who cross the virtual boundary of a targeted location, such as a reproductive or sexual health facility.

In California, Assemblymember Bauer-Kahan's law (2022 CA AB 1242) bars California-based tech companies from complying with any out-of-state warrants related to abortion. A bill in Massachusetts (2024 MA SB 2770) would prevent Big Tech companies from sharing "data processed concerning an individual's sexual orientation, sex life or reproductive health, including, but not limited to, the use or purchase of contraceptives, birth control, abortifacients or other medication, [and] products or services related to reproductive health," including geolocation information and biometric data.

Legislation passed in Illinois (2024 IL HB 5239) prohibits the state from providing any information, including through a FOIA request, or using resources to assist any out-of-state civil or criminal investigation of a lawful healthcare activity. Colorado passed a shield law (SB23-188) that protects people who travel to the state for abortion or gender-affirming care and people who assist such patients from lawsuits and criminal prosecution initiated in other states.

A bill in Hawaii (2023 HI SB 1503) would prohibit county police departments from cooperating with or providing information related to "any investigations concerning abortion-related conduct, gender-affirming treatments, or other reproductive health care or services that are lawful in the State, including any subpoenas or search warrants issued by another state."

A law in Maryland (2023 MD HB 812) is the first in the country to shift the burden of protecting health information from healthcare providers to health information exchanges and electronic health record systems. It prohibits the transfer of protected health information that has been coded as abortion care (procedural or medication).

POLICY RECOMMENDATIONS

Policy solutions like the above are steps toward creating a world where people can maintain bodily autonomy and seek abortion care without fear of being tracked, surveilled, and prosecuted. More states need policies that protect their constituents' digital data from being collected and sold without clear consent or opting in — including medical records and other health data, location data, search history data, and messages.

While policies aimed at protecting data privacy are of the utmost importance for individuals, solutions must also regulate companies that harm abortion seekers and prohibit law enforcement overreach. This could look like:

- Requiring companies to provide users with opt-in mechanisms for data collection option, instead of an opt-out process, and to never condition users' access based on them opting on.
- Mandating transparency from Big Tech companies regarding what data they are currently collecting and sharing.
- Mandating data minimization and data deletion policies to prevent companies from maintaining forever archives, ensuring the minimum amount of data is collected and stored for the minimum amount of time needed to deliver a service, and that data is not shared, sold, or used beyond its original purpose.
- Requiring platforms to make it easy for users to flag online disinformation about established health and safety facts and state policies for removal, including when it applies to reproductive care.
- Ensure that laws that shield abortion providers from out-of-state investigations are broad enough to prevent the disclosure of digital records of people supporting access to abortion care.
- Prohibiting geofencing and limiting companies from collecting, sharing, selling, and using geolocation and other information related to reproductive healthcare access.

ADDITIONAL RESOURCES

User Error: The Internet Post-Roe (Kairos): This report outlines the ways that Google and Meta (formerly Facebook) have aided and abetted the restriction of abortion access to people seeking care, and provides a framework for organizers to fight back against Big Tech.

Tools for Taking on Big Tech's Economic Power (American Economic Liberties Project): The threats posed to reproductive rights by heightened surveillance and criminalization are directly connected to tech corporations' unchecked greed and power. Monopolistic Big Tech corporations constantly surveil consumer data and will easily cooperate with states that enforce draconian anti-abortion laws, which disproportionately target historically criminalized communities: Blacks, immigrants, women, queer people, and people experiencing poverty. Our partners at American Economic Liberties Project have released a toolkit for state legislators to tackle many of these challenges with solutions already proposed in states across the country.

The Threat of Mobile Driver's Licenses (Surveillance Resistance Lab): For years, the Department of Homeland Security (DHS) and U.S. Immigration and Customs Enforcement (ICE) have used information from state Department of Motor Vehicles (DMV) databases to identify, track, and detain and deport noncitizens, immigrant justice activists, and others. The threat is even more severe as states and corporations move quickly to implement mobile driver's licenses (mDLs) across the country. In a post-Roe world, those seeking abortion care are also directly threatened, as mobile driver's licenses can be used for tracking and monitoring by governments and corporations, and allow law enforcement to easily seize cell phones during routine traffic stops. Similarly, transgender individuals with updated gender markers on their driver's licenses are under threat. Our partners at the Surveillance Resistance Lab break down the risks of mDLs, highlighting the dangers for individuals and policymakers.

Privacy First: A Better Way to Address Online Harms (Electronic Frontier Foundation): The truth is that many of the ills of today's internet have a single thing in common: they are built on a system of corporate surveillance. Multiple companies, large and small, collect data about where we go, what we do, what we read, who we communicate with, and so on. They use this data in multiple ways and, if it suits their business model, will sell it to anyone who wants it — including law enforcement. Addressing this shared reality will better allow us to promote human rights and civil liberties, while simultaneously holding space for free expression, creativity, and innovation, than many of the issue-specific bills we've seen over the past decade. In other words, whatever online harms we want to alleviate, we can do it better, with a broader impact, if we look at privacy first.