The Harms of Data Abuse After *Roe*:

Why Washington needs meaningful, enforceable protections.

The U.S. does not have a comprehensive data privacy law that requires transparency and accountability for how companies can use an individual's data. As a result, people have little insight into and even less control over how their information is collected, used, shared and sold. There is serious harm caused by data abuse that is heightened in a post-Roe world. Many states are moving rapidly to criminalize abortion care and jeopardize access to needed health care services. In this new landscape, data shared between companies, private parties, and the government could be used to target and harass individuals who seek or access reproductive health care.

These are just a few examples of the types of data that companies are exploiting and the many individuals and communities who may face harm as a result in a post-*Roe* United States.

Abortion patients: According to a 2016 Rewire article, geolocation data was used to target visitors to 140 abortion clinics with ads for anti-abortion pregnancy counseling services. In May 2022, *Motherboard* revealed that SafeGraph, a location data broker, sold the aggregated location data of people who visited abortion clinics, including more than 600 Planned Parenthoods over a one week period for just $160. The data showed where patients traveled from, how much time they spent at the healthcare centers, and where they went afterwards. The data collected by the company includes an analysis of where people appear to live, based on where their cell phones are commonly located overnight. Those who obtain abortions should not be subjected to targeted ads about their private health care decisions and people should not have their locations tracked and shared via geotargeting when seeking health care.

Cell phone users: According to a 2019 Vice Motherboard investigation, AT&T, T-Mobile, and Sprint have all sold customers' locations and personally identifying information to third-party companies, with the information eventually falling into the hands of bail bonds firms and bounty hunters. Providers of cell phone service, which is an essential utility in modern-day society, should not be allowed to share their customers' identities and real-time location with shady third-party companies. Cell phone information was also critical in the prosecution of a woman who experienced a pregnancy loss after searching online for medication abortion information. In our new reality, where abortion is criminalized, cell phone data could be used to target, threaten, and prosecute those seeking health care.

Social media and messaging app users: A teenager and her mother were indicted in the summer of 2022 in Nebraska. The mother's charges included violating the state's law banning abortion. In investigating the case, law enforcement obtained information from the daughter's social media messaging app. According to Forbes, Meta, the parent company of Facebook, Instagram, and Messenger, shared the information with law enforcement in response to a judicial warrant that did not mention abortion. People who use social media and messaging apps can find themselves at risk when companies are allowed to retain and access private conversations between individuals.

Emergency room patients: Patients waiting for emergency room medical care in Philadelphia were targeted with ads for personal injury lawyers, according to a 2018 NPR article. Given that those seeking emergency medical care are often frightened and in pain, they should not be pushed into making weighty decisions while awaiting care for their injuries. In an environment where miscarriage could result in a criminal investigation, geolocation data could carry risks that go far beyond unwanted advertising.

Menstrual cycle tracking app users: Even though users' location is not needed to use the app, individuals who use the MyDays cycle tracking app are continually having their location tracked, according to a January 2021 Norwegian Consumer Council report. Their location and personal information is then shared with a company that markets users' personal life details like "User has arrived at a clinic" or "User might be unfit to drive due to sleep deprivation" to insurance companies and others. In 2021, Flo Health, one of the most popular period tracking apps, settled with the FTC over allegations that it shared health information on its 100 million users with third-party data analytics firms.

M. Lorena González, *Legislative Director* | mlgozalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington

People trying to achieve or avoid pregnancy should not fear that insurance companies may use their information to discriminate against them.

The Supreme Court's ruling also opens the door to potential future restrictions on other rights and freedoms such as same-sex marriage, interracial marriage, same-sex intimate relationships, and contraception.

Dating app users: People who use dating apps are encouraged to be extremely forthcoming with intimate details about their lives in order to be matched with the most compatible romantic prospect. Apps then take advantage of this trove of sensitive information by sharing it with other companies. A January 2021 Norwegian Consumer Council report found that OKCupid was sharing users' location and information about their sexual desires, alcohol use, political views, and ethnicity with third parties, while Tinder was sharing users' location, age, gender, and partner preferences.

LGBTQIA2S+ dating app users: In 2018, Buzzfeed discovered that the Grindr LGBTQIA2S+ dating app was sharing its users' HIV status and personally identifying information with third parties. Though users have a true interest in knowing the HIV status of their potential partners, one user noted that he stopped sharing his HIV status on the app, explaining that indiscriminate sharing of that information "can put people in danger, and it feels like an invasion of privacy."

M. Lorena González, *Legislative Director* | mlgozalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington