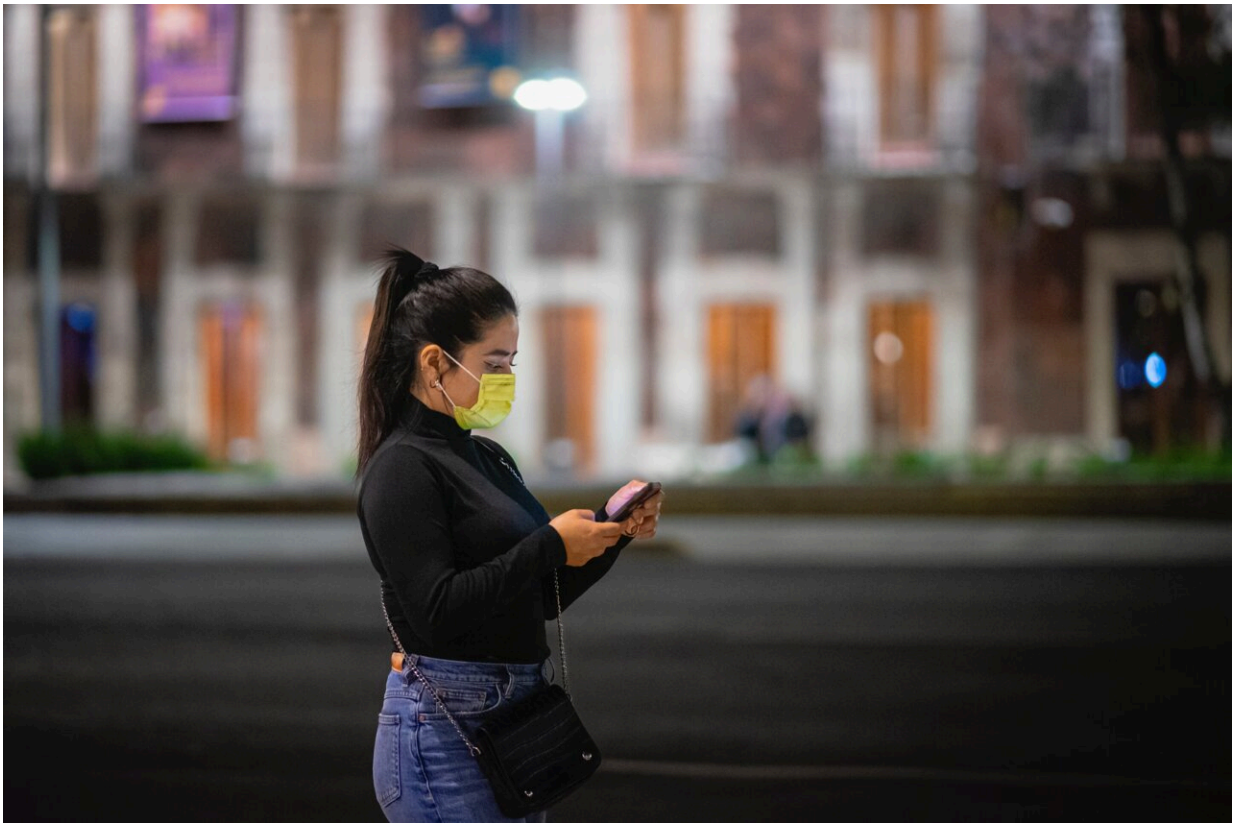
The importance of protecting privacy in a post-Roe world

August 10 2022, by Dee Patel



Credit: Unsplash/CC0 Public Domain

After the U.S. Supreme Court's controversial decision in June 2022 to overturn Roe v. Wade and eliminate an almost 50-year federal right to abortion, data privacy advocates are sounding the alarm about the

potential dangers of authorities weaponing digital data from prospective health care patients.

The potential harm isn't theoretical, says Jessa Lingel, an associate professor at the Annenberg School for Communication. In less than two months, nearly half of the states have or will pass laws that ban abortion while others have enacted strict measures regulating the procedure. Everyday apps such as GPS, text messages, location tracking services, web search histories, and other data fragments could be used against people in the U.S.

"Smartphones have become powerful communication tools and important sources of connection and entertainment, but they also have the capacity for incredible amounts of surveillance," she says. "Even before Roe was overturned, tech companies were under fire for failing to protect access to abortions, for example, Siri failing to find nearby abortion clinics or Google Maps directing people to anti-choice clinics when searching for Planned Parenthood."

Advocates against intimate partner violence have long pointed to smartphones as a tool for monitoring and controlling a partner's movements, explains Lingel.

"Now that abortion is criminalized in huge parts of the country, the stakes around surveillance and reproductive health are even higher," she says. "Google has said it will delete location history for visits to reproductive health centers, but it's risky to put our faith in Big Tech to protect privacy. And that's not even getting into cases like Texas, where the law has essentially encouraged anti-choice activists to surveil their friends, coworkers, and neighbors who seek out reproductive care."

To what extent individual state law enforcement agencies may adopt such tactics to enforce anti-abortion statues is still unclear. However,

Lingel advises not waiting to find out.

"Big Tech has shown again and again that they will choose monetizing user data over protecting individual privacy, and the federal government has been reluctant to offer serious regulation," she says. "So if people want to keep their information private, especially when it comes to reproductive care, the time to learn the basics of online privacy is now. Some of my favorite resources are the Our Data Bodies project, the Tech Learning Collective, and the Electronic Frontier Foundation."

According to Lingel, users should learn and familiarize themselves with using encrypted communications. Experts recommend that patients buy a phone and phone number that is not associated with their identity. Once they purchase that device, they should check the privacy settings of programs such as menstruation-tracking apps and turn off advertising identifiers on a personal device. Lingel says there is a lot people can do to control what information they are providing to tech companies.

"Taking control of our online data is largely about shifting habits," she says. "Install anti-tracking plug-ins and apps on your devices, use encrypted texting, like Signal, and emailing, like Protonmail. Use VPNs to protect your search history. Turn off location tracking for your phone, and go through each of your social media platforms and familiarize yourself with the different privacy options. These are small steps that take a few minutes to learn and install, and can really provide a great deal more privacy. They also build more literacy in terms of how platforms operate and what our individual rights are."

Another way to protect one's privacy is to use a pre-paid credit card whenever possible, in order to avoid exposing any payment data.

"The absolute worst way to pay for things is with apps like Venmo or Zelle," Lingel cautions. "These apps leave a digital trail that's easy to

follow, and these companies haven't really been tested yet in terms of protecting user privacy when it comes to things like pushing back on subpoenas. It's important to remember that it's not just state and local governments you have to worry about; in cases where someone is trying to get an abortion against the wishes of an abusive partner, credit card statements can be a dangerous source of evidence."

Data about a user's location, demographics are collected as a matter of course by mobile apps—often by way of mundane tasks like buying groceries or getting driving directions.

"If you keep your location tracking on at all times and if you don't use private web browsers, your phone not only knows where you've been, it knows where you're going," Lingel says. "For over a decade, researchers have been able to use smartphone data to predict people's movements, often doing so with accuracy within a few feet. Of course, there are positive sides to this—being able to find a missing child or an elderly person with dementia. But the negative implications are also clear and pretty terrifying."

In addition, the data broker industry scours the web for personal data, and repackages it and sells it to other organizations. Recently, Vice News was able to buy data—for about $160—showing where people who visited Planned Parenthood came from and where they went afterwards.

"Data brokers are the companies that buy and sell user data, the middlemen between social media companies and advertisers," Lingel says. "Some people don't mind data gathering and targeted ads, while others find them creepy and intrusive. But what's at stake here is the question of how this data can be used unfairly. It has been used to discriminate against people of color in the housing market, sometimes called digital redlining. The technology clearly exists to gather personal data in order to market products in ways that can discriminate."

Lingel explains that with digital redlining, there was a clear government agency that could step in and regulate: the Department of Housing and Urban Development. But it's not clear what the counterpart is to protect people's personal information around reproductive health.

"It's important to remember that searches and location data are not protected under HIPAA," she says. "We've seen over and over again how easy it is to reidentify personal information that is allegedly anonymous."

Provided by University of Pennsylvania