Post Roe, women in America are right to be concerned about digital surveillance. And it's not just period-tracking apps

28 June 2022, by Uri Gal

Credit: Shutterstock

The reversal of Roe v. Wade by the American Supreme court last week is a watershed moment in American politics. The ruling withdraws constitutional protections for abortion rights and sends the issue to the states, around half of which are expected to ban abortions.

Unlike the last time abortion was illegal in the United States, almost half a century ago, we now live in an era of pervasive digital surveillance enabled by the internet and mobile phones. Digital data may well be used to identify, track, and incriminate women who seek abortion.

Over the past 20 years or so, large tech companies, mobile app operators, data brokers, and online ad companies have built a comprehensive system to collect, analyze, and share huge amounts of data. Companies can follow our every movement, profile our behavior, and snoop on our emotions.

Until now, this system has mostly been used to sell us things. But following last week's ruling, many are concerned that personal data could be used to surveil pregnancies, shared with law enforcement agencies, or sold to vigilantes.

Data everywhere

There are various sources of data that could be used to identify, track, and prosecute women who are suspected of seeking an abortion.

Google routinely shares private user information with law enforcement agencies, even without a warrant. This includes search terms, which could be used as evidence by law enforcement agencies investigating or prosecuting abortion-related cases.

Online surveillance can also include location data. American police already use location data from mobile devices to collect evidence against suspected criminals.

What's more, many mobile apps track your location and share it with data brokers. The brokers then sell the data on to a myriad of unknown third parties, including law enforcement agencies. This happens even when people have opted out of location data collection.

The same technology could be used to track women's movements, and report when they went near an abortion facility or traveled to a different state where abortions are legal.

Social media

Social media activity, and data collected by social media platforms, can also be used to infer whether someone may be pregnant or is interested in getting an abortion.

A recent investigation showed hundreds of "crisis pregnancy centers"—quasi-health care clinics that aim to dissuade women from having

abortions—around the U.S. shared website visitor information with Facebook. In some cases, this revealed people's names and addresses, as well as whether a woman was considering an abortion.

The investigation also showed anti-abortion organizations were able to get access to some of this information. If abortion is made a crime, this information could be used against women in legal proceedings.

Period trackers

Data from fertility and health apps could also be used to identify and track women who are suspected of seeking abortion. These apps record highly private information including menstruation cycles, sexual activity, and hormonal treatments.

However, many of these apps share unencrypted sensitive information with data brokers and ad companies without users' knowledge or consent.

With the end of institutional protections for abortions, many worry that data from such applications could be used as evidence against women in legal proceedings.

A unique moment for democracies

Following last week's ruling, there have been calls for women to delete fertility and period tracking apps, switch off location tracking on their phones, or even use "burner phones".

However, such piecemeal individual efforts are likely to be ineffective or impractical. The digital surveillance apparatus is too vast for us to effectively evade it.

Billions of webpages contain trackers that collect detailed data. More than 6.5 billion phones globally can be easily repurposed as sophisticated surveillance tools. It is becoming increasingly difficult to avoid the gaze of cameras whose images can be stored in biometric databases and algorithmically identified and analyzed.

What is worse, these data are collected, stored, and traded in ways we don't understand very well, with only minimal rules and regulations.

Privacy advocates and researchers have been warning us for years of the destructive potential of the digital surveillance apparatus.

Critics have often noted how this system could bolster and embolden totalitarian regimes, such as in China. Surveillance in Western countries, like the U.S., has been seen as less of a problem because it was focused on commerce.

The overturning of Roe v. Wade is an era-defining moment because of its significance for women's reproductive rights. It may also define the era in another way: we may see the existing digital surveillance system routinely used to criminalize individual citizens.

Not too late for better privacy rules

Much of the existing legislation is out of step with current technologies and in need of reform, not only in the U.S. but also in Australia.

What would new rules look like? To rein in digital surveillance, they would

- strictly limit the collection, storage, sharing, and recombination of digital data
- tightly regulate the use of facial recognition technologies
- require digital platforms, websites, and mobile apps to provide users with easy and genuine non-tracking options, and
- require companies to offer true end-to-end encryption to protect user data.

We are on the cusp of an era where digital surveillance is used at scale against ordinary citizens. Huge changes are required, not only to protect women's reproductive choice but also to protect everybody's privacy and freedom from undue surveillance.

Provided by The Conversation