Should you delete your period-tracking apps? A look at data privacy post-Roe

September 9 2022, by Lisa Marshall

Credit: University of Colorado at Boulder

In the wake of the Supreme Court's decision to eliminate the constitutional right to an abortion in the U.S., the White House, the Federal Trade Commission and President Biden himself have warned women to be wary of online platforms that collect personal data—especially about reproductive health.

The concern: That law enforcement agencies or private citizens could use things like data from period-tracking apps, Google searches for abortion clinics or medications, social media posts or location information as evidence of a crime in places where abortion is illegal.

CU Boulder Today caught up with Margot Kaminski, an associate professor at Colorado Law who specializes in data privacy, to discuss how our personal data can be used, what's at stake now that Roe v. Wade has been overturned, and how we can protect ourselves.

What new data privacy concerns have arisen due to the fall of Roe v. Wade?

If a state ends up criminalizing abortion, there's a wide range of surveillance techniques that can be used by local law enforcement to identify somebody who is either considering having an abortion, has had an abortion or has provided an abortion. We don't have a general federal data privacy law in the U.S. so, with the exception of some state laws and wiretapping laws, almost anything that you do online related to your health is not protected. That lack of protection has serious implications. You can imagine a local law enforcement agency deciding to surveil a vast amount of intimate, sexual health-related information about women.

How might a private citizen or law enforcement agency get that personal data?

A lot of times, companies surveil ordinary behavior online, including your search engine requests, your use of apps or your location, and bundle that information and sell it. For example, in 2020, the Federal Communications Commission arrived at a $200 million settlement with several mobile phone companies that had been taking their customers'

location data and bundling it up and selling it, including to local law enforcement, without any real privacy protections.

Is it legal for companies to do that?

Generally, yes. The Fourth Amendment of the U.S. Constitution protects against government searches and seizures but not surveillance by a private party. A company that gathers location information and sells it voluntarily to law enforcement isn't stopped by the Fourth Amendment. Some states—including Colorado—have started enacting data privacy laws that can impede (though usually do not completely stop) that kind of behavior, by for example allowing individuals to opt out of the sale of their personal data. As the example of the FCC settlement shows, in some contexts like telecommunications law, there are government regulators who might place restrictions on particular activities or actors.

What about location tracking on our phones? Should women be worried about that, especially if they are in the vicinity of an abortion clinic?

Yes. And there are unfortunately not a lot of ways to get around it. Women should be really cautious about relying on privacy self-help strategies. It may be that they've turned off everything they can on their phone and the app, etc., and their mobile phone providers or browsers or broadband providers are still tracking where they are.

How are you supposed to protect yourself?

With unfortunately great difficulty. An individual can, for example, use a search engine like DuckDuckGo, which doesn't store your search history. Or she can make sure that when she's at home, she's using a virtual private network, or VPN, whenever she's browsing the internet.

That will prevent her information from being gathered by some of these big tech intermediaries and potentially sold down the road. The issue is that many people are not that technologically sophisticated. People don't think about the fact that every different website that you go to is obtaining more information about you.

Should women delete their period-tracking apps?

Some of these apps have a notoriously bad track record around privacy, including selling poorly anonymized information to employers. It is hard to imagine that when faced with demands from law enforcement and no law telling them not to, period-tracking apps won't turn over highly personal information. California is trying to address this: A law currently on Gov. Newsom's desk would make it illegal for tech companies based in California to turn over information in an out-of-state abortion investigation.

What else can be done?

Colorado and California and a number of other states have been enacting these big data privacy laws that actually do give consumers significantly more protections in the online environment. The issue is that these laws are only protecting the residents of certain states and, so far, they are largely blue states whose residents are not going to be dealing with lawsuits about abortions. Second, these laws don't address law enforcement. They may cut off some of that spigot of the flow of consumer data from private organizations to the general world, but they're not going to prevent law enforcement from 100 other ways of trying to obtain that data via various technologies.

If you could offer one key takeaway, what would it be?

Data privacy is something that seems incredibly abstract to most people. But when you have a government that now has the capability to touch some of the most intimate areas of people's lives, then suddenly data privacy becomes extraordinarily important.

Provided by University of Colorado at Boulder