Online data could be used against people seeking abortions if Roe v. Wade falls

May 17 2022, by Nora McDonald

Credit: Unsplash/CC0 Public Domain

When the draft of a Supreme Court decision that would overturn Roe v. Wade was leaked to the press, many of us who have been studying privacy for vulnerable individuals came to a troubling realization: The marginalized and vulnerable populations whose online risks have been the subject of our attention are likely to grow exponentially. These groups are poised to encompass all women of child-bearing age,

regardless of how secure and how privileged they may have imagined themselves to be.

In overturning Roe, the anticipated decision would not merely deprive women of reproductive control and physical agency as a matter of constitutional law, but it would also change their relationship with the online world. Anyone in a state where abortion becomes illegal who relies on the internet for information, products and services related to reproductive health would be subject to online policing.

As a researcher who studies online privacy, I've known for some time how Google, social media and internet data generally can be used for surveillance by law enforcement to cast digital dragnets. Women would be at risk not just from what they reveal about their reproductive status on social media, but also by data from their health applications, which could incriminate them if it were subpoenaed.

Who is tracked and how

People who are most vulnerable to online privacy encroachment and to the use or abuse of their data have traditionally been those society deems less worthy of protection: people without means, power or social standing. Surveillance directed at marginalized people reflects not only a lack of interest in protecting them, but also a presumption that, by virtue of their social identity, they are more likely to commit crimes or to transgress in ways that might justify preemptive policing.

Many marginalized people happen to be women, including low-income mothers, for whom the mere act of applying for public assistance can subject them to presumptions of criminal intent. These presumptions are often used to justify invasions of their privacy. Now, with anti-abortion legislation sweeping Republican-controlled states and poised to go into effect if the Supreme Court overturns Roe v. Wade, all women of

reproductive age in those states are likely to be subject to those same presumptions.

Before, women had to worry only that Target or Amazon might learn of their pregnancies. Based on what's already known about privacy incursions by law enforcement against marginalized people, it's likely that in a post-Roe world women will be more squarely in the crosshairs of digital forensics. For example, law enforcement agencies routinely use forensic tools to search people's cellphones when investigating a wide range of crimes, sometimes without a search warrant.

Imagine a scenario in which a co-worker or neighbor reports someone to the authorities, which gives law enforcement officials grounds to pursue digital evidence. That evidence could include, for example, internet searches about abortion providers and period app data showing missed periods.

The risk is especially acute in places that foster bounty-hunting. In a state like Texas where there is a potential for citizens to have standing to sue people who help others access abortion services, everything you say or do in any context becomes relevant because there's no probable cause hurdle to accessing your data.

Outside of that case, it's difficult to do full justice to all the risks because context matters, and different combinations of circumstances can conspire to elevate harms. Here are risks to keep in mind:

- Sharing information about your pregnancy on social media.
- Internet search behavior related directly or indirectly to your pregnancy or reproductive health, regardless of the search engine you use.
- Location tracking via your phone, for example showing that you visited a place that could be linked to your reproductive health.

- Using apps that reveal relevant sensitive data, like your menstrual cycle.
- Being overconfident in using encryption or anonymous tools.

Heeding alarms

Scholars, including my colleagues and me, have been raising alarms for years, arguing that surveillance activities and lack of privacy threatening those most vulnerable are ultimately a threat to all. That's because the number of people at risk can rise when political forces identify a broader population as posing threats justifying surveillance.

The lack of action on privacy vulnerability is due in part to a failure of imagination, which frequently blinkers people who see their own position as largely safe in a social and political system.

There is, however, another reason for inattention. When considering mainstream privacy obligations and requirements, the privacy and security community has, for decades, been caught up in a debate about whether people really care about their privacy in practice, even if they value it in principle.

I'd argue that the privacy paradox—the belief that people are less motivated to protect their privacy than they claim to be—remains conventional wisdom today. This view diverts attention from taking action, including giving people tools to fully evaluate their risks. The privacy paradox is arguably more a commentary on how little people understand the implications of what's been called surveillance capitalism or feel empowered to defend against it.

With the general public cast as indifferent, it is easy to assume that people generally don't want or need protection, and that all groups are at equal risk. Neither is true.

All in it together?

It's hard to talk about silver linings, but as these online risks spread to a broader population, the importance of online safety will become a mainstream concern. Online safety includes being careful about digital footprints and using anonymous browsers.

Maybe the general population, at least in states that are poised to trigger or validate abortion bans, will come to recognize that Google data can be incriminating.

Provided by The Conversation