

What you need to know about surveillance and reproductive rights in a post Roe v Wade world

July 6 2022, by Julia Slupska and Laura Shipp



Credit: Dids . from Pexels



After the <u>overturning of Roe v Wade</u> in the U.S., tracking reproductive information has never been riskier. In many U.S. states, millions seeking and providing abortions could soon face criminal charges. <u>Online</u> <u>conversations</u> have turned to digital self-defense, and questions about the privacy of period tracking apps and other digital traces.

This concern is justified. Gender and racial justice researcher Cynthia Conti-Cook has documented the use of <u>digital evidence</u> to prosecute people accused of seeking abortions in the U.S. So far, this has been used in multiple cases against <u>women of color</u> who already face significant barriers in <u>reproductive health care</u>.

Abortion tracking is likely to fit into other forms of criminalization and surveillance marginalized communities face. This includes surveillance of low-income people seeking welfare, and the use of racially biased data-driven policing.

Law enforcement could gain access to intimate data by extracting it from phones during a criminal investigation. Some may even purchase data from "data brokers" which acquire and sell personal information without court oversight. And subpoenas may require companies that store data to share it. Some companies are already starting to respond to these fears—Google announced recently that it will delete location history data for users who visit abortion care providers.

We research digital <u>privacy</u> and <u>security</u> from a <u>feminist perspective</u>. If you are wondering how to protect yourself and your data, here are a few things to consider.

Period trackers

Millions of people use period tracking apps to better understand their menstrual cycle, or to help them avoid or get pregnant. There is fear that



cycle histories could become evidence that someone has had an abortion. This is because apps can chart early signs of pregnancy or common side-effects of a miscarriage or abortion, if a user enters these.

There is good reason to be wary of these apps, but everyone should make decisions about whether to keep or delete their app on the basis of their own circumstances (for example, where you live and how much criminalization risk you face). There are some useful things to know about these apps when you're considering what to do.

Companies collect and store a lot of data. Many store cycle <u>data</u>, often in large, anonymised data sets, in order to generate new products, complete research, make inferences about their users, or <u>sell to third parties</u>.

Although most companies promise not to share this data with authorities, they might not be able to keep this promise. Digital service providers are obliged to follow the laws of the countries where they operate, and may have to comply with subpoenas from <u>law enforcement</u>.

Without laws in the U.S. enshrining the <u>right to be forgotten</u>, deleting apps that could hold "incriminating" reproductive information is not enough, as data remains stored on servers. Deleting data often requires email contact with those companies—although this is yet another digital paper trail, it can sometimes be the only way to make sure data is fully deleted. Be particularly wary of companies that don't have information on this in their privacy policies.

Generally speaking, if you do use period trackers, make sure you're using a privacy-first app such as <u>drip</u>, <u>Read Your Body</u> or <u>Pow!</u>. These do not collect any of your data on their servers, only store your cycle history on your phone and allow you to delete data easily. For these apps, simply uninstalling them does delete all your cycle data.



Defending yourself online

Digital privacy has long been a feminist issue. Privacy tools are already important for women experiencing <u>technology-enabled intimate partner violence</u> or <u>online harassment</u>. Now that we know data about our <u>sexual and intimate lives</u> is being collected and could be used for new purposes, we need these tools more than ever.

Resources developed by feminist and digital rights collectives, such as the <u>DIY Guide to Feminist Cybersecurity</u> and the <u>Holistic Security</u> <u>Guide</u> are useful tools that provide digital security guidance for protecting yourself on the internet. If you become familiar with privacy-first messengers such as Signal, or secure browsing options such as VPNs now, you won't need to learn about them suddenly when you or someone close to you is in crisis.

People in the U.S. who need abortions will now increasingly depend on networks of abortion funds which help people access and pay for abortion care. As both care seekers and providers are at high risk of surveillance and criminalization, the role of digital security will be critical in protecting these organizations.

Security guidance from digital privacy advocates <u>DCRYPTD</u> and the <u>Electronic Frontier Foundation</u> provide advice specifically for reproductive care seekers and providers.

Organizations such as <u>Chayn</u> and <u>Glitch</u> have led the way in developing resources on online safety and digital self-care. <u>Reconfigure</u>, a project we collaborated on, ran community workshops on feminist digital privacy and security. These initiatives provide not only resources for personal self-defense, but also models for how we can all invest in community support as a way to keep each other safe.



A key consequence of the Roe v Wade ruling is that the <u>constitutional</u> <u>right to privacy</u> now seems under threat. The U.S. needs better data protection laws, including a federal equivalent of the EU's General Data Protection Regulation (GDPR) to make it harder to sell personal data, and easier for people to delete their own data. But no amount of <u>digital</u> <u>privacy</u> regulation or self-defense guidelines will remove the enormous risks and harms of reproductive health care being criminalized.

Post-Roe abortion restrictions are just one piece of a decades-long puzzle of anti-choice campaigning and attempts to control people's bodies. This has been particularly acute for disabled people and people of color, through forced sterilization and people being criminalized for having miscarriages. Reproductive justice therefore involves not just digital defense, but the defense of the right to bodily autonomy for all.

This article is republished from <u>The Conversation</u> under a Creative Commons license. Read the <u>original article</u>.

Provided by The Conversation

Citation: What you need to know about surveillance and reproductive rights in a post Roe v Wade world (2022, July 6) retrieved 5 May 2024 from https://techxplore.com/news/2022-07-surveillance-reproductive-rights-roe-wade.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.