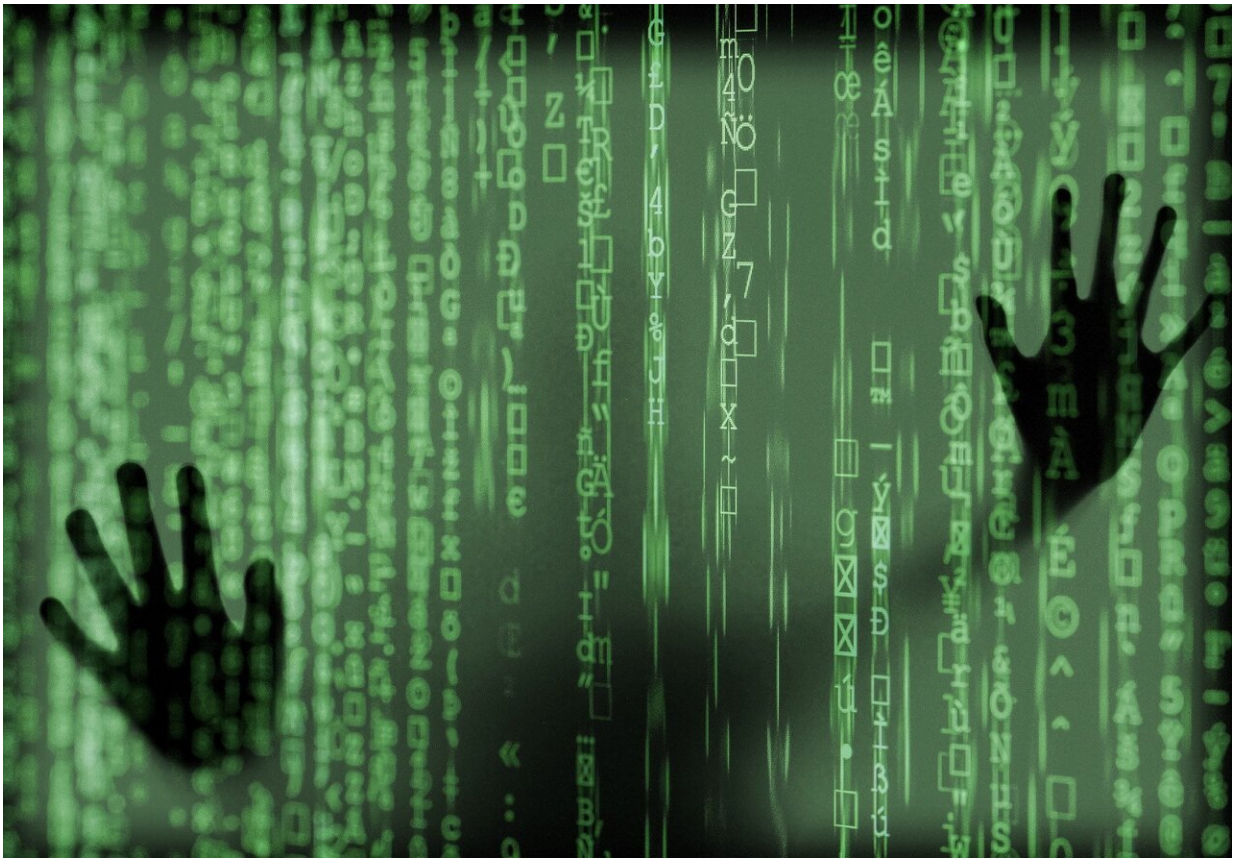
Navigating data privacy in a post-Roe world

July 18 2022, by Melissa de Witte



Credit: CC0 Public Domain

The end of Roe v. Wade—a woman's constitutional right to an abortion—has led some digital privacy experts, including Stanford's Riana Pfefferkorn, to ask what could happen to women seeking reproductive healthcare in a world where their online behavior can be

used against them.

With little regulation about how websites and apps can gather data about their users, coupled with a legal system that allows authorities to access that information (sometimes without even a warrant), the end of Roe illustrates how the seemingly mundane digital tools people use every day can turn sinister, said Pfefferkorn, a research scholar at the Stanford Internet Observatory, a cross-disciplinary program that studies the abuse of the internet and provides policy and technical solutions.

Here, Pfefferkorn talks about the importance of digital privacy and why the federal government must do more to protect it, especially now in a post-Roe v. Wade world.

In a post-Roe v. Wade world, why is data privacy an important issue right now?

In the United States, we don't have a comprehensive legal framework at the federal level for protecting people's data privacy. Legislators are playing catch-up after years of light regulation regarding how our digital data can be collected, stored, used, and disclosed by private entities.

That makes data privacy important post-Roe for two reasons. One, with the right legal process, law enforcement can go to private entities that hold digital data about us and request it from them. For example, with a warrant, the police can get your email, your browser history, or your search history on a search engine. And sometimes they don't need legal process at all—law enforcement can buy data about people from data brokers just like any other customer, circumventing the need for a warrant. Two, entities that are hostile to abortion rights can gather information about abortion seekers and then use it for purposes that are not in that person's interest. For example, crisis pregnancy centers trick

people searching for abortion information into visiting their websites and providing information about themselves, and they are savvy users of online tracking and advertising technologies.

For these reasons, we're seeing tech companies and pro-choice legislators scrambling to figure out how to protect people's online privacy when it comes to abortion.

Some people might argue that they have nothing to hide or fear about being surveilled digitally. What would you say to make people care about the issues at stake?

Privacy is for everybody because everyone has something to hide. You might not need to hide it today, but you might need to hide it next year. The end of Roe provides a stark illustration of how once-innocuous digital surveillance can turn sinister with a shift in the political winds. Something that was a constitutional right for half a century just became a crime in a large swath of the country. Protecting our digital privacy today is a way of trying to "future proof" ourselves against what might happen tomorrow.

Even outside the context of criminalization, all of us have aspects of our lives that are simply nobody else's business. They're not illegal, they're not bad or wrong, they're just private. We deserve protection for those things too. People need privacy in order to be fully human. We need privacy for our thoughts, for our conversations, for our intimate relationships. It shouldn't be as hard as it is to keep our private lives and thoughts and needs from being leveraged by someone else, whether that's for commercial purposes, law enforcement purposes, or malicious or illegal purposes.

We need actual laws to protect our digital privacy, instead of expecting 330 million Americans to do it themselves, do it perfectly, and do it against all those parts of the online data-gathering ecosystem that they may not even know exist.

What do you make of President Biden's recent executive order to protect data privacy and patient information?

The executive order (EO) is a good start, although it necessarily leaves the details up to others. The EO inherently recognizes how difficult it will be for Congress to pass anything—whether that's abortion-related legislation, such as codifying Roe, or legislation about online and/or offline privacy more generally.

The EO also respects the subject-matter competence of federal agencies, getting them to think creatively (which I'm sure they already were) about how to leverage their regulatory power. The EO identifies the agencies most relevant to the fight to preserve abortion access and reproductive privacy at the federal level, such as the Department of Health and Human Services and the Federal Trade Commission, as well as agencies that will be crucial to helping specific populations—for example, servicemembers and their families, who don't really have a lot of control over what state they are stationed in.

Do you think the EO goes far enough? What other protections ought to be put in place to protect privacy?

The EO could certainly go further. I wrote in a recent op-ed for The Hill that we are going to see state investigators seeking the federal

government's help with digital evidence collection from the phones of people suspected of seeking, having, or performing an abortion. The federal government has a lot more resources than state and local law enforcement agencies do, so there are existing federal/state partnerships in place to share access to those resources, provide training, and so on. I think it's imperative for the federal government to refuse to let federal resources (equipment, technology, personnel, etc.) be used to prosecute people for state crimes relating to abortion.

In the meantime, what can people do to manage their online data and minimize their digital footprint?

The Biden EO has a link to HHS guidance on protecting your health information. Beyond that, I would suggest using an end-to-end encrypted messaging app such as Signal to protect your private conversations from eavesdroppers. Turn on disappearing messages so that your chats disappear after a particular time period. Check out privacy-oriented web browsers like Tor or Firefox Focus, and install extensions to block ads and stymie online trackers (such as AdBlock and Privacy Badger). If you don't want your search queries logged, try DuckDuckGo, or, if you'd rather stick with your current search engine, change its settings to stop saving your search history (but be aware your searches will still be logged in a way that could be traced back to you). Do a privacy and security check-up of the services that you use (such as your search engine or maps app) and select the most data-minimizing options. Review the access privileges that the apps on your phone have: you might find some surprises. Look over what's backing up to the cloud, too: is there app data (such as your messaging conversations) that you'd rather not back up?

And what about tech companies and the people that work for them?

Review what data you collect and store, for how long you store it, how securely you store it, whether it's kept in a way that can reasonably be linked back to a specific user, and, most importantly, why. Why are you collecting specific types of data in the first place? Do you really need to collect it at all, or in a way that's identifiable to the user, or for so long? Can you expunge what you've already collected? It was heartening to see Google's announcement that it will start promptly deleting users' location history around sensitive places such as abortion clinics, for example. More like that, please.

I would also caution tech companies to tighten up internal access controls for people's data. There's a long and sordid history of employees at tech companies abusing their data access privileges for malicious purposes. I think we can expect to see that in the abortion context too.

Provided by Stanford University