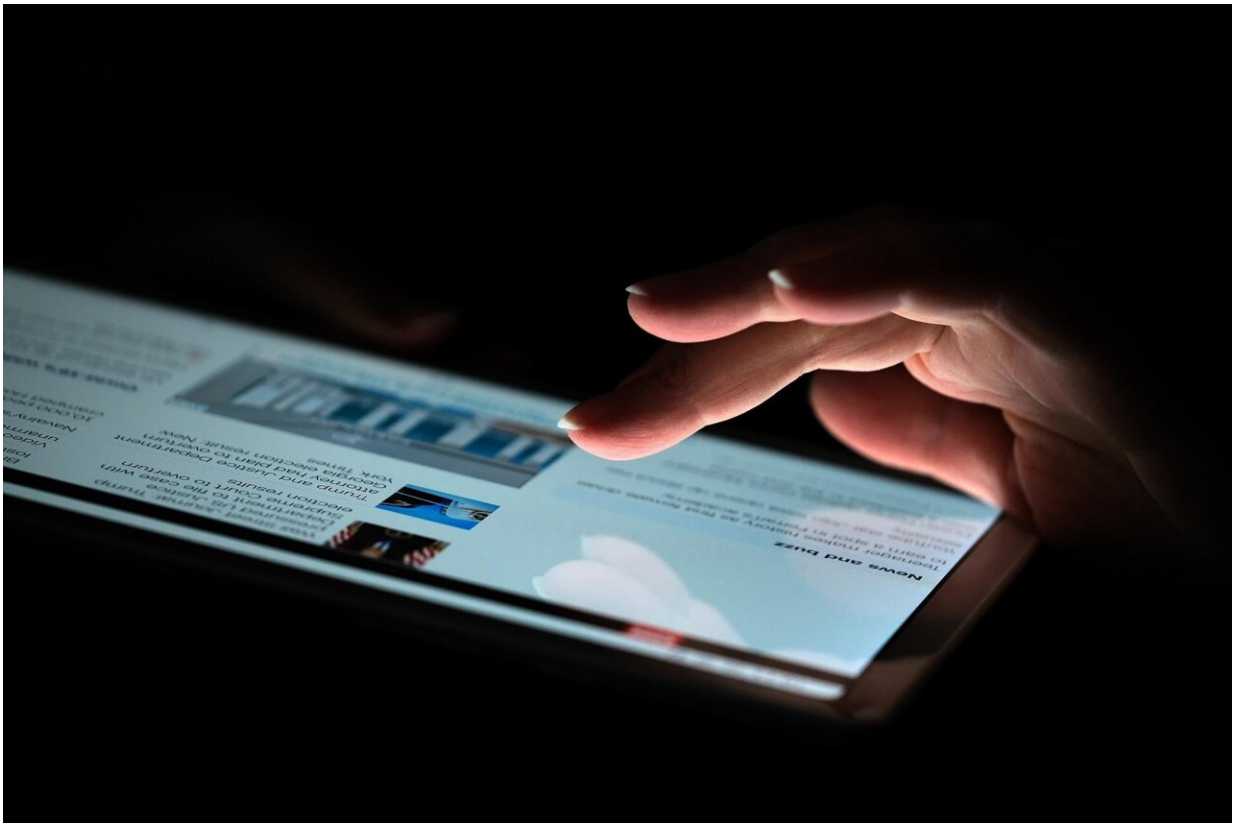
Abortion clinic websites may unwittingly aid patient prosecutions

September 21 2022, by Karl Stark



Credit: Pixabay/CC0 Public Domain

After the Supreme Court's Dobbs decision eliminated the constitutional right to abortion, legislators in several states promised to pass laws that would cause women to be prosecuted even if their procedures occurred

in another state.

And now those prosecutions could be aided by an unexpected source—the patients' own web browsing history—concludes a team of researchers from Penn and Carnegie Mellon University.

More than 99% of abortion clinic web pages studied in May included widely used code that transferred user data to a median of nine external entities, which in turn could sell the data or provide it to law enforcement, according to the team's research letter, published in *JAMA Internal Medicine*. The clinics may not even be aware that visitors' data is being disseminated since the practice is so standard across the web.

While the Penn-CMU team urged consumers to install tracking-blocking browser extensions and adjust privacy settings on browsers and smartphones, those actions are unlikely to provide enough protection, say Ari Friedman and Matthew McCoy, co-authors and senior fellows of the Leonard Davis Institute of Health Economics, Penn's hub for health policy research.

Abortion clinics need to audit their websites and remove third party trackers immediately, says Friedman and McCoy, who are part of the Penn-CMU Digital Health Privacy Initiative.

Federal oversight also is needed to resolve this potentially massive breach of privacy, they said. The federal Data Privacy Bill before Congress would help, but its passage is uncertain.

Why is digital privacy so crucial in the case of abortions?

What makes this different is that for the first time, the harms are so tangible. In this case, state attorneys general have announced that they

intend to pursue people who receive abortions, including those who cross state lines. So this type of routinely collected tracking data can easily be used to find people who have done so.

Friedman: We've been doing digital privacy research for two and a half years. Everywhere we look on the internet, we find that website tracking of visitors is ubiquitous. And that's true even on health-related web pages.

There's been a lot of research attention on location data and smartphone apps. But website-based tracking is notable because it's health care providers themselves, whether they know it or not, that are partnering with tech companies and data brokers to send their patents' data to these companies. So, they have the ability to change that. First, the clinics have to be informed they are actually doing it. It may be just the web administrator making the decision to add functionality and not thinking about the organization's mission.

McCoy: One thing that makes tracking on these pages particularly insidious is that people might be mistakenly assuming that what they do on the webpages of health care providers is protected by privacy laws. They've heard of the federal health privacy law HIPAA. They have an understanding that medical information is legally protected in the U.S. But those protections don't extend to information that can be gleaned from what somebody does on a health providers' website.

Friedman: Even before Dobbs, there have been cases where people's search history and location history were used in prosecutions. That use is now likely to grow.

McCoy: To put this into context, web tracking information is one piece of the puzzle that can be linked with other kinds of information about somebody to determine if they sought an abortion. So you might have

location data that somebody visited an abortion clinic. You might be able to link that to their browsing data to know that three days before they visited the clinic, they were navigating on that clinic's website. You might have some purchase histories after the fact that are linked to the visit to the clinic. Any one of these pieces doesn't give you a conclusive case, but the more pieces of the puzzle you have, the more conclusive a prosecutor's case can be. Every little bit of information counts.

What's a brief summary of the research that has been done in this area?

Friedman: We've known since 2015, when the co-founder of our Penn-CMU institute, Tim Libert, who now works in the industry, did a study that showed tracking on health-related webpages is quite common. At the time, it was 91%. Then, Joshua Niforatos of Johns Hopkins and others looked at the top 50 hospitals and showed how widespread web tracking is in that domain. And there's some qualitative work interviewing thought leaders and technologists, by Penn professors and LDI Fellows Carolyn Cannuscio, David Grande and others, who surfaced perceptions that this kind of routinely collected, not directly health-related web tracking data could give a lot of information about your health status.

McCoy: Early in the pandemic, Ari and I looked at specific pockets of tracking, including COVID-19 websites. Now we know who is doing the tracking and where the information is going. The next phase of our research is really trying to understand what these entities can infer about your health from the webpages you look at.

Which firms are collecting the most information on abortion clinics?

McCoy: You see these big behemoth tech companies, like Google and Meta (aka Facebook) at the top of the list. But there's also an extremely long tail of smaller companies you've never heard of.

Friedman: There are 66 unique parent companies tracking on abortion clinic sites. The most interesting and potentially troubling finding in our study is that 73% of web pages have at least one tracker whose parent company we just couldn't identify.

McCoy: People are resigned to tracking. They think Google already knows everything about them. We don't think people should be so comfortable about this. There's a bunch of other entities that are also collecting information about you. A lot of them don't have any consumer-facing business. You never interact with them the way you do with Google and Meta. And you don't really know what they're doing with your data.

What are the potential solutions?

McCoy: The first thing the clinics should do is figure out what trackers they have on their website and get rid of them. It's our supposition that a lot of people running these clinics probably have no idea what trackers are on their websites. The web administrator set that up some time ago. They are told that "This is how we get analytics on our web page" or "This is how we measure the success of our fundraising campaigns." But it's probably the case that a lot of decision makers at these clinics don't appreciate how many different entities are collecting user data from their websites. There are plenty of consumer-facing products that they can use to get a quick audit of what's on their website. The only way people are going to be protected is if their data is not collected on these websites.

Planned Parenthood says it is aware of the problem and is taking action

to remove trackers, according to a June 30 story in the Washington Post. But when we spot checked a few Planned Parenthood sites, they still had a lot of tracking.

In the meantime, there are things individuals can do like use browser plug-ins that limit trackers. But that's always going to be a second-best solution. Sure, you can spend hours a day trying to understand threats to your online privacy. But most people don't have that luxury. What we need is for clinics to get this stuff off their websites and in the long run to have a federal law that limits or prevents this kind of health-related tracking.

Friedman: I think a lot about this and have taken some steps that take a lot of energy like separating out my browser profiles. Even with that, I'm still quite sure these companies have an enormous amount of information about me. We can't expect our entire society to stop what they're doing and worry about tracking. The personal responsibility paradigm fails here. The ability of tech companies to make it hard to opt out is much greater than the ability of individuals to opt out. Given that, we have to turn to policy solutions. There is the Data Privacy Act that is working its way through Congress that would mark a major step forward for online health privacy. It wouldn't stop targeted advertising altogether, but it would prohibit targeted advertising using sensitive data, including health-related information and Internet browsing histories. It also aims to provide consumers with a clear opt-out method for other forms of targeted advertising, but it's unclear whether the law will be passed.

More information: Ari B. Friedman et al, Prevalence of Third-Party Tracking on Abortion Clinic Web Pages, *JAMA Internal Medicine* (2022). DOI: 10.1001/jamainternmed.2022.4208

Provided by University of Pennsylvania