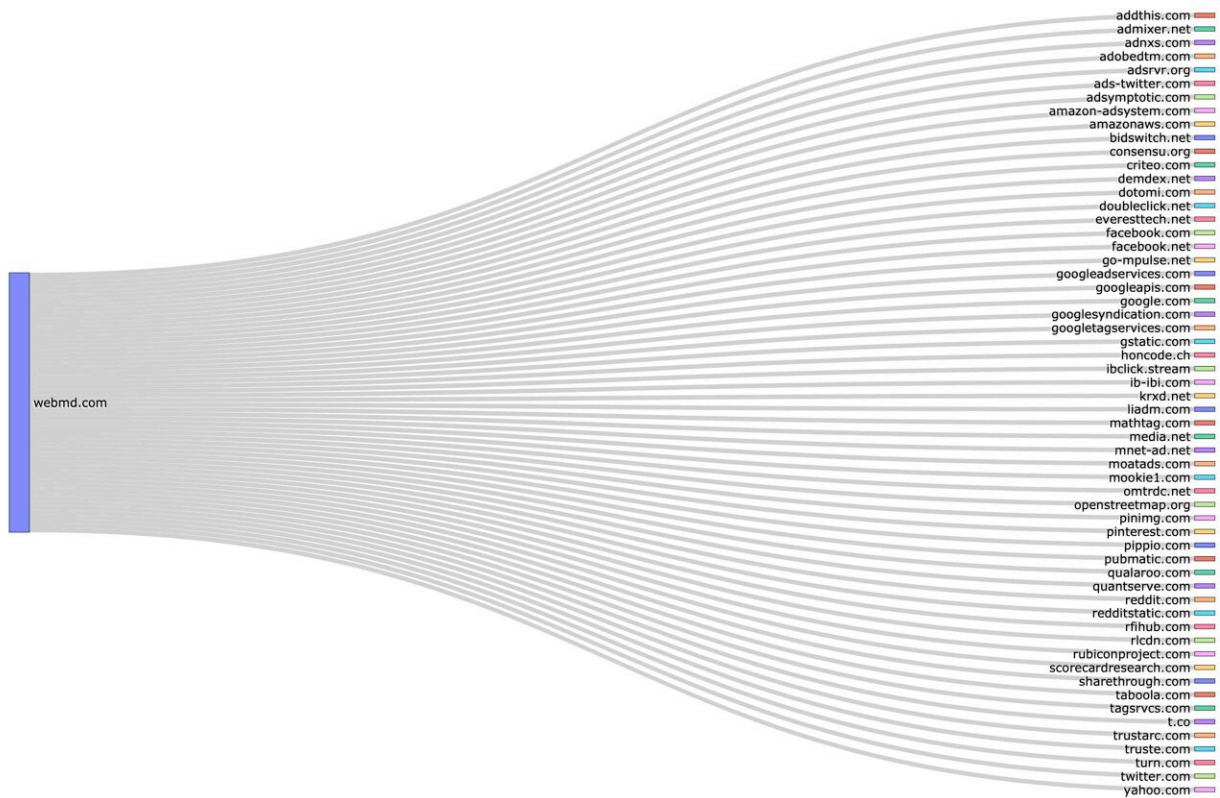


What can browser history inadvertently reveal about a person's health?

May 2 2022, by Michele W. Berger



When users visit the website WebMD.com, more than 50 other websites—listed on the right here—get pinged. Credit: Ari Friedman and Matthew McCoy

One day a few years back, Penn emergency medicine physician Ari Friedman decided to see what would happen if he declined third-party cookies on a medical journal website. "I'd read enough about privacy and

leaks and what was going on with the data that I wanted to turn them off," says Friedman.

Not only couldn't he access the journal article he sought, but he couldn't even get to the issue's table of contents. "I was shocked," he says. "I still have a lot of idealism around academia, and that felt antithetical to the mission of these journals, which is to share knowledge."

At that point, Friedman couldn't do much more than accept cookies when he needed to view something that required them. But the experience stuck with him, to the point that he incorporated the subject into his research agenda, which otherwise centers around gerontology and geriatric emergency medicine.

Out of that grew the Penn-CMU Digital Health Privacy Initiative, which Friedman now runs with Penn Medicine's Matthew McCoy and Lujo Bauer, a computer scientist at Carnegie Mellon University. Funded by the Public Interest Technology University Network (PIT-UN), facilitated at Penn by the SNF Paideia Program, the initiative aims to pinpoint precisely how the routine collection of non-[health data](#) might inadvertently reveal a person's health profile and what implications this has for a range of areas, from insurance coverage to credit scores.

During its first year, the group has worked toward comprehensively mapping third-party tracking across the online health ecosystem, including on websites for [medical journals](#) and hospitals. The next step, according to McCoy and Friedman, is to assess how this tracking might lead to inferences about a person, targeted ads, and more.

"In a lot of different corners of the web, you can't access [health information](#) without being tracked," says McCoy, an assistant professor of medical ethics and health policy. "Most people probably know about cookies, but they likely don't think about their implications, about what

it means to have an entity know all the pages you look at. We want to help people understand why this matters."

Online browsing during a pandemic

When Friedman joined the faculty at Penn's Perelman School of Medicine in 2019, he began thinking about the trajectory of his research agenda. During one early conversation with Penn medical ethicist Atheendar Venkataramani, Friedman described the wall he'd hit turning off cookies for a medical journal website. Venkataramani suggested he talk to McCoy, and soon the two began collaborating, partnering with Timothy Libert, a Penn alum then at CMU, who has since left for a job in the private sector.

Then the pandemic hit. "It's almost hard to put yourself back in this head space, but one thing people really worried about early on were the privacy implications of these contact-tracing and proximity-detection apps," McCoy says. Conversely, people weren't concerned about the dozens of entities pinged each time someone visited a website related to COVID-19.

The researchers decided to analyze 500 or so of the most highly trafficked COVID-related websites, places people were turning to learn about symptoms of the new virus, for example, or find a testing location. "We wanted to figure out, if you visited one of these sites, how many parties would be able to tell that you did?" McCoy says. "Even on academic and government sites where people aren't expecting to be tracked, this kind of third-party tracking was prevalent."

Specifically, the researchers found that 99% of these webpages included a third-party data request, and 89% included a third-party cookie, results they shared in the [*Journal of the American Medical Association*](#) in October 2020.

Around the same time, Friedman and McCoy learned about PIT-UN, a partnership of colleges and universities that Penn joined in 2020. For several years, PIT-UN has given millions of dollars in seed funding for projects aimed at "promoting public interest in technology at the university level." Through the 2021 PIT-UN Challenge and backed by support from the SNF Paideia Program, the researchers secured funding to officially launch the Penn-CMU Digital Health Privacy Initiative.

Implications and long-term solutions

Since their initial paper on COVID-19 websites, they've put out findings about medical journal websites, including one in *JAMA Network Open* on the denial of access for users who block cookies (work inspired by the original experience that led to the initiative), and another in *JAMA Health Forum* on the prevalence of third-party tracking on such sites. In mid-April, they published their latest results, in the journal *Gerontology and Geriatric Medicine*, about online health privacy risks for older adults.

"Right now, we're really in the first quarter of year two, taking the next steps to understand how the companies that are doing this tracking then use it to make inferences about your health and to target different ads to you," McCoy says. "For example, does somebody whose browsing history suggests a diagnosis of diabetes get different ads than someone whose doesn't?"

"We've documented over and over again that most health-related webpages have some tracking," says Friedman. "What are the implications of that?"

Though he and McCoy don't yet know the answer, they have some guesses. These range from relatively innocuous ad targeting to much more damaging privacy loss and the domino effect that could have on credit scores, insurance coverage, and many as-yet-undiscovered facets

of someone's life. For that reason, they say they hope this research also makes consumers more aware of the potential reverberations of their browsing history.

Most people simply click "yes" on the pop-up asking about cookie use, without much thought behind what they're agreeing to, McCoy says. "The way the web is set up, right now, you don't often have an alternative to protect yourself from tracking besides unilaterally opting out of online life." The Digital Health Privacy Initiative team knows that's not realistic in most cases. Rather, they say the solutions need to come at the policy level and should address data privacy and transparency.

"The next generation of cookies isn't going to look like cookies," Friedman says. "Eventually, we hope to address just how much tracking you need to figure out someone's health status." They'll keep peeling back the layers of this opaque system—this "black box," as Friedman describes it—until they can fully follow the path these data travel across the web.

More information: Ari B. Friedman et al, Prevalence of Medical Journal Websites That Deny Access to Users Who Block Browser Cookies, *JAMA Network Open* (2021). [DOI: 10.1001/jamanetworkopen.2021.3492](https://doi.org/10.1001/jamanetworkopen.2021.3492)

Ravi Gupta et al, Prevalence of Third-party Tracking on Medical Journal Websites, *JAMA Health Forum* (2022). [DOI: 10.1001/jamahealthforum.2022.0167](https://doi.org/10.1001/jamahealthforum.2022.0167)

Ari B. Friedman et al, Addressing Online Health Privacy Risks for Older Adults: A Perspective on Ethical Considerations and Recommendations, *Gerontology and Geriatric Medicine* (2022). [DOI: 10.1177/23337214221095705](https://doi.org/10.1177/23337214221095705)

Provided by University of Pennsylvania

Citation: What can browser history inadvertently reveal about a person's health? (2022, May 2)
retrieved 23 April 2024 from

<https://medicalxpress.com/news/2022-05-browser-history-inadvertently-reveal-person.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.