The private sector steps in to protect online health privacy, but critics say it can't be trusted

May 25 2022, by Darius Tahir, Kaiser Health News

Credit: Pixabay/CC0 Public Domain

Most people have at least a vague sense that someone somewhere is doing mischief with the data footprints created by their online activities: Maybe their use of an app is allowing that company to build a profile of

their habits, or maybe they keep getting followed by creepy ads.

It's more than a feeling. Many companies in the health tech sector—which provides services that range from mental health counseling to shipping attention-deficit/hyperactivity disorder pills through the mail—have shockingly leaky privacy practices.

A guide released this month by the Mozilla Foundation found that 26 of 32 mental health apps had lax safeguards. Analysts from the foundation documented numerous weaknesses in their privacy practices.

Jen Caltrider, the leader of Mozilla's project, said the privacy policies of apps she used to practice drumming were scarcely different from the policies of the mental health apps the foundation reviewed—despite the far greater sensitivity of what the latter records.

"I don't care if someone knows I practice drums twice a week, but I do care if someone knows I visit the therapist twice a week," she said. "This personal data is just another pot of gold to them, to their investors."

The stakes have become increasingly urgent in the public mind. Apps used by women, such as period trackers and other types of fertility-management technology, are now a focus of concern with the potential overturning of Roe v. Wade. Fueled by social media, users are exhorting one another to delete data stored by those apps—a right not always granted to users of health apps—for fear that the information could be used against them.

"I think these big data outfits are looking at a day of reckoning," said U.S. Sen. Ron Wyden, D-Oregon. "They gotta decide—are they going to protect the privacy of women who do business with them? Or are they basically going to sell out to the highest bidder?"

Countering those fears is a movement to better control information use through legislation and regulation. While nurses, hospitals, and other health care providers abide by privacy protections put in place by the Health Insurance Portability and Accountability Act, or HIPAA, the burgeoning sector of health care apps has skimpier shields for users.

Although some privacy advocates hope the federal government might step in after years of work, time is running out for a congressional solution as the midterm elections in November approach.

Enter the private sector. This year, a group of nonprofits and corporations released a report calling for a self-regulatory project to guard patients' data when it's outside the health care system, an approach that critics compare with the proverbial fox guarding the henhouse.

The project's backers tell a different story. The initiative was developed over two years with two groups: the Center for Democracy and Technology and Executives for Health Innovation. Ultimately, such an effort would be administered by BBB National Programs, a nonprofit once associated with the Better Business Bureau.

Participating companies might hold a range of data, from genomic to other information, and work with apps, wearables, or other products. Those companies would agree to audits, spot checks, and other compliance activities in exchange for a sort of certification or seal of approval. That activity, the drafters maintained, would help patch up the privacy leaks in the current system.

"It's a real mixed bag—for ordinary folks, for health privacy," acknowledged Andy Crawford, senior counsel for privacy and data at the Center for Democracy and Technology. "HIPAA has decent privacy protections," he said. The rest of the ecosystem, however, has gaps.

Still, there is considerable doubt that the private sector proposal will create a viable regulatory system for health data. Many participants—including some of the initiative's most powerful companies and constituents, such as Apple, Google, and 23andMe—dropped out during the gestation process. (A 23andMe spokesperson cited "bandwidth issues" and noted the company's participation in the publication of genetic privacy principles. The other two companies didn't respond to requests for comment.)

Other participants felt the project's ambitions were slanted toward corporate interests. But that opinion wasn't necessarily universal—one participant, Laura Hoffman, formerly of the American Medical Association, said the for-profit companies were frustrated by "constraints it would put on profitable business practices that exploit both individuals and communities."

Broadly, self-regulatory plans work as a combination of carrot and stick. Membership in the self-regulatory framework "could be a marketing advantage, a competitive advantage," said Mary Engle, executive vice president for BBB National Programs. Consumers might prefer to use apps or products that promise to protect patient privacy.

But if those corporations go astray—touting their privacy practices while not truly protecting users—they can get rapped by the Federal Trade Commission. The agency can go after companies that don't live up to their promises under its authority to police unfair or deceptive trade practices.

But there are a few key problems, said Lucia Savage, a privacy expert with Omada Health, a startup offering digital care for prediabetes and other chronic conditions. Savage previously was chief privacy officer for the U.S. Department of Health and Human Services' Office of the National Coordinator for Health Information Technology. "It is not

required that one self-regulate," she said. Companies might opt not to join. And consumers might not know to look for a certification of good practices.

"Companies aren't going to self-regulate. They're just not. It's up to policymakers," said Mozilla's Caltrider. She cited her own experience—emailing the privacy contacts listed by companies in their policies, only to be met by silence, even after three or four emails. One company later claimed the person responsible for monitoring the email address had left and had yet to be replaced. "I think that's telling," she said.

Then there's enforcement: The FTC covers businesses, not nonprofits, Savage said. And nonprofits can behave just as poorly as any rapacious robber baron. This year, a suicide hotline was embroiled in scandal after Politico reported that it had shared with an artificial intelligence company online text conversations between users considering self-harm and an AI-driven chat service. FTC action can be ponderous, and Savage wonders whether consumers are truly better off afterward.

Difficulties can be seen within the proposed self-regulatory framework itself. Some key terms—like "health information"—aren't fully defined.

It's easy to say some data—like genomic data—is health data. It's thornier for other types of information. Researchers are repurposing seemingly ordinary data—like the tone of one's voice—as an indicator of one's health. So setting the right definition is likely to be a tricky task for any regulator.

For now, discussions—whether in the private sector or in government—are just that. Some companies are signaling their optimism that Congress might enact comprehensive privacy legislation. "Americans want a national privacy law," Kent Walker, chief legal

officer for Google, said at a recent event held by the R Street Institute, a pro-free-market think tank. "We've got Congress very close to passing something."

That could be just the tonic for critics of a self-regulatory approach—depending on the details. But several specifics, such as who should enforce the potential law's provisions, remain unresolved.

The self-regulatory initiative is seeking startup funding, potentially from philanthropies, beyond whatever dues or fees would sustain it. Still, Engle of BBB National Programs said action is urgent: "No one knows when legislation will pass. We can't wait for that. There's so much of this data that's being collected and not being protected."

2022 Kaiser Health News. Distributed by Tribune Content Agency, LLC.

Citation: The private sector steps in to protect online health privacy, but critics say it can't be trusted (2022, May 25) retrieved 22 September 2023 from https://techxplore.com/news/2022-05-private-sector-online-health-privacy.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.