Privacy Daily

Under the terms of your subscription agreement, you may print one copy of an individual article for your own use. Please respect that limit.

Telehealth Suit Provides Road Map for Privacy, Consumer Protection Regulation, Experts Say

August 21, 2026 by Kara Thompson and Adam Bender

The FTC's recent lawsuit with California and Utah against a telehealth provider that shared customer data with third-party advertisers illustrates a road map for companies to follow to protect privacy and ensure a positive consumer experience, consumer advocates and lawyers said recently.

The complaint accused Hims & Hers of failing to clearly and conspicuously disclose that health data would be shared, charging consumers for unwanted prescriptions without consent, misrepresenting free consultation offers, and making it difficult for customers to cancel their subscriptions. The company refuted the charges (see 2607290043).

The biggest thing that stood out to Jade Davis, data privacy lawyer at Shumaker, was that the lawsuit was about the "entire consumer experience," not just one piece. "In modern times, I haven't seen so much jammed into [one] action," she told *Privacy Daily*.

Given that focus, it's "super important for companies to put themselves in a consumer's shoes" to understand what it looks like from their perspective, even if the company doesn't have "malicious intentionality."

For consumer privacy advocates, the action against Hims & Hers is significant because "we have not seen that much action out of the FTC" and it involves a partnership among regulators who "don't often team up for political reasons," said Hayley Tsukayama, Electronic Frontier Foundation state affairs director. "This is really encouraging because it really shows that privacy is ... a bipartisan issue." While the action is "in line" with the FTC's guidance and public statements about going after unfair and deceptive practices, "it is exciting to see enforcement follow up more of those talking points," she added.

California and Utah joining the FTC shows "the state-federal overlay" when it comes to certain privacy and consumer issues, Davis said. Hims is based in San Francisco, and California "is a very good state to bring" consumer protection claims in, she said.

Utah's Division of Consumer Protection is alleging violations of the Utah Consumer Sales Practices Act as well, based on the same general conduct with subscriptions, billing practices, and representations about health-data privacy. This highlights that "a state does not necessarily need a specialized health-privacy statute to pursue this type of conduct," and "general consumer-protection authority can be sufficient" instead, Davis said.

One “interesting question” is why more states didn’t join the suit, said Davis, adding that it “may also signal Utah’s broader regulatory posture going forward.”

Utah “has been notably active on children’s data privacy and social media legislation,” with the legislature describing itself as leading the nation on those fronts, noted the attorney: The state's “participation in the Hims action may reflect that expanding focus."

Lessons for Companies

“This case brings several regulatory scares and concerns together,” which “makes it a useful road map,” Davis said. It’s an example of how “regulators may evaluate the entire consumer experience as a whole, rather than each compliance issue separately.”

It also “validates the concerns” around a privacy policy not matching the technology behind it, which is something companies should be testing themselves, she said.

As Cobun Zweifel-Keegan, IAPP Managing Director for Washington, D.C., blogged after the lawsuit was announced in late July, “the FTC's allegations are generally applicable” to any company using tracking technology. “If data reveals or strongly suggests a person's health condition, treatment status, diagnosis, reproductive condition, addiction issues, mental health status or similar protected characteristic, disclosure to advertising platforms is high risk and should usually occur only with explicit, informed consent.”

Another takeaway is it’s “still possible to violate the FTC Act even with detailed privacy policy disclosures,” Zweifel-Keegan said. While Hims’ marketing claims “don't explicitly mention no information will ever be shared ... the FTC suggests such claims should have been coupled with clear and conspicuous disclosures about the company's actual privacy practices so as not to be deceptive.”

The lawsuit is also a sign that companies “can't operate in silos,” Davis said. “In the privacy and security world, it's really ... an entire enterprise thing” where communication within a business is crucial. Further, the consumer experience “is a representation of what the company looks like,” and the complaint showed that Hims had “lots of issues” there.

Tsukayama said Hims & Hers pushed back on the lawsuit “harder than [she] would have expected,” considering the length of the investigation. “Even if companies are saying that they're focusing on transparency” and helping consumers make informed decisions, “the way that companies design [products] does not always translate that well to actual people who are using the website.”

The EFF official applauded the regulators for focusing on customer expectations. Companies must “think about what people are expecting, and when things are not in line with those expectations.” Tsukayama added that the action highlights how, “if people can't actually understand what you're saying, then [you] might face some questions."

In a recent LinkedIn post, Elevare Law digital health lawyer Rebecca Gwilt said the action is a warning to companies that may be following the lead of a larger organization concerning compliance.

"If any part of your intake, billing, cancellation, or data-sharing flow was modeled on what a bigger platform does, the useful question is not whether they got away with it so far," she said. "It is how many years that clock has already been running, and whether you would rather learn the answer from your own counsel or from a federal complaint."

Further Regulation

One of the "biggest misconceptions" companies have is that certain data falls outside of HIPAA, particularly if it's regulated by another privacy law, said Davis: But in this action, the FTC emphasized that while HIPAA is included, there's also a health data issue broader than that federal statute.

This lawsuit isn't just a warning to telehealth companies, but any business collecting information -- particularly sensitive data -- from customers, Davis said. She noted that companies using "sophisticated advertising technologies" should pay attention to this case.

Many years ago, the companies that typically used this sophisticated ad technology were large and "pretty sophisticated themselves," meaning they had staff that understood the technology as well as money to cover themselves if something happened, the Shumaker lawyer said. But now, even smaller mom-and-pop businesses have access to it, said Davis: While it can be positive for them, often "they don't really understand what they're using," which can lead to liability.

Because of this, Davis wants to see more regulation on the entities that make and sell these tools and their disclosures about what the tools do. It might also help if the vendor selling the tracking technology provided its business customer with a walkthrough of what exactly a tool does before it's implemented, she said.

Copyright© 2026 by Warren Communications News, Inc. Reproduction or retransmission in any form, without written permission, is a violation of Federal Statute (17 USC101 et seq.). Please review our User Agreement.