



# CLIENT ALERT

March 2023

1

## FTC BANS BETTERHELP, INC. FROM REVEALING CONSUMERS' SENSITIVE HEALTH DATA TO THIRD PARTIES FOR ADVERTISING

by Ashley Fernandez

The practice of turning over our personal data to online platforms is nothing new and, some may argue, a routine practice of using the Internet today. A survey by the [Pew Research Internet Project](#) reveals that roughly six-in-ten U.S. adults do not think it is possible to go through daily life without having data collected about them by companies or the government – and more than 60% of people are concerned about this.

Most of the time, providing this information feels non-threatening. For example, consider going to the grocery store and entering your phone number for your loyalty rewards account. Harmless enough. What we do not tend to think about, though, is that phone number then attaching to your name and all of your shopping preferences each time you enter it into the kiosk and begin to scan your items. Now, by providing merely your phone number, a substantial profile of your eating habits now exists, explaining why you might receive just the coupon you needed in the mail only a few days later. This is no coincidence, and, indeed, many times, it is an added convenience to everyday life.

But when does the collection of personal data cross the line? The FTC helped answer this question through their issuance of a proposed order last week following an investigation into the practices of BetterHelp, Inc. ("BetterHelp"), an online platform that provides a variety of mental health services.

BetterHelp aims to pair individuals with online counselors that fit their particularized needs. To do so effectively, consumers must answer a series of questions that inquire into their sensitive health information from whether they have ever experienced suicidal thoughts to whether they are on any medications. This is in addition to the, what has become, "standard", personal information they must provide, like their name, email address, and date of birth. Throughout this process, consumers are reassured every step of the way by BetterHelp's representation that it does not use or disclose this personal health data. For example, directly below the question inquiring about whether the consumer is currently taking any medication is the following [statement](#): "Rest assured – your health information will stay private between you and your counselor." Again, seems harmless enough.

However, following the FTC's investigation, the Commission discovered this was not the case. Indeed, all along, BetterHelp would turn consumers' email addresses, IP addresses, and health questionnaire information over to Facebook, Snapchat, Criteo and Pinterest to fuel the ability of these third parties to target potential new clients with ads.

"For example, the company used consumers' email addresses and the fact that they had previously been in therapy to instruct Facebook to identify similar consumers and target them with advertisements for BetterHelp's counseling service, which helped the company bring in tens of thousands of new paying users and millions of dollars in revenue," said the [FTC website](#).

Now, the FTC is taking action by agreeing 4-0 to issue a proposed order that would require the company to pay a staggering \$7.8 million to provide partial refunds to consumers who signed up and paid for BetterHelp's services between August 1, 2017 and December 31, 2020.

The action is the first of its kind that would return funds directly to consumers impacted by the disclosure of their health data.

"When a person struggling with mental health issues reaches out for help, they do so in a moment of vulnerability and with an expectation that professional counseling services will protect their privacy," said [Samuel Levine, Director of the FTC's Bureau of Consumer Protection](#). "Instead, BetterHelp betrayed consumers' most personal health information for profit. Let this proposed order be a stout reminder that the FTC will prioritize defending Americans' sensitive data from illegal exploitation."

Additionally, the proposed order:

- Imposes a complete ban on BetterHelp's disclosure of health information for advertising;
- Requires BetterHelp to obtain affirmative express consent before disclosing personal information to certain third parties for any purpose;
- Requires BetterHelp to establish a comprehensive privacy program with the purpose of protecting consumer data;
- Requires BetterHelp to direct third parties to delete the consumer health and other personal data that BetterHelp revealed to them; and
- Limits how long it can retain personal and health information according to a data retention schedule.

A description of the consent agreement package is set for publication in the Federal Register in the coming days where it will be subject to public comment for 30 days. Following public comment, the Commission will make its definitive decision as to whether to make the proposed consent order final. Instructions for filing comments will appear in the published notice, and once processed, will also be available for public viewing at [Regulations.gov](#).

# CLIENT ALERT

The FTC action serves as an important reminder to companies that having a sound privacy policy in place is only half the battle. Being compliant on paper is only as good as the company's ultimate actions. Working with DW's Privacy and Cybersecurity Team can reassure companies that they are not only displaying a privacy policy that is in compliance with the ever-changing labyrinth of privacy laws, but that they are sticking to the words contained in that policy through their everyday actions – particularly when it is, and when it is not, OK to disclose data.

## ABOUT THE AUTHORS



**Ashley N. Fernandez** is an Associate in Dickinson Wright's Detroit office. She can be reached at 313.223.3582 or [afernandez@dickinsonwright.com](mailto:afernandez@dickinsonwright.com).