New Class Certification Decision in App-Tracking Case Provides Critical Guidance for Businesses Facing Privacy Claims

Insights
5.30.25

A California federal court just certified a significant class action involving allegations that a health-tracking app improperly shared sensitive health information with third parties without user consent. The court's May 22 class certification marks a pivotal moment in ongoing litigation concerning the collection and disclosure of personal data and may serve as a bellwether in predicting how courts will address key issues related to data privacy, user consent, and class action waiver enforceability.

What Happened?

In *Frasco v. Flo Health, Inc.*, the court certified both a nationwide class and a California subclass consisting of individuals who entered personal information into the Flo Health App.

- Women from various states alleged that the Flo App – marketed as a tool for tracking reproductive health – secretly transmitted users' personal information to third parties for commercial purposes without their consent.
- This data included details about menstruation, ovulation, and pregnancy goals.
- The plaintiffs brought claims against Flo and several third-party tech companies, asserting violations of (1) the California Confidentiality of Medical Information (CMIA); (2) breach of contract; (3) common law invasion of privacy; (4) the Comprehensive Data Access and Fraud Act (CDAFA); and (5) California Invasion of Privacy Act (CIPA).
- They argued that the defendants' actions not only violated these laws but also breached contractual promises to keep user data confidential.

What is Class Certification?

Class certification is the process by which a court determines whether a lawsuit can move forward to trial on behalf of an individual or on behalf of a class of individuals – as a class action. In federal court, the requirements for class certification are set out in the Federal Rule of Civil Procedure Rule 23. A plaintiff seeking certification of a class must show:

- the class is so numerous that joinder of all members is **impracticable**;
- there are questions of law or fact **common** to the class;

- the claims or defenses of the representative parties are **typical** of the claims or defenses of the class; and
- the representative parties will **fairly and adequately protect** the interests of the class.

Federal Court Greenlights Class Certification

The court granted class certification on all but two causes of action, allowing the case to proceed. A key requirement for class certification is that plaintiffs must show that common factual and legal issues can be determined on a class-wide basis without the need for individualized inquiry into each class member's claims. Defendants opposed certification, arguing that issues of implied consent, contractual limitations period, class action waiver, and standing presented individualized questions that prevented the court from granting certification.

The court rejected these arguments and certified a nationwide class for claims under the California Confidentiality of Medical Information Act (CMIA), breach of contract, and intrusion upon seclusion against Flo. Additionally, a California subclass was certified for claims under the California Constitution's privacy provisions. The court denied class certification for claims under the CDAFA and certain aspects of CIPA.

Impact of Decision And Your Next Steps

The court's decision in the *Frasco v. Flo Health, Inc.* has significant implications for businesses, technology and app development sectors, and those that rely on user data for both software development and revenue generation.

1. Unenforceability of Class Action Waiver

One of the significant aspects of the court's decision was its finding that the class action waiver in Flo's Terms of Service was unenforceable. The court found it particularly problematic that the arbitration and class action waiver was "buried in a manner that made it likely a user's attention was not drawn to it." This finding underscores some courts' skepticism of clauses buried in Terms of Service, even if consumers "check the box" that they've read and understood those terms.

Your Next Steps

If your business's Terms of Service contain an arbitration agreement and class action waiver, it is essential to highlight these provisions, such as include bolded, all-caps language at the top of the Terms of Use advising that such terms are included. Additionally, reference the existence of the arbitration agreement and class action waiver wherever users are accepting the Terms of Service. If sued, it is helpful to show that you clearly informed users of the arbitration agreement and class action waiver provisions in multiple conspicuous locations to demonstrate that they gave unequivocal consent.

It also is important to remember that enforcing arbitration agreements can vary by states. While not addressed specifically in this case, you should consider how best to present the arbitration agreement and class action waiver provisions to prospective clients in a manner that meets the enforceability requirements for the jurisdictions in which your business operates.

2. Standing Despite Anonymization

The court also rejected the argument that the plaintiffs and class members lacked standing because the information shared was anonymized. The court emphasized that the legal injury occurred at the point of data interception without consent, regardless of whether the data was later anonymized. This court instead held that this type of unauthorized data collection constitutes a concrete injury, regardless of whether it is anonymized.

Your Next Steps

The court pointed a pathway forward for risk minimization: consent from end-users. Ensure that your privacy and cookie policies account for anonymized data and that cookie consent management allows for the control of data that will ultimately be anonymized.

Consider providing website visitors the option to choose whether they opt-in or opt-out of the use of data. Opt-in consent may not be required by applicable consumer privacy laws like the California Consumer Privacy Act (CCPA). However, providing website users more control of their privacy choices is another way to align user expectations of privacy with their experience on your website and obtain consent, mitigating against privacy litigation.

3. Multiple Claims Proceeded Based on Alleged Misrepresentations in Terms of Service and Privacy Policy

Although the case involved multiple theories of liability, there was a common throughline for purposes of class certification: did Flo misrepresent its privacy practices in its Terms of Service and Privacy Policy? While this was not the sole issue in all of the claims, its recurring nature emphasized that a user's expectations about privacy can be set – or at least molded – by the disclosures and representations made to them in such documents.

Your Next Steps

Review your Terms of Use, Privacy Policy, and any other representations on your website (including statements on individual pages or in Frequently Asked Questions) for accuracy on a regular cadence. You should ensure your representations about your privacy practices – no matter the location on your website – reflect your actual privacy practices.

Conclusion

Fisher Phillips will continue to monitor developments in this area. We will provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's Digital Wiretapping Litigation Team or Consumer Privacy Team.

Related People

Catherine M. Contino
Associate
610.230.6103
Email

Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Danielle Kays
Partner
312.260.4751
Email

Xuan Zhou, CIPP/US, CIPM, CIPP/E
Associate
858.597.9632
Email

Service Focus

Litigation and Trials

Privacy and Cyber

Digital Wiretapping Litigation

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

Woodland Hills