After Apple: What Online Businesses Need to Know About Privacy Expectations After Recent Court Decision

Insights
2.11.26

A recent federal court decision from California in *In re Apple Data Privacy Litigation* reflects an evolving judicial approach to how courts will define the boundaries of privacy in a platform-driven world. The January 20 decision – which was a mixed bag of wins and losses for businesses for companies operating online – exposes a growing tension regarding what users can reasonably expect when they interact with digital services and what businesses can reasonably rely on when designing their data practices. Here's a review of the decision and some practical takeaways you should consider for your business.

2024 Dismissal of Claims

The *Apple* case, filed in the Northern District of California, arose from users' interactions with Apple's first-party apps on their mobile Apple devices. The plaintiffs alleged that Apple improperly collected and used their data, such as app usage details, app browsing communications, personal information, and device information, when users interacted with Apple apps. The consolidated complaint asserted 12 claims, including breach of express and implied contracts, breach of the implied covenant of good faith and fair dealing, invasion of privacy, violation of California Invasion of Privacy Act (CIPA) Section 632, violation of California Unfair Competition Law (UCL), violation of Pennsylvania's Wiretapping and Electronic Surveillance Control Act (WESCA), New York Gen. Bus. Law § 349 and § 350 ("GBL"), New Jersey's Consumer Fraud Act (NJCFA), Illinois's Consumer Fraud and Deceptive Business Practices Act (ICFDA), and unjust enrichment.

Initially, the court dismissed a series of claims in its decision issued on September 26, 2024.

- **CIPA Section 632:** Although plaintiffs plausibly alleged the Apps constituted a "device" under Section 632 and alleged collection despite disabling the "Share [Device] Analytics" setting, they failed to allege details about what information was collected that constituted as a "communication" under CIPA.
- **WESCA:** The court did not base its dismissal on the prior consent requirement, but because the plaintiffs did not plausibly allege interception of the "contents" of a communication. General logging or record-type data was not enough.
- **Invasion of Privacy:** Reasoning that no reasonable consumer would expect to transact with Apple through apps such as Books without some data being collected to process the

transaction, the court rejected this claim.

The court dismissed plaintiffs' contract claims relating to the "Allow Apps to Request to Track" setting, finding that plaintiffs consented to the challenged data collection, failed to allege withdrawal of consent, and did not plausibly plead a third-party beneficiary theory based on Apple's Family Disclosure. It likewise dismissed the implied covenant claim to the extent it relied on those same theories. The court further dismissed plaintiffs' consumer protection claims under the UCL, GBL, NJCFA, and ICFDA for failure to plead with particularity, dismissing the misrepresentation claims tied to advertisements and the tracking setting, while allowing the claim concerning the "Share [Device] Analytics" setting to proceed. Plaintiffs' fraudulent omission claim was also dismissed for insufficient pleading.

Recent Rulings Clarify Standards

The plaintiffs had another bite at the apple (pun intended) to amend their complaint and in fact added a new claim in the hopes that something would stick.

- **CIPA Section 638.51:** The plaintiffs amended the complaint to add a pen register claim. The court acknowledged that the pen register statute could apply to internet communications but dismissed the claim. It concluded that Apple's apps were first-party tools integral to the communication, not third-party interceptors, and that the theory contradicted plaintiffs' Section 632 allegations.
- **CIPA Section 632**: The court again dismissed the 632 claim – again – holding that plaintiffs failed to plausibly allege the data at issue (such as referral URLs and search terms) were "confidential," particularly where such data was necessary for Apple to respond to user requests.
- **WESCA:** The WESCA claim failed for similar reasons: search terms reflecting app titles were not "contents," the court said, and the alleged "device" performing interception must be separate from the source of communication.
- **Invasion of Privacy:** This claim was also dismissed because plaintiffs failed to differentiate between "necessary" and "unnecessary" data collection, and general URLs or non-sensitive routing information did not rise to a highly sensitive level.
- **UCL:** Additionally, the court dismissed plaintiffs' renewed claim under the UCL for the same reason articulated in its 2024 decision – namely, that plaintiffs failed to plausibly allege what was false or misleading about Apple's marketing materials or explain how those materials were misleading in light of the data collection practices at issue.
- **Miscellaneous Claims:** The court also dismissed the implied contract and unjust enrichment claims, finding that they were duplicative of and dependent upon the express contracts forming the basis of plaintiffs' breach of contract claim.

- Finally, the court dismissed all allegations relating to Apple's Game Center because none of the plaintiffs alleged that they had ever used that service.

Nevertheless, the court granted plaintiffs leave to amend, affording them a third opportunity to revise their complaint. We expect to see this battle continue as the plaintiffs will once again try to identify a pathway forward for the litigation.

What the Decision Means for Business

While the *Apple* litigation centered on a major technology platform, the court's reasoning has broader implications for any company delivering services online.

How Courts Can Treat Data as a Mechanical Component

- A consistent theme in the court's reasoning is that data such as search terms, URLs, device identifiers, and routing information may be considered part of the mechanics of delivering a service rather than interception of "confidential" content.
- For companies, data that is operationally necessary to process user requests, when transparently disclosed, may not automatically trigger wiretapping liability.
- However, the decision should not be read as an endorsement of broad data practices. The court's analysis turned in part on the plaintiffs' inability to distinguish between operational necessity and additional, potentially exploitative uses.

"Content" v. "Record" Is a Critical Legal Distinction

- A recurring issue in both the CIPA and WESCA analyses was the distinction between content of communication and record or routing data. The court repeatedly found that logging app titles or general URL did not constitute interceptions of communication "content."
- For business, this underscores the importance of categorizing data flows, such as what information is required to complete the transaction, what information is stored temporarily or persistently, what information is used internally or shared externally. Clear internal documentation of these distinctions can be critical in litigation or regulatory inquiries.

First-Party Platforms Carry Different Risk Profiles

- The dismissal of the pen register claim is particularly instructive. The court emphasized that the interception device must be separate from the source of communication. Because Apple's apps were integral to the communication itself, they were not treated as third-party interceptors.
- For companies operating integrated digital platforms, this distinction may reduce exposure under certain interception statutes. By contrast, embedding third-party tracking technologies that operate independently from core functionality may invite greater scrutiny.

"Necessary" v. "Unnecessary" Data Will Be the Next Battleground

- Plaintiffs attempted to argue that reasonable consumers would not expect "unnecessary" data collection. The court rejected this theory because plaintiffs failed to articulate what data was unnecessary and the reasons.
- For companies, necessity will increasingly be examined through the lens of functionality. Courts may ask whether the data required is to deliver the service requested, whether it is used to secure transaction, or whether it is used to prevent fraud. When companies can articulate a clear functional rationale tied to service delivery, litigation risk may be reduced. Conversely, where data collection appears tangential, commercially driven, or insufficiently disclosed, scrutiny and exposure may increase.

Key Takeaways for Businesses

The *Apple* decisions indicate that courts are reluctant to expand interception statutes to ordinary platform-enabled data processing. At the same time, they leave open room for liability where data practices exceed operational necessity or contradict user-facing representations (see, for example, the Pennsylvania Supreme Court's recent guidance on reasonable expectations of privacy in internet search activity). For companies operating online, several practical lessons emerge:

- Courts are defining privacy expectations less by abstract notions of secrecy and more by how digital architecture actually operates in practice.
- Courts acknowledge that digital platforms cannot function without collecting and processing certain categories of transactional and routing data.
- Companies should understand how courts differentiate between operational logging (e.g., routing information, app titles, device identifiers) and substantive communication content, as this distinction is central to interception claims.
- Conduct periodic reviews of what data is collected at each user interaction point, how it is categorized, and whether it is necessary to deliver the requested service.
- Embedded third-party tools may create interception-style risks that differ from first-party data processing within an integrated ecosystem.

Conclusion

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group.

Related People

Danielle Kays
Partner
312.260.4751
Email

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

Service Focus

Privacy and Cyber

Consumer Privacy Team

Litigation and Trials