Published on *The National Law Review* https://natlawreview.com

PRIVACY ON ICE: A Chilling Look at Third-Party Data Risks for Companies

Article By:

Blake Landis

An intelligent lawyer could tackle a problem and figure out a solution. But a brilliant lawyer would figure out how to prevent the problem to begin with. That's precisely what we do here at Troutman Amin. So here is the latest scoop to keep you cool. A recent case in the United States District Court for the Northern District of California, *Smith v. Yeti Coolers, L.L.C.*, No. 24-cv-01703-RFL, 2024 U.S. Dist. LEXIS 194481 (N.D. Cal. Oct. 21, 2024), addresses complex issues surrounding online privacy and the liability of companies who enable third parties to collect and use consumer data without proper disclosures or consent.

Here, Plaintiff alleged that Yeti Coolers ("Yeti") used a third-party payment processor, Adyen, that collected customers' personal and financial information during transactions on Yeti's website. Plaintiff claimed Adyen then *stored this data* and *used it for its own commercial purposes*, like marketing fraud prevention services to merchants, *without customers' knowledge or consent*. Alarm bells should be sounding off in your head—this could signal a concerning trend in data practices.

Plaintiff sued Yeti under the California Invasion of Privacy Act ("CIPA") for violating California Penal Code Sections 631(a) (wiretapping) and 632 (recording confidential communications). Plaintiff also brought a claim under the California Constitution for invasion of privacy. The key question here was whether Yeti could be held derivatively liable for Adyen's alleged wrongful conduct.

So, let's break this down step by step.

Under the alleged CIPA Section 631(a) violation, the court found that Plaintiff plausibly alleged Adyen violated this Section by collecting customer data as a third-party eavesdropper *without proper consent*. In analyzing whether Yeti's Privacy Policy and Terms of Use constituted enforceable agreements, it applied the legal frameworks for "clickwrap" and "browsewrap" agreements.

Luckily, my Contracts professor during law school here in Florida was remarkable, Todd J. Clark, now the Dean of Widner University Delaware Law School. For those who snoozed out during Contracts class during law school, here is a refresher:

Clickwrap agreements present the website's terms to the user and require the user to affirmatively click an "I agree" button to proceed. Browsewrap agreements simply post the terms via a hyperlink

at the bottom of the webpage. For either type of agreement to be enforceable, the Court explained that a website must provide 1) reasonably conspicuous notice of the terms and 2) require some action unambiguously manifesting assent. *See Oberstein v. Live Nation Ent., Inc.*, 60 F.4th 505, 515 (9th Cir. 2023).

The Court held that while Yeti's pop-up banner and policy links *were conspicuous*, they did not create an enforceable clickwrap agreement because "Defendant's pop-up banner does not require individuals to click an "I agree" button, nor does it include any language to imply that by proceeding to use the website, users reasonably consent to Defendant's terms and conditions of use." *See Smith*, 2024 U.S. Dist. LEXIS 194481, at *8. The Court also found no enforceable browsewrap agreement was formed because although the policies were conspicuously available, "Defendant's website does not require additional action by users to demonstrate assent and does not conspicuously notify them that continuing to use to website constitutes assent to the Privacy Policy and Terms of Use." *Id.* at *9.

What is more, the Court relied on *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1179 (9th Cir. 2014), which held that "where a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice." Here, the Court found the pop-up banner and link on Yeti's homepage presented the same situation as in *Nguyen* and thus did not create an enforceable browsewrap agreement.

Thus, the Court dismissed the Section 631(a) claim due to insufficient allegations that Yeti was aware of Adyen's alleged violations.

However, the Court held that to establish Yeti's derivative liability for "aiding" Adyen under Section 631(a), Plaintiff had to allege facts showing Yeti acted with *both knowledge* of Adyen's unlawful conduct and the *intent* or *purpose* to assist it. It found Plaintiff's allegations that Yeti was "aware of the purposes for which Adyen collects consumers' sensitive information because Defendant is knowledgeable of and benefitting from Adyen's fraud prevention services" and "assists Adyen in intercepting and indefinitely storing this sensitive information" were too conclusory. *Smith*, 2024 U.S. Dist. LEXIS 194481, at *13. It reasoned: "Without further information, the Court cannot plausibly infer from Defendant's use of Adyen's fraud prevention services alone that Defendant knew that Adyen's services were based on its allegedly illegal interception and storing of financial information, collected during Adyen's online processing of customers' purchases." *Id.*

Next, the Court similarly found that Plaintiff plausibly alleged Adyen recorded a confidential communication without consent in violation of CIPA Section 632. A communication is confidential under this section if a party "has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 776-77 (2002). It explained that "[w]hether a party has a reasonable expectation of privacy is a context-specific inquiry that should not be adjudicated as a matter of law unless the undisputed material facts show no reasonable expectation of privacy." *Smith*, 2024 U.S. Dist. LEXIS 194481, at *18-19. At the pleading stage, the Court found Plaintiff's allegation that she reasonably expected her sensitive financial information would remain private was sufficient.

However, as with the Section 631(a) claim, the Court held that Plaintiff did not plead facts establishing Yeti's derivative liability under the standard for aiding and abetting liability. Under *Saunders v. Superior Court*, 27 Cal. App. 4th 832, 846 (1994), the Court explained a

defendant is liable if they a) know the other's conduct is wrongful and substantially assist them or b) substantially assist the other in accomplishing a tortious result and the defendant's own conduct separately breached a duty to the plaintiff. The Court found that the Complaint lacked sufficient non-conclusory allegations that Yeti knew or intended to assist Adyen's alleged violation. *See Smith*, 2024 U.S. Dist. LEXIS 194481, at *16.

Lastly, the Court analyzed Plaintiff's invasion of privacy claim under the California Constitution using the framework from *Hill v. Nat'l Coll. Athletic Ass'n*, 7 Cal. 4th 1, 35-37 (1994). For a valid invasion of privacy claim, Plaintiff had to show 1) a legally protected privacy interest, 2) a reasonable expectation of privacy under the circumstances, and 3) a serious invasion of privacy constituting "an egregious breach of the social norms." *Id.*

The Court found Plaintiff had a protected informational privacy interest in her personal and financial data, as "individual[s] ha[ve] a legally protected privacy interest in 'precluding the dissemination or misuse of sensitive and confidential information.'" *Smith*, 2024 U.S. Dist. LEXIS 194481, at *17. It also found Plaintiff plausibly alleged a reasonable expectation of privacy at this stage given the sensitivity of financial data, even if "voluntarily disclosed during the course of ordinary online commercial activity," as this presents "precisely the type of fact-specific inquiry that cannot be decided on the pleadings." *Id.* at *19-20.

Conversely, the Court found Plaintiff did not allege facts showing Yeti's conduct was "an egregious breach of the social norms" rising to the level of a serious invasion of privacy, which requires more than "routine commercial behavior." *Id.* at *21. The Court explained that while Yeti's simple use of Adyen for payment processing cannot amount to a serious invasion of privacy, "if Defendant was aware of Adyen's usage of the personal information for additional purposes, this may present a plausible allegation that Defendant's conduct was sufficiently egregious to survive a Motion to Dismiss." *Id.* However, absent such allegations about Yeti's knowledge, this claim failed.

In the end, the Court dismissed Plaintiff's Complaint but granted leave to amend to correct the deficiencies, so this case may not be over. The Court's grant of "leave to amend" signals that if Plaintiff can sufficiently allege Yeti's knowledge of or intent to facilitate Adyen's use of customer data, these claims could proceed. As companies increasingly rely on third parties to handle customer data, we will likely see more litigation in this area, testing the boundaries of corporate liability for data privacy violations.

So, what is the takeaway? As a brilliant lawyer, your company's goal should be to prevent privacy pitfalls before they snowball into costly litigation. Key things to keep in mind are 1) ensure your privacy policies and terms of use are properly structured as enforceable clickwrap or browsewrap agreements, with conspicuous notice and clear assent mechanisms; 2) conduct thorough due diligence on third-party service providers' data practices and contractual protections; 3) implement transparent data collection and sharing disclosures for informed customer consent; and 4) stay abreast of evolving privacy laws.

In essence, taking these proactive steps can help mitigate the risks of derivative liability for third-party misconduct and, most importantly, foster trust with your customers.

National Law Review, Volume XIV, Number 306

Source URL:https://natlawreview.com/article/privacy-ice-chilling-look-third-party-data-risks-companies