

# Ubisoft Win Offers Defense Blueprint for VPPA Consent Challenges

MAY 12, 2025

Authors: [David M. Krueger](#)

A recent decision from the Northern District of California may signal an important shift in the trend of how courts interpret “consent” under the Video Privacy Protection Act (VPPA). In *Lakes v. Ubisoft, Inc.*, No. 24-cv-06943-TLT (N.D. Cal. Apr. 1, 2025), district Judge Trina L. Thompson dismissed a privacy class action at the pleading stage and without leave to amend, holding that the plaintiffs’ consent to Ubisoft’s data-sharing practices—delivered via a cookie banner, account creation process, and checkout flow—was sufficient to defeat claims under the VPPA and several other state and federal privacy statutes. The decision reflects a potentially more pragmatic and defense-friendly approach to VPPA consent, one that focuses less on formalism and more on the totality of the user experience. Most importantly, it holds that consent under the VPPA does not need to be obtained on a “standalone” consent form, as many plaintiffs have urged.

## Background: The VPPA and the “Distinct and Separate” Requirement

The VPPA prohibits video service providers from knowingly disclosing personally identifiable information (“PII”) about a consumer without that consumer’s informed, written consent. Crucially, the statute requires that such consent be obtained “in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer.” This requirement has proven fatal to many defendants’ motions to dismiss, particularly where consent is included within privacy policies, terms of use, or other bundled disclosures. Plaintiffs have pushed for arguing that “distinct” consent under the VPPA requires the consent to be on a separate or “standalone” document from other disclosures commonly seen in privacy policies, essentially ignoring that the statute only requires the consent to be “distinct” from any document that imposes legal or financial obligations on the consumer.

## The Ubisoft Decision

In *Ubisoft*, the plaintiffs alleged that the company violated the VPPA and other privacy laws by embedding Meta’s tracking Pixel on its website. This Pixel allegedly transmitted the plaintiffs’ Facebook IDs and video viewing activity (such as game cutscenes) to Meta without adequate disclosure or consent.

The court disagreed. It held that the plaintiffs had consented to the data-sharing through multiple interactions:

- A cookie banner presented on first visit, which offered a clear “OK” button and a link to customize preferences;

- An account creation process that required agreement to Ubisoft's Terms of Use and Privacy Policy; and
- A checkout flow that reiterated the Privacy Policy.

The court emphasized that the Privacy Policy disclosed Ubisoft's use of cookies and third-party data-sharing tools and provided users with options to withdraw or adjust their consent. The court found that the VPPA's "distinct and separate" requirement was satisfied because the consent disclosures were not bundled with legal or financial obligations imposed on the user, but rather served as informational notices.

### Contrast with Other Privacy Cases

The decision stands in contrast to a recent high-profile privacy ruling in *Calhoun v. Google, LLC*, 113 F.4th 1141 (9th Cir. 2024), where the Ninth Circuit rejected consent defenses due to vague, inconsistent, or overly general disclosures.

In *Calhoun*, the Ninth Circuit held that Chrome users who opted not to sync their browser could reasonably believe that Google would not collect certain personal information, even though Google's policies mentioned data collection broadly. By contrast, the *Ubisoft* court took a more holistic view. It considered the layered consent process and gave significant weight to user-facing design-indicating that when users are clearly informed and presented with meaningful options, that may suffice under the VPPA.

### Takeaways for Companies

While *Ubisoft* is just one district court opinion, it may offer a useful playbook for companies seeking to insulate themselves from VPPA liability:

- **Use layered disclosures:** Combine cookie banners, account creation checkpoints, and checkout consent flows to reinforce user awareness.
- **Enable real-time user control:** Provide clear, accessible options for users to modify or withdraw consent.
- **Avoid bundling:** Keep consent requests separate from legal or financial terms to satisfy the VPPA's formal requirements.

The ruling also could reflect an emerging trend: some courts are willing to consider user interface design and consent flows-not just dense legal text-when evaluating the sufficiency of notice and consent.

### Conclusion

The *Ubisoft* decision is important not just for the guidance it provides, but also in litigation defense. Far too often, plaintiffs argue that the "distinct" consent requirement of the VPPA requires consent to be essentially in a standalone document from a defendant's other privacy disclosures. But the court's decision in *Ubisoft*

frames the critical distinction that consent under the VPPA must be “distinct” only from a document that sets forth other legal or financial obligations of a consumer. In other words, including VPPA consent in a general privacy policy may suffice *so long as* the privacy policy is geared towards disclosures and consent alone, and does not attempt to impose any legal or financial obligations on the consumer. Plaintiffs will still argue for strict construction of the statute’s consent provisions, but defendants may now point to *Ubisoft* as a signal that clear, layered, and accessible consent mechanisms suffice. The case offers both a cautionary tale and a strategic blueprint for digital platforms navigating the evolving intersection of user experience and privacy law.

Making necessary changes to websites, and any privacy policies, sooner rather than later is key. Statutory damages are significant under the VPPA at \$2,500 per violation, and companies face significant class action exposure from potential missteps. Making changes now can mitigate the risk of substantial liability down the line. As the legal landscape continues to evolve, staying informed and proactive is the best defense.

**David Krueger is Co-Chair of Benesch's Privacy Litigation & Compliance Group. He can be reached at [dkrueger@beneschlaw.com](mailto:dkrueger@beneschlaw.com) or 216.363.4683.**

**Stanton Williams is a Managing Associate in Benesch's Litigation Practice Group. He can be reached at [swilliams@beneschlaw.com](mailto:swilliams@beneschlaw.com) or 216.363.6107.**