No. 25-2857

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

TREVOR LAKES AND ALEX RAJJOUB,
Plaintiffs-Appellants

v.

UBISOFT, INC.,
Defendant-Appellee.

On Appeal from the United States
District Court for the Northern District of California
No. 3:24-cv-06943-TLT
The Honorable Trina L. Thompson, District Court Judge

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFF-APPELLANTS AND REVERSAL

August 27, 2025

Alan Butler
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

Attorney for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amicus curiae* the Electronic Privacy Information Center states that it has no parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC regularly participates as *amicus* in this Court and other courts in cases concerning privacy rights and harmful data practices. EPIC also regularly advocates for meaningful regulation of extractive, invasive, and unfair data collection and profiling systems. EPIC is interested in this case because of EPIC's concern that the internet's digital surveillance systems rely on harmful data practices and invade users' privacy.[1]

[1] Both parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no party or party's counsel authored this brief in whole or in part nor contributed money intended to fund the preparation of this brief. No outside person contributed money intended to fund the preparation of this brief. EPIC's Legal Fellow, Hayden Davis, participated in the drafting of this brief.

SUMMARY OF THE ARGUMENT

Congress enacted the Video Privacy Protection Act ("VPPA") to provide strong privacy protections for a specific category of sensitive personal data: records of the videos (and games) that we buy, borrow, or watch. At the heart of the VPPA is a prohibition on disclosure of this sensitive personal information by video service providers to third-parties. The law, like most privacy laws, includes narrow exceptions to tailor this prohibition. But including a broad disclaimer in a privacy policy, cookie banner, or other web notice does not trigger an exception, and disclosing purchase or rental records to marketing partners in such instances is illegal.

The Defendant in this case, Ubisoft, is alleged to have disclosed the personally identifiable information of their customers to third parties in violation of the VPPA. Their defense, and the lower court's ruling, is based on a claim under the law's consent exception, 18 U.S.C. § 2710(b)(2)(B). But, in recognition of the highly sensitive nature of the data involved, the VPPA imposes one of the strictest consent standards of any federal privacy law. The statute requires that consent be written, informed and in a form distinct and separate from any other rights or

obligations. Even then, any consent must be expressly temporally limited, effective for two years at most. The lower court ignored these unambiguous requirements in the law, accepting Ubisoft's consent defense on the basis of a clickwrap agreement and cookie banner that did not inform its customers, was not distinct and separate, was not expressly temporally limited. It is not even clear based on the record that any form of (electronic) written consent was collected as to these disclosures. The lower court's ruling that the plaintiffs' complaint should be dismissed on the consent defense as a matter of law was a clear error and contrary to the statute and the record.

In fact, Ubisoft's consent solicitations were so deficient that they should not even satisfy the general consent standard applied by this Court. The data-sharing notices were so perfunctory and subtle that no reasonable consumer would infer that Ubisoft would share their sensitive purchase and viewing data with third parties. Instead of grappling with this fact-intensive inquiry, the lower court cursorily dismissed Plaintiffs' claims on consent grounds, a move that jeopardizes consumers' ability to vindicate their statutorily protected privacy rights. This Court should reverse the lower court's dismissal.

ARGUMENT

In 1987, President Reagan nominated Judge Robert Bork to the U.S. Supreme Court and sparked a high-profile standoff in the Senate. The prominent judge was known in his jurisprudence for opposing the concept of a general constitutional right to privacy under *Griswold*, and a local reporter asked the clerk at his neighborhood video rental shop to give him a copy of Bork's rental list so that he could write a story about the Judge's personality (and to make a tongue-and-cheek point about privacy).[2] The article, and its implication that any prominent figure might have their rental records subject to inspection, sparked congressional action in a way that few events ever do. The Video Privacy Protection Act ("VPPA") was signed into law on November 5, 1988, barely 13 months after the article was published in the City Paper.

The law is simple, and its purpose is clear. Any business that provides video services to consumers is obligated to protect the privacy of its users' personal information. Specifically, a provider cannot

---

[2] *See* Michael Dolan, *Borking Around*, New Republic (Dec. 20, 2012), https://newrepublic.com/article/111331/robert-bork-dead-video-rental-records-story-sparked-privacy-laws.

disclose information that "identifies a person as having requested or obtained specific video materials or services," except in limited circumstances. 18 U.S.C. §§ 2710(b)(1), 2710(a)(3). One of those limited circumstances is disclosure "with the informed, written consent" of the consumer, so long as that consent meets the requirements laid out in the statute. 18 U.S.C. § 2710(b)(2)(B). This is the strictest consent standard in any federal privacy law; a recognition of the fact that Congress viewed disclosure of video-viewing records to be an acute affront to individual privacy.

In many ways, the VPPA is the quintessential privacy statute—it aims to limit the use of private information about people by generally prohibiting disclosure and providing for narrow carve outs necessary to allow people to obtain the services they are seeking.

But the lower court in this case has turned the law on its head. The law prohibits the disclosure of Plaintiffs' personally identifiable information ("PII")—but the lower court allowed it. The law requires the consent exception to be narrowly limited to circumstances where consumers provide "informed, written consent" that is "distinct and separate" from other legal terms—but the lower court found that the

mere existence of a privacy policy referenced in a clickwrap cookie banner was sufficient to trigger the exception. And the strict consent standard under the law necessarily requires a finding of fact that the consent was both written and informed—but the lower court dismissed the suit as a matter of law under FRCP 12(b)(6). These conclusions were contrary to law and the decision below should be reversed.

I. Cookie banners and clickwrap privacy policies are not sufficient to meet the stringent VPPA consent standard.

The lower court erred when it applied a general common law or state statutory consent analysis to the VPPA claim in this case. Congress was clear that the consent standard in the VPPA is strict. The statutory protections are tailored to protect a specific subset of especially sensitive data: personal video rental, purchase, and viewing histories. The law protects this data by limiting disclosure to narrow circumstances, including when an individual consumer has provided informed, written consent (separate from general legal terms) to allow the disclosure. Ubisoft's Cookie Banner and clickwrap agreements do not come close to satisfying the law's exacting consent standard.

A. Congress required a strict consent standard in the VPPA because of the sensitive nature of personal video viewing records.

When Congress enacted the VPPA in 1988, it was clear that the purpose was to shut down the unauthorized disclosure of private information about people's video viewing habits, as had happened with Judge Bork's rental records. S. Rep. No. 100-599, at 5 (1988). The disclosure of Judge Borks rental records, even to a reporter pursuing commentary on a public figure, sparked bipartisan outrage in Congress and spurred immediate action. One lawmaker noted that the leak "seem[ed] more real than anything [he had] know[n] about the right to privacy after practicing law for 18 years." *Id.* at 5 (quoting *Hearings on Nomination of Robert H. Bork*, 100th Cong., 1st Sess. 1372 (Sept. 28, 1987)).

Congress was especially concerned with the deeply intimate and personal nature of this information. As Senator Paul Simon put it, video service provider data is "a window into our loves, likes, and dislikes." *Id.* at 7 (quoting 134 Cong. Rec. S5401 (May 10, 1988)). In the words of Congressman Al McCandless, who sponsored the first video privacy bill, "Books and films are the intellectual vitamins that fuel the growth of

individual thought . . . . This intimate process [of intellectual growth] should be protected from the disruptive intrusion of a roving eye." *Id.* at 7.

Indeed, the legislative history of the VPPA overwhelmingly shows Congress' recognition of the unusual sensitivity of video tape service provider ("VTSP") data, and its awareness that advances in technology would make it even more urgent to guarantee the privacy of such information. *See id.* at 6. The Senate Report on the VPPA situates the law alongside statutes like FERPA and FCRA, laws which protect some of the most strictly controlled and high-risk information from disclosure. *Id.* at 2.

It is unsurprising, consequently, that like FERPA and FCRA, the VPPA imposes extremely robust restrictions on disclosure. To be clear, the VPPA is a narrow, targeted statute. It applies only to a small subset of companies (video service providers), and even then it covers only PII about their customers. More than this, in recognition of the heavy restrictions it was putting in place, Congress included in the VPPA many carveouts and exceptions for disclosure "under appropriate and clearly defined circumstances," *id.* at 7, including those made to law

enforcement, to the consumer, and those incident to the ordinary course of business. Where no exception applies, however, disclosure is permitted only with the consumer's consent. And, to ensure sensitive VTSP information was protected, Congress set the bar for such consent under the VPPA deliberately high.

Specifically, for disclosures of PII to a third party to be permissible, the VPPA requires "the informed, written consent" of the consumer. 18 U.S.C. § 2710(b)(2)(B). This informed, written consent must be made in a form that is "distinct and separate from any form setting forth other legal or financial obligations of the consumer." *Id.* §§ (b)(2)(B)(i). This consent standard is far more exacting than the "reasonable consumer" standard often used by this Court in privacy cases.

As a preliminary matter, the statute requires that consent must be "written." When Congress "amended the VPPA in 2012 'to reflect the realities of the 21st Century,'" *Ellis v. , Inc.*, 803 F.3d 1251, 1253 (11th Cir. 2015) (quoting 158 Cong. Rec. H6849-01 (Dec. 18, 2012)), it clarified that informed, written consent may be made "through an electronic means using the Internet." Video Privacy Protection Act Amendments

Act, Pub. L. 112-258, 126 Stat. 2414, 2414 (2012). But this change does not replace the requirement that consent be written, it simply clarifies that written consent may be provided electronically. *See* S. Rep. No. 112-258, at 3 (2011) ("The bill . . . retains the requirement in current law that consumers provide informed written consent."); *see also* 158 Cong. Rec. H6849-01 (Dec. 18, 2012) ("[The amendment] does not change the requirement for informed, written consent by a consumer." (statement of Rep. Lamar Smith)).

In short, electronic consent is allowed, but that consent must still take the form of an affirmative act taken by the consumer in writing. To the extent that this is not unambiguous from the text, the legislative history supports the conclusion that, even after the amendments, "[t]he consumer would have to affirmatively opt in." 158 Cong. Rec. H6849-01 (Dec. 18, 2012) (statement of Rep. Mel Watt). *See also* S. Rep. No. 112-258, at 3 (2011) ("The legislation retains the privacy protections already in the law which requires that consumers 'opt-in' to the sharing of their video viewing information."). This forecloses any argument of "implied consent" or consent through inaction under the VPPA.

Written consent is not the only requirement under the VPPA though. Crucially, this written consent must also be informed. This is a high standard reserved for decisions of particular importance and requires more than what is required for mere affirmative consent. While few cases have explored the meaning of "informed consent" under the VPPA specifically, there has been considerable clarification of the term's meaning in other contexts.

At its core, informed consent can best be viewed as requiring that the consumer not only affirmatively consents to the disclosure, but that the consumer makes this consent after having been (1) provided an explanation of the nature of the act for which consent is being given and the material facts relating to it, that is (2) presented in a manner that facilitates the consumer's understanding.

For example, HHS regulations governing testing on human subjects offer a particularly clear formulation. Under these guidelines, informed consent "must begin with a concise and focused presentation of the key information that is most likely to assist a prospective subject or legally authorized representative in understanding the reasons why one might or might not want to" consent. 45 CFR 46.116(a)(5)(i).

Additionally, this information "must be organized and presented in a way that facilitates comprehension." *Id.*

This standard is consistent across various contexts in which informed consent is required. In the medical context, "informed consent" requires that the patient be "inform[ed] . . . of the nature of the operation or the extent of the harm that is necessarily involved." Restatement (Second) of Torts § 892B cmt. i (Am. L. Inst. 1979). Some courts have found that informed consent actually requires disclosure of all "significant risks" involved as well. *Id.* Some definitions go even further. In the context of attorney conflicts, informed consent typically requires that the client actually "be aware of the material respects in which" providing consent could have adverse effects on the client's interests. Restatement (Third) of the Law Governing Lawyers § 122, cmt. c(i) (Am. L. Inst. 2000).

The requirement of informed consent is essential to achieving the VPPA's purpose. The statute was adopted to "allow[] consumers to maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers." S. Rep. No. 100-599, at 8 (1988). Ensuring that consumers *understand*

what disclosures they are consenting to is necessary to give them actual control over their personal information. Without such a guarantee, this control would be illusory, constantly subject to erosion through hidden terms and byzantine contractual provisions without consumers even realizing.

Reflecting the importance of preventing inadvertent or undesired disclosures, the VPPA goes even further than requiring informed, written consent—as stringent as this already is. The statute specifically requires that the written, informed consent be "distinct and separate" from any form containing any other "legal or financial obligations of the consumer." 18 U.S.C. § 2710(b)(2)(B). This further clarifies that VTSPs cannot obtain consent through mediums in which the consumer is likely to be distracted by other obligations or issues.

In practical terms, the "plain language of the VPPA" requires that the informed, written consent be obtained through "a privacy disclosure that addresses only the use of personally identifiable information connected with video purchases and no other privacy topic," and that this be obtained "separately from the consumer's agreement to the retailer's terms of use, general privacy policy, and the commercial terms

of the purchase." *Cappello v. WalMart Inc.*, No. 18-cv-06678-RS, 2019 WL 11687705, at *2 (N.D. Cal. Apr. 5, 2019). The consent must also be temporally limited, with consent either given at the time the disclosure is actually sought to occur, or given in advance but only to last for a period no longer than two years. 18 U.S.C. § 2710(b)(2)(B)(ii). And the consumer must be given a "clear and conspicuous" opportunity to withdraw consent at any time. *Id.* §§ (b)(2)(B)(iii).

These specific and unambiguous consent requirements go beyond the general consent standard applied by this Court in privacy cases where no such special requirements are imposed. The heightened consent standard under the VPPA is a direct reflection of the deeply personal nature of the information involved, and serves Congress' clearly annunciated purpose (in both the original adoption of the VPPA and its amendment in 2012) to allow disclosure of this especially sensitive information to third parties only when such disclosure truly reflects the wishes of the consumer. The VPPA's efficacy hinges on rigorous application of its consent requirements.

B. Ubisoft's Cookie Banner and clickwrap agreements do not satisfy the strict VPPA consent standard.

Ubisoft asserts that the requisite consent was obtained through its use of a cookie banner and clickwrap agreements during account creation (with an additional referral to its Privacy Policy at checkout). Even if these separate elements are analyzed together—which they should not be, since the statute requires all consent requirements be met at the time consent is given, not over the course of a prolonged website visit—these "consent" mechanisms are wildly inadequate under the VPPA. Finding that the Plaintiffs here had given informed, written consent would not only contradict the plain text of the statute, it would also undermine Congress' stated purpose in the law and threaten to erode informed consent standards in other areas of law as well (e.g. medical consent and attorney-client relationships).

1. Ubisoft's clickwrap agreements were neither informed nor distinct and separate.

First, Ubisoft's clickwrap agreements do not meet the "informed" consent requirement in the VPPA. Ubisoft claims it obtained consent during the account creation process, because the account creation form included a pre-checked box that purported to authorize Ubisoft to

"[s]hare . . . personal and game data with select partners for marketing purposes." ER-125. This opt-out checkbox did not provide any additional explanation or information. Rather, the details of this information-sharing were buried in Ubisoft's Privacy Policy, which users were prompted to agree to by checking a single checkbox to accept Ubisoft's hyperlinked Terms of Use, Terms of Sale, and Privacy Policy. *Id.* Ubisoft claims consent was also obtained at checkout due to a disclaimer at the bottom of the checkout screen that links again to its Privacy Policy. ER-126. These bundled "clickwrap" consents might meet a basic written consent requirement, but they do nothing to ensure that consumers are informed about the terms—quite the opposite.

It is well documented that consumers seldom ever read clickwrap agreements. *See, e.g.*, Florence Marotta-Wurgler, *Does Contract Disclosure Matter?*, 168 J. Institutional & Theoretical Econ. 94, 107 (2012) (finding that only seven out of more than 4,500 surveyed participants actually followed hyperlinks to policies before consenting to them through clickwrap). A 2018 study involving over 500 participants found that 74% accepted a clickwrap privacy policy without accessing, viewing, or reading any part of it. Jonathan A. Obar & Anne Oeldorf-

Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 Info., Comm. & Soc'y 128 (2018). Even among those studied who did *look* at the policy, the vast majority did not read it, spending an average of only 73 seconds on it. *Id.* More noteworthy, 93% of participants agreed to clickwrap terms of service that included a clause promising to surrender their first-born child. *Id.* Only 1.7% of respondents noticed this provision. *Id.*

As alarming as these findings are, they are not surprising. Clickwrap privacy agreements are long and difficult to read. An analysis of the length and readability of the privacy policies of nearly 150 popular websites found that the "vast majority . . . exceed the college reading level," with many more complex than Immanuel Kant's famously dense "Critique of Pure Reason." Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. Times (June 12, 2019).[3] Furthermore, a review of over 50,000 privacy policies from 1996 to 2021 found they have been getting

[3] https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

longer and more complex over time, doubling in length in the ten years between 2011 and 2021, and quadrupling in length since 2000. Isabel Wagner, *Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996–2021*, 26 ACM Transactions on Privacy & Security 3, 1 (2023); *see also* Litman-Navarro, *We Read 150 Privacy Policies*, *supra* (noting that Google's privacy policy, as just one example, has "evolved over two decades… from a two-minute read in 1999 to a peak of 30 minutes by 2018").

Not only is it understandable that consumers do not read clickwrap privacy policies, it would not be rational or beneficial for them to do so in their current form. A 2008 study found that it would take the average American well over 200 hours (the equivalent of more than five weeks of full-time work) to read all the privacy policies they are subjected to in a single year. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J.L. & Pol'y for Info. Soc'y 543, 563–65 (2008); *see also* Irma Slekyte, *NordVPN Study Shows: Nine Hours to Read the Privacy Policies of the 20 Most Visited Websites in the U.S.*, NordVPN (Oct. 23, 2023) (a more recent estimate suggesting the number has since ballooned to over 500 hours

annually).[4] If every American actually spent their time this way, it would lead to an estimated total national cost of $781 billion annually (over $1.2 trillion today when adjusted for inflation). *Id.* at 563–65.

In sum, we know that most consumers do not read clickwrap privacy policies, and that if they were required to read them it would consume hundreds of hours of their time. Therefore, burying information in a privacy policy should not be treated as relaying to consumers the material facts necessary for informed consent.

Second, Ubisoft's clickwrap also fails to meet the VPPA consent requirement because it was not provided to users in a manner "distinct and separate" from "other legal or financial obligations of the consumer." U.S.C. § 2710(b)(2)(B)(i). The especially sensitive nature of PII protected under the VPPA requires consent to disclosure of this information to stand out. Specifically, consent must be given "in a form distinct and separate from any form setting forth other legal or financial obligations." 18 U.S.C. § 2710(b)(2)(B).

[4] https://nordvpn.com/blog/privacy-policy-study-us/?srsltid=AfmBOorMm0Snz3Q5ApO0qCPPH_vMcHp4cnbGAInnfp2sKZyvQezdouck

This was not the case here. The form containing the data-sharing and Privacy Policy checkboxes was not focused on privacy/data-sharing alone. Rather these matters were incidental to the main focus of the form—creating a user account. *See* ER-125. Since this account creation form—and even the checkbox for the Privacy Policy itself—involved the assumption of other legal or financial obligations, such as those in Ubisoft's Terms of Use and Terms of Sale, none of the consent solicitations included in this form satisfy the VPPA's consent requirements.

Ubisoft's argument that consent was given at checkout is even less availing. Here, there was no checkbox at all, but rather a reminder—at the bottom of the checkout form—about the use of personal data. ER-126. It is impossible for this disclaimer to be "distinct and separate" from the purchase transaction, since the only action taken by the consumer is the click to purchase the item. That purchase decision is not presented as a choice to disclose PII, and it certainly is not "distinct and separate" from that choice.

At no point did Ubisoft's checkboxes or other references to its Privacy Policy amount to informed, written consent of the kind required

under the VPPA consequently. Because of this, these mechanisms cannot form the consent necessary to authorize Ubisoft's disclosure of Plaintiffs' PII to third-parties.

2. Ubisoft's cookie banner did not provide informed or written consent.

Ubisoft's argument that its Cookie Banner met the VPPA consent requirement as a matter of law also falls flat because its banner did not meet any of the statutory requirements. Even if a banner could, theoretically, be used as a mechanism for obtaining the specific, informed, written consent to disclosure of video viewing data from a consumer, the evidence in this case does not support that factual conclusion and the lower court erred in finding that consent must have been present as a matter of law.

Customers who visit the Ubisoft site are presented with a banner at the bottom of their browser that provides notice regarding Ubisoft's use of cookies. ER-145. The content and format of that banner has changed over the last five years but only the most recent version of the banner (published a few days before this suit was filed) actually includes options to "accept" or "decline" the disclosure of specific personal data. ER-153. The earlier operative versions of the banner

stated that by clicking "OK" *or by proceeding to use the website* the users were consenting to data collection described elsewhere in the Privacy Policy. ER-150–ER-151 These pre-litigation banners provided notice (at best) of the existence of cookies and data collection practices that were referenced in a separate policy. They did not meaningfully inform the consumers about disclosure of viewing, purchasing, or shopping history and they did not include any mechanism for written consent.

Though the 2012 amendments to the VPPA authorized consent through electronic means, this did not weaken the fundamental requirement that consent still be both informed and in writing. While there could be a triable dispute over whether clicking "OK" constitutes written consent to any data collection specifically described in the banner, simply proceeding with using the website clearly does not. Notice accompanied by continued use is not the same as written consent. Even in contexts where written consent is *not* required, the Ninth Circuit has been reluctant to enforce "browsewrap" agreements (those where the user supposedly manifests assent simply by continuing to use the website) absent actual knowledge. *See, e.g.*, *Berman v.*

Freedom Fin. Network, LLC, 30 F.4th 849 (9th Cir. 2022); *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014).

Even where a consumer did click "OK" on the Cookie Banner, that would still not meet the VPPA consent standard because the consent was not *specific* or *informed*. Informed consent requires disclosure of material information in a manner that facilitates the consumer's understanding of this information and the decision to be made. But Ubisoft's Cookie Banner was instead designed in a way that prompted users to accept all disclosures without engaging with this decision.

This is an unfortunately common practice today. As former FTC Chief Technologist Lorrie Cranor has noted, "[t]he Web is now littered with inscrutable cookie banners that . . . use dark patterns to nudge users to [accept] all cookies." Lorrie Faith Cranor, *Cookie Monster*, 65 Comm. ACM 30, 30 (2022). "Dark patterns" are "user interfaces whose designers knowingly confuse users, make it difficult to express their actual preferences, or manipulate users into taking certain actions." Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J.L. Analysis 43, 44 (2021). Studies show that dark patterns, as subtle as they may be, are "strikingly effective in getting

consumers to do what they would not do when confronted with more neutral user interfaces." *Id.* at 46 (finding for instance that even "[r]elatively mild dark patterns more than doubled the percentage of consumers who signed up for a dubious theft protection service").

In the context of cookie banners, dark patterns manipulate consumers into accepting more data processing than the consumer would wish by making it harder to refuse than to accept. Through her lab at Carnegie Mellon, Professor Cranor tested different cookie banner designs on more than 1,000 U.S. participants. Cranor, *Cookie Monster*, *supra* at 30. Her results both confirmed the efficacy of dark patterns at manipulating consumer behavior and identified specific design features commonly used for this purpose. *Id.*

Ubisoft's Cookie Banner deployed many of these identified dark patterns. First, Ubisoft's Cookie Banner made opting in to all cookies—and accepting the disclosure of PII—the default. ER-148–ER-151. As a result, if the consumer either ignored the banner and continued to use the website or clicked "OK" to dismiss it, non-essential cookies would be used and the consumer's PII would be shared. This is particularly concerning as studies show that "when a banner sits unobtrusively at

the bottom of the screen," as Ubisoft's banner did, "many users do not interact with it, and thus end up with the website's default," which in Ubisoft's case was disclosure of PII. Cranor, *Cookie Monster*, *supra* at 30.

Even when consumers did engage with the banner, the banner was designed to draw attention to the "OK" button (accepting disclosures), which was highlighted in a different shade, rather than the "Set Cookies" button (providing a mechanism for opting out), which was made the same color as the banner itself. ER-148–ER-151. More than this, the process for opting out was designed to be more burdensome than the process for accepting. While users could easily "consent" by clicking "OK," to opt-out or limit data processing, users had to first click "Set Cookies" and then manually select which types of cookies they did and did not consent to. *Id.* This manual selection itself encourages consumers to give up and simply accept all cookies and disclosures, since the terms used to describe cookie categories are generally unclear to consumers. Only 48% of participants in Cranor's study correctly identified the definition of "performance cookies," and only 16%

correctly identified the definition of "functional cookies." Cranor, *Cookie Monster*, *supra* at 32.

Taken together, this design created a strong bias towards blind acceptance. Website users, often confused and frustrated by cookie banners, tend to "click[] whatever seems most expedient to get obtrusive cookie banners out of the way." *Id.* Users are generally far less inclined to follow a link in a cookie banner as they "do not know what they will find behind the link and how long it will take them to manage cookies." *Id.* at 31. In other words, by designing the Cookie Banner as Ubisoft did, Ubisoft drove consumers to quickly and unthinkingly click "OK" to dismiss the banner.

This is a far cry from informed consent. Clicking "OK" on, or simply ignoring, a banner that notes that cookies will be used by Ubisoft and its partners to "offer advertising adapted to your interests, collect visit statistics and allow you to use the social network share buttons," is not the same as making an informed decision to allow Ubisoft to share PII with third-parties. ER-148–ER-151. Ubisoft's Cookie Banner, which funnels consumers into giving blanket

acknowledgement of any and all data collection and disclosure, is plainly inadequate under the VPPA's exacting consent standards.

3. None of Ubisoft's purported sources of consent satisfy the VPPA's temporal requirements.

In addition to these individual shortcomings, neither source of consent asserted by Ubisoft—the Cookie Banner nor the Privacy Policy—satisfies the VPPA's temporal requirements. The VPPA requires that consent to the disclosure of PII either be "given at the time the disclosure is sought" or be "given in advance for a *set period of time*, not to exceed 2 years…." 18 U.S.C. § 2710(b)(2)(B)(ii) (emphasis added). The district court held that this did not present an issue since Plaintiffs' action was necessarily brought within two years of their consent being obtained (due to the VPPA's two-year statute of limitations). But the statute does not merely require—as the lower court seems to have assumed—that a VTSP not disclose information more than two years after consent was received. Rather, the law requires that any future consent, to support the disclosure exemption, provide the exact period of time it shall be valid for.

Ubisoft's Privacy Policy and Cookie Banner did not do this. It is a well-established canon of construction that "courts must presume that a

legislature says in a statute what it means and means in a statute what it says there." *Connecticut Nat'l Bank v. Germain*, 503 U.S. 249, 253–54 (1992). Ubisoft's failure to provide "a set period of time" for future disclosures rendered these agreements inadequate to authorize future disclosures under the VPPA.

4. There are many non-burdensome ways Ubisoft could have complied with the VPPA.

Demanding that Ubisoft and other VTSPs comply with the express requirements of the VPPA before disclosing protected PII is not unrealistic. The VPPA is not an anachronistic statute; it was forward-looking when first designed and has been specifically updated for the internet age. *See Salazar v. Paramount Glob.*, 133 F.4th 642, 660 (6th Cir. 2025) (Bloomekatz, J., dissenting) ("Congress recognized that the computer age would bring technological innovations with the ability to be more intrusive than ever before. And while it may not have anticipated all those innovations precisely . . . the VPPA was meant to protect consumers' privacy in the face of those advances, not become obsolete." (cleaned up)). There are many non-burdensome ways VTSPs like Ubisoft can obtain valid consent online.

Even tools like cookie banners could be adequate methods of obtaining valid consent, if designed and deployed fairly to prompt consumers to make an active and considered choice to opt-in, rather than by making the process of opting out so burdensome that consumers simply click away and the default assumes their consent to disclosure. To comply with the VPPA's requirements, a cookie banner should recognize that the default is no consent without a specific affirmative choice by the user.

Cookie banners should also be designed neutrally, rather than highlighting the accept option over options to refuse, and should not make the process of refusal more difficult or time-consuming than the process of agreeing. Specifically, VTSPs who wish to use cookie banners to obtain consent should provide a clearly visible option to reject all non-essential cookies/disclosures if they wish, rather than having to navigate to a separate screen to opt-in or out of specific disclosures and categories of cookies. *See* Cranor, *Cookie Monster*, *supra* at 31–32 (describing features of a "good" cookie banner).

Designing cookie banners in this way would be no more costly or difficult for VTSPs—indeed, many companies already follow these best

practices. It would also substantially reduce friction for consumers by allowing them to swiftly and easily express their genuine preferences about disclosures, or take no action at all without unwittingly surrendering their right to privacy.

It is true that this would likely lead to fewer consumers consenting to disclosure of their personal data. Studies show that "when users can just as easily select any available cookie options, they accept fewer cookies than when it is easiest to accept all cookies," and it seems natural to expect the same would be true of PII disclosures to third-parties. *Id.* at 30. This is, fundamentally, the point. The VPPA was not created to give companies as many opportunities as possible to disclose PII. It was created to prevent this practice, allowing it only in instances where meaningful—and time-limited—consumer consent had been given. If the disclosures sought by a VTSP are such that consumers would not, when presented with an actual choice, agree, then courts should not restructure the VPPA's text to lower the standard for consent. Courts should recognize that this is exactly the type of unauthorized disclosure that the VPPA was enacted to prevent.

The 2012 VPPA amendments are further evidence of Congress' intent to safeguard consumer privacy in the modern age. But under the highly lenient consent standard applied by the lower court, it is unlikely that the statute would even prevent the sort of brazen disclosure Judge Bork suffered in 1987. A company could place a broad, blanket consent authorization in its privacy policy—the sort of policy nobody, even a judge, would be expected to read—or even, apparently, *infer* consent through a consumer's use of its services, and for two years they would have carte blanche to disclose any and all PII to any parties they wish. To prevent such an absurd outcome, this Court should follow the plain text of the VPPA and honor the express intent of Congress.

II. Ubisoft's notices and disclaimers are inadequate even under the general consent standard.

Even under the more lenient general consent standard, Ubisoft's consent solicitations should not be accepted as sufficient. In common law and statutory privacy cases, this Court has recognized a limited affirmative defense of consent when "'the circumstances, considered as a whole, demonstrate that a reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization.'" *Calhoun v. Google*, 113 F.4th 1141, 1147 (9th

Cir. 2024) (quoting *Smith v. Facebook, Inc.*, 745 F.App'x 8, 8 (9th Cir. 2018)). This consent does not necessarily have to be express, but whether express or implied, it must be *actual*. *Calhoun*, 113 F.4th at 1147 (quoting *In re Google, Inc.*, No. 13-md-2430, 2013 WL 5423918, at *12 (N.D. Cal Sept. 26, 2013)).

Given the need to consider the circumstances as a whole, a court's role in determining whether a company should be able to assert the affirmative defense of consent in an online privacy case is about more than simply reviewing whether the company's privacy policy contains a disclosure that arguably describes the invasive conduct at issue. The court must evaluate what a reasonable user would understand given the full context: the nature of the service provided, the preferences and expectation of users of that service, and the promises and representations made by the company.

Studies conducted over the last few decades have shown that consumers assume privacy policies are drafted to solidify privacy protections, with a majority of consumers polled agreeing with the statement that "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users."

Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, Pew Resch. Ctr. (Dec. 4, 2014).[5]

The reasonable person inquiry is thus highly fact-intensive, making finding consent as a matter of law at the motion-to-dismiss stage inappropriate. *See Chamberlin v. BNSF Ry. Co.*, No. 22-cv-00005-RS, 2022 WL 717818, at *2 (N.D. Cal. Mar. 10, 2022) (characterizing fact-intensive inquiries as "ill-suited for resolution at the pleading stage"); *see also Americas Outlaw Spirits Inc. v. Gunn*, No. CV 12-041320 SJO, 2012 WL 12886419, at *2 (C.D. Cal. Sep. 21, 2012) (noting that fact-intensive inquiries around consumer confusion or understanding are fact-intensive and thus "ill suited for disposition on a motion to dismiss"); *Fan v. NBA Props. Inc.*, No. 23-cv-05069-SI, 2024 WL 1297643, at *3 (N.D. Cal. Mar. 26, 2024) ("Whether reasonable consumers would understand, based on the . . . Privacy Policy, that by using [the defendant's] website they were consenting to the disclosure of their personally identifiable information to Meta, is a question that should be resolved on a fuller factual record."). The routine dismissal of

[5] https://www.pewresearch.org/short-reads/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/.

privacy actions on dispositive consent grounds before a full factual record could be built—as the district court did here—would seriously undermine the ability of consumers to enforce the privacy rights granted to them by statute.

To the extent the district court *was* in a position to make a determination on consent as a matter of law in this case, it should have been in favor of Plaintiffs. Ubisoft's Cookie Banner was classic browsewrap (where a website "offers terms that are disclosed only through a hyperlink and the user supposedly manifests assent to those terms simply through continuing to use the website," *Berman v. Freedom Fin. Network LLC*, 30 F.4th 849, 856 (9th Cir. 2022))). The Cookie Banner stated that "continuing to navigate on this site," was an acceptance of the use of cookies, requiring users to follow a hyperlink to "learn more." ER-148–ER-151. This Court has been consistently, and rightfully, reluctant to recognize browsewrap agreements, accepting that browsewrap can seldom manifest assent on the part of the consumer. *Berman*, 30 F.4th at 856.

Ubisoft's other consent solicitations—both the clickwrap agreements and the Cookie Banner when consumers actually clicked

"OK" to dismiss it—while not browsewrap, are similarly inadequate. In the context of contract formation, the courts have been generally willing to recognize the validity of certain types of clickwrap, specifically those "where a website presents users with specified contractual terms *on a pop-up screen* [where] users must check a box explicitly stating 'I agree' in order to proceed," *id.*, since this style of agreement is designed to attract user attention. The clickwrap employed by Ubisoft here though was different to this. While the consumer was required to engage in an action superficially manifesting assent (clicking "OK" or checking a checkbox), albeit an extremely perfunctory one, the terms did not dominate the screen like a pop-up. Rather, the precise terms had to be accessed via hyperlink, with the link itself either tucked in the bottom of the screen or listed alongside other links next to a single checkbox in a larger form.

Indeed, the design of virtually every part of Ubisoft's clickwrap encouraged users to confirm without reading or understanding. The data-sharing checkbox was pre-checked, meaning that consumers who do not read or notice it were deemed to have agreed simply because they did not actively opt-out. The checkbox's description was also so vague as

to fail to place consumers on notice of what types of disclosures they should expect. Instead, the details were placed in Ubisoft's Privacy Policy—hyperlinked in a separate checkbox. As already discussed, it is widely recognized that consumers do not, and often could not, read privacy policies. And the mere knowledge of a privacy policy's existence does nothing to inform the consumer due to widespread misconceptions about what a privacy policy is or serves to do.

"Website users are entitled to assume that important provisions—such as those that disclose the existence of proposed contractual terms—will be prominently displayed, not buried in fine print." *Berman*, 30 F.4th at 857. Consent to the disclosure of sensitive PII, protected by numerous statutes, is an important provision. Consumers should not be expected to assume that smallprint buried in a hyperlinked privacy policy would permit the sharing of sensitive information collected on them by Ubisoft's website.

When considered in the circumstances as a whole, Ubisoft's disclosures thus would not place a reasonable consumer on notice that Ubisoft would provide their PII to third parties. As a result, Ubisoft's consent solicitations do not satisfy even the general consent standard

recognized by the Ninth Circuit. The district court was incorrect in finding adequate consent in this case, and even more incorrect to make this determination at the pleading stage.

CONCLUSION

For the foregoing reasons, EPIC respectfully urges the Court to reverse the district court's order granting Ubisoft's motion to dismiss.

Date: August 27, 2025

/s/_____

Alan Butler
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorney for Amicus Curiae
Electronic Privacy Information Center

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

This brief contains 6,998 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select one only)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[X] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-1(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length permitted by Cir. R. 32-2(b) because *(select one only)*:

- [ ] it is a joint brief submitted by separately represented parties;
- [ ] a party or parties are filing a single brief in response to a longer joint brief.
- [ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature: /s/ Alan Butler **Date**: August 27, 2025

CERTIFICATE OF SERVICE

I certify that on August 27, 2025, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the Ninth Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: August 27, 2025

/s/_____

Alan Butler
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorney for Amicus Curiae
Electronic Privacy Information Center