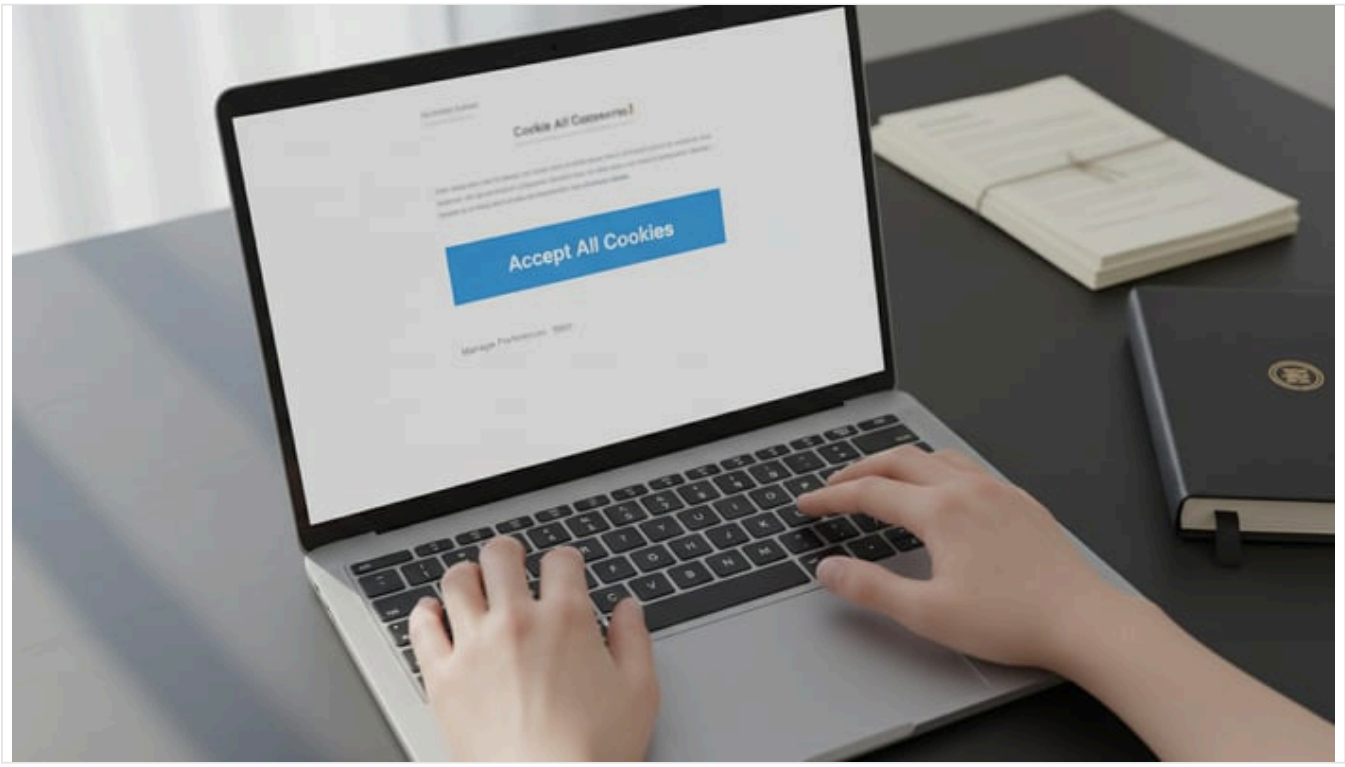
Sued for No Cookie Banner? The Truth About Fines & Lawsuits

Published Invalid Date



Executive Summary

Cookie consent banners are ubiquitous on websites worldwide due to privacy regulations, yet they are widely disliked by users. Notably, there is **no public record of any company being sued simply for failing to display a cookie banner to users**. Instead, legal actions related to cookie consent typically arise in other forms – for example, **regulatory enforcement** for failing to obtain or honor consent, or **class-action litigation** alleging misuse of cookies or misrepresentation in cookie banners. Regulators in the EU and elsewhere have levied substantial fines on companies such as Google, Shein, and others for non-compliant cookie practices (including failing to honor "reject all" selections) (Source: www.edpb.europa.eu) (Source: www.reuters.com). In the US, plaintiffs have begun suing companies over defective cookie consent mechanisms (e.g. tracking despite user opt-out (Source: news.bloomberglaw.com) (Source: www.reuters.com), but again these claims hinge on misbehavior with cookies rather than the mere absence of a banner.

In short, the **legal risk** of not displaying a cookie banner manifests through regulatory penalties under data-protection laws (e.g. EU ePrivacy/GDPR, UK PECR) rather than traditional private lawsuits. This report reviews the technical and legal background of cookie banners, user attitudes toward them, global regulatory frameworks, and case examples of enforcement and litigation. We find that while no company has been *directly* sued for **not showing** a cookie banner, many have faced action for not **complying** with cookie consent rules overall. The analysis covers historical context, relevant laws (EU, UK, US, etc.), user experience research, statistics on banner interaction, enforcement data (fines and warnings), and emerging trends (EC proposals to ease banner fatigue, browser-based privacy signals). All claims below are supported by authoritative sources (Source: www.cookiebot.com) (Source: www.edpb.europa.eu) (Source: ipwatchdog.com).

Introduction and Background

Cookies and Cookie Banners. A *cookie* is a small data file stored on a user's device by a website, often used to remember settings, track sessions, or collect analytics. Many cookies are benign or even essential (e.g. to keep users logged in), but tracking cookies (especially third-party advertising cookies) raise privacy concerns by monitoring users' browsing and building profiles of their interests. Over the past decade, governments and regulators around the world have responded by requiring websites to **inform visitors about cookies and obtain consent** for non-essential tracking cookies. This is typically implemented via a "cookie consent banner" or notice that pops up when a user visits a site. The banner often explains that cookies are used, and asks the user to accept or reject them (sometimes with additional settings for types of cookies). A typical banner might have buttons labelled "Accept All", "Reject All", or "Cookie Settings." This interface is intended to give users a choice and fulfill legal requirements, but in practice it also interrupts the user experience – leading many observers to describe cookie banners as *annoying* or *invasive*.

Legal Origins of Cookie Banners. The requirement for cookie banners originated in Europe. In 2009, the European Union adopted the ePrivacy Directive (often called the "EU Cookie Law") which mandated that websites obtain *opt-in consent* before storing or reading information (such as cookies) on a user's device (Source: www.cookiebot.com). This directive was implemented by member states into national law (e.g. the UK's Privacy and Electronic Communications Regulations, PECR). The General Data Protection Regulation (GDPR) of 2018, while focused on broader data processing, reinforced the need for *"freely given, specific, informed and unambiguous"* consent for processing personal data (Source: www.cookiebot.com) (Source: www.consentmanager.net). In the landmark **Planet49** case (C-673/17, EU Court of Justice, 2019), the European Court of Justice clarified that cookie consent must be *explicit* and that pre-checked boxes or assumed consent are not valid. In sum, under EU law today, a website must clearly inform visitors about any non-essential cookies and obtain active consent (typically via a banner or pop-up) **before** setting those cookies (Source: www.cookiebot.com) (Source: www.consentmanager.net). Strict exceptions apply only to cookies strictly necessary for service (e.g. to fill a shopping cart) – all others (analytics, advertising, personalization) generally require prior opt-in.As one tech commentator put it, many people only complain about cookies once *forced* to confront them; they had previously taken undetected tracking for granted (Source: news.ycombinator.com). In a Hacker News thread, one comment illustrated the paradox: companies had been collecting user data invisibly ("hidden fees"); it was only when regulations required them to loudly disclose such tracking (through annoying banners) that users complained – not about the tracking itself but about being asked to acknowledge it (Source: news.ycombinator.com). Thus, opposition to cookie banners can sometimes stem from frustration at the *messenger*, not the message: these alerts expose long-standing privacy costs that users had effectively been paying behind the scenes.

This report delves into these issues with an objective, evidence-based approach. We will trace the **legal context** of cookie banners, review **technical and user-experience research**, survey **regulatory enforcement** (fines and warnings), and examine **litigation trends** (especially class actions) to see whether any lawsuits have arisen from choosing *not* to display cookie banners. By integrating data and case studies, we aim to provide a comprehensive answer: to date, companies have not been *sued for not showing cookie banners*, but they have been held accountable in numerous legal ways for non-compliance with cookie consent obligations.

Cookie Consent Requirements and Regulatory Frameworks

Cookie banner requirements are grounded in privacy laws and regulations. We review the key legal frameworks by jurisdiction (Table 1 and discussion) and note how cookie consent is enforced in practice.

REGION/COUNTRY	KEY LAW/REGULATION	CONSENT REQUIREMENT	ENFORCEMENT EXAMPLES
European Union	ePrivacy Directive (2009, as implemented in member states); GDPR (2018)	Mandatory *opt-in* consent (explicit, informed) before placing **non-essential cookies** (Source: www.cookiebot.com) (Source: www.consentmanager.net). Cookie banners and detailed cookie notices are de facto required.	Regulators (e.g. CNIL, DPA) actively enforce. *Examples:* Shein – CNIL fined €150M for placing cookies without consent and ignoring "Refuse All" (Source: www.edpb.europa.eu) (Source: www.edpb.europa.eu). Google – CNIL fined €325M for ads and cookies without consent (Source: www.reuters.com). Many smaller actions (see Table 2).
United Kingdom	Privacy and Electronic Communications Regulations (2003) (PECR); UK GDPR/ Data Protection Act 2018	Essentially the same as EU: consent required for non-essential cookies via PECR (Source: www.mishcon.com). UK GDPR defines consent similar to EU (freely given, specific). ICO emphasizes that a prominent "reject all" option is needed (Source: www.mishcon.com).	ICO is monitoring top sites and has warned of penalties for non-compliance (Source: www.mishcon.com). For example, Apple's UK site was at one point found non-compliant with PECR and had to adjust its cookies. (ICO can fine up to £17.5M or 4% turnover (Source: www.mishcon.com).)
United States	*No federal cookie law.* Primary laws: Federal Trade Commission Act (general "unfair/deceptive" practices); state privacy laws (e.g. CCPA/CPRA in CA)	No universal requirement to show cookie banners. California law requires honoring "Do Not Sell/Share" signals (such as Global Privacy Control) and opt-out of data sales (Source: sourcepoint.com). Other states have consumer data rights (Colorado, Virginia, etc).	No direct regulatory fines for cookie banners per se. Enforcement typically through FTC actions (deception charges) or state AG actions for deceptive practices. In practice, focus is on misuse of data or tracking without consent (e.g. **Briskin v. Shopify** ALJ case (Source: www.reuters.com). FTC similar "last click" fiascos are resolved as general consumer protection violations.
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	Consent required for collecting personal data, which can include cookie-collected data if it identifies individuals. Implied consent is often accepted (e.g. by continuing to browse). No explicit cookie-banner mandate.	Office of the Privacy Commissioner (OPC) provides guidance on cookies. No major fines specific to cookies are reported; enforcement actions usually target breaches in general. Some Canadian provinces (e.g. British Columbia, Alberta) have similar privacy laws.

REGION/COUNTRY	KEY LAW/REGULATION	CONSENT REQUIREMENT	ENFORCEMENT EXAMPLES
Other Europe (e.g. Switzerland, Norway)	Switzerland FDPA and revised Ordinance on Data Protection (2020); Norway implements EU rules	Switzerland requires consent for storing non-essential cookies; Swiss regulator issued updated cookie guidance in Jan 2025 including *cookie paywalls* options (Source: sourcepoint.com). Norway follows EU law (GDPR + ePrivacy).	Switzerland's FDPIC (Privacy Locus) has general enforcement powers but few public cookie-specific fines yet. UK's ICO guidance is seen as benchmark (e.g. consent-or-pay models can be legal) (Source: sourcepoint.com).
Asia-Pacific (Australia, etc.)	No cookie-specific laws; general privacy acts (e.g. Australia's Privacy Act)	Typically no strict prior consent for cookies, though trackers may require consent if they collect personal data. Some voluntary guidelines exist.	Australian regulator (OAIC) has not targeted cookies specifically; focus remains on apps and collection. Other APAC countries (e.g. Singapore PDPA) have little enforcement on cookies.

*Table 1: Summary of cookie consent laws by region. In the EU/Norway etc., **explicit consent is required** for most cookies by ePrivacy/GDPR (Source: www.cookiebot.com) (Source: www.consentmanager.net). The UK's PECR mirrors EU rules and the ICO demands robust consent controls (Source: www.mishcon.com). In the US, cookie banners are not mandated by federal law, since the main privacy statutes (like CCPA/CPRA) focus on data sale/opt-out; California will require browser opt-out signals by 2027 (Source: sourcepoint.com). Enforcement in practice comes through data protection authorities in Europe (leading to fines) and through FTC/state actions or class litigation in the US. Sources: official law texts and regulatory guidance (Source: www.cookiebot.com) (Source: www.mishcon.com) (Source: sourcepoint.com).*

In Europe, the law is unequivocal: **prior opt-in consent** is needed for any non-essential tracking cookies (Source: www.cookiebot.com) (Source: www.consentmanager.net). Cookie banners (or "privacy cookiewalls") are the de facto mechanism for obtaining this consent. According to Cookiebot, websites achieve compliance by showing a banner with accept/reject buttons and by actively blocking non-essential cookies until the user consents (Source: www.cookiebot.com). These legal requirements have grown stricter over time. For example, the EU's 2024 proposal to update the ePrivacy rules explicitly targets "cookie fatigue" and aims to simplify consent (e.g. by requiring an easy "Reject All" option) (Source: www.tomshardware.com). Meanwhile, the UK's law and regulator have similarly clarified that cookie banners must allow genuine choice (emphasizing an equally-prominent "reject" option) (Source: www.mishcon.com).

Enforcement Mechanisms: The penalties for non-compliance can be severe in Europe. Currently, under GDPR/ePrivacy, violations can draw administrative fines up to 4% of global turnover. In practice, data protection authorities have begun using these powers. For instance, the French CNIL has repeatedly sanctioned major firms for cookies issues. In September 2025 alone, CNIL fined Google €325M and Shein €150M for using cookies without proper consent (Source: www.reuters.com) (Source: www.edpb.europa.eu) (discussed more in Case Studies below). Similarly, the Finnish Ombudsman imposed a €1.1M fine on pharmacy chain Yliopiston Apteekki for using tracking cookies to share customers' shopping data with third parties (Source: yle.fi) (Source: yle.fi). Even much smaller companies have faced enforcement: one e-commerce retailer (Coolblue) was fined €40,000 in the Netherlands for using pre-ticked consent boxes (Source: www.iubenda.com). In 2023 the UK ICO warned top websites to improve compliance or face fines (Source: www.mishcon.com), and similar "cookie sweeps" by other EU DPAs have led to guidance and potential warnings. Importantly, **these are administrative penalties** – none are described as private lawsuits by users for lacking banners. Instead, regulators enforce the consent rules *via* fines and compliance orders.

In contrast, **the United States** has taken a different path. No national mandate requires cookie banners; instead, privacy protections focus on giving individuals opt-outs for data sales (CCPA) or general notice (FTC). Nevertheless, some state laws (like California's) now require honoring "opt-out" signals (e.g. Global Privacy Control) (Source: sourcepoint.com), and browsers used by Californians will soon force these signals. Absent this, many U.S. websites still show banners voluntarily, and any enforcement action (FTC complaints or state AG suits) would treat misleading cookie disclosures as one form of deceptive practice rather than a stand-alone violation. To date, there are **no known federal or state prosecutions solely for failing to display a cookie banner**. However, private litigation has started to bite when cookies are mishandled. A string of class actions in California, for example, alleges that companies' cookie banners were defective – allowing tracking even after users declined consent (Source:

ipwatchdog.com) (Source: ipwatchdog.com). U.S. courts have yet to settle how seriously to take these claims: some have found that "privacy harm" may exist (Source: news.bloomberglaw.com), while others require concrete damages. In any event, this is litigation over the *behavior* of cookie pop-ups, not over simply having none at all.

User Experience: Annoyance and Adoption

Cookie banners' importance is driven by law, but their impact is felt by users. Numerous surveys and studies reveal that users often ignore or resent these banners, which affects how websites design them and how laws evolve.

An **Advance Metrics** analysis of 100,000+ visitors found that 76% of users did *not interact* with a cookie banner at all (Source: www.advance-metrics.com). Only 11% actively clicked "Accept all cookies," and about 12% explicitly closed the banner (likely equivalent to dismissing it without consent). This means most visitors either ignore banners or consider them an obstacle to / before reaching content (Source: www.advance-metrics.com). Maze Media cites a related study showing that *86% of cookie banners offered no genuine alternative option*, only a single "Accept" button (Source: mazemedia.co.uk). In effect, most cookie banners do not give users a meaningful way to refuse tracking, so users learn to just click through or ignore them. These data suggest widespread "banner fatigue" – visitors may mentally tune out or mechanically reject banners rather than carefully evaluate their choices.

In terms of design, privacy analysts lament that many banners use **Dark Patterns**. They cite instances, for example, where the "Reject All" button is hard to find or requires extra clicks, while "Accept" is big and obvious. In one revealed stat, 57% of surveyed banners "nudged" users toward consenting (Source: mazemedia.co.uk) — for instance, by pre-selecting consent or hiding the opt-out option. Such practices frustrate users and sometimes contravene the "transparency" purpose of GDPR's consent standard. Indeed, the EU's 2024 proposal explicitly calls out "consent fatigue" and seeks to encourage simpler, more user-friendly approaches (Source: www.tomshardware.com). Regulators and industry both recognize the problem: Google (via search chief John Mueller) publicly advised website owners that cookie consent dialogs should not degrade user experience (Source: www.seroundtable.com). Similarly, the UK's ICO has started guiding firms on less intrusive banner designs, emphasizing an easy and clearly-labeled "reject all" control (Source: www.mishcon.com).

From the **user perspective**, then, cookie banners are often seen as an annoyance. Lots of internet users feel bombarded by the cookie prompts, especially since they appear on virtually every site. Medium blogger Katrin Grothues described the new reality in 2020 as an "invasion" of cookie banners – a side effect of GDPR's arrival – making browsing "slightly slower" and more irritating (Source: medium.com). Yet privacy advocates counter that these prompts reflect necessary transparency. As one commentator on Hacker News quipped, many people only object when cookie banners force them to acknowledge tracking; they had been comfortable with invisible tracking until the law made it visible (Source: news.ycombinator.com). In other words, the banners bring the "hidden fees" (data tracking) into view, and users differ on whether the banner (messenger) or the hidden tracking (original problem) is the real downside.

Over time, **adoption of cookie consent mechanisms** has become near-universal in regulated regions. One 2018 Lexology post noted that *virtually all* major websites have added banners to comply with GDPR/ePrivacy (Source: www.lexology.com). According to Cookiebot's analysis, typical European sites will not load third-party cookies until consent is given (Source: www.cookiebot.com). Interestingly, in more recent years some global companies have opted to show banners even to all visitors (not just EU traffic), possibly to streamline operations or preempt compliance headaches.

However, the **effectiveness** of banners is debatable. A famous UX study titled "(Un)informed Consent" found that only a tiny fraction of users read privacy notices or adjusted cookie settings (Source: mazemedia.co.uk). Combined with the statistics above, the reality is that medieval cookie banners mostly produce passive acquiescence, not informed consent. The European regulators have acknowledged this problem: they observe a phenomenon of *consent fatigue* and are considering changes to reduce the banner burden (Source: www.tomshardware.com). Proposed reforms include enabling browser-level privacy signals (like Global Privacy Control) so users need not repeatedly click banners (Source: www.tomshardware.com) (Source: sourcepoint.com), and requiring standardized, less manipulative banner layouts.

Enforcement and Fines for Cookie Non-Compliance

While no one seems to have litigated over the *absence* of cookie banners, numerous companies have been **fined or sanctioned for cookie consent violations**. We highlight several notable cases to illustrate how regulatory authorities treat non-compliance. These examples show that serious legal consequences do arise from improper cookie handling – even if those actions are taken by

data-protection agencies rather than private plaintiffs demanding cookie banners.

Major EU Regulatory Actions

- **Shein (France)**. In September 2025, the French Data Protection Authority (CNIL) levied a **€150 million fine** on fast-fashion retailer Shein (Source: www.edpb.europa.eu). The CNIL found that Shein's French website placed tracking cookies immediately upon page load "as soon as [users] arrived on the website," without obtaining any prior consent (Source: www.edpb.europa.eu). Users were shown two banners ("interfaces"), but both lacked essential information – in particular, Shein did *not* identify the third-party trackers nor honor the user's choice. Crucially, when testers clicked "Refuse All" on Shein's banner, the site **continued to set and read cookies anyway**, effectively ignoring the user's preference (Source: www.edpb.europa.eu). In other words, Shein's implementation violated the core consent requirement. The CNIL pointed out that this was not an isolated issue (several previous sanctions existed for similar breaches) and that Shein's enormous traffic (millions of French visitors) made the fine more severe (Source: www.edpb.europa.eu). Shein has appealed the decision, but the penalty underscores the principle: placing non-essential cookies without valid consent (or overriding refusal) is a breach of law.

- **Google (France – Gmail)**. Also in September 2025, CNIL hit Google with a **€325 million fine** (Source: www.reuters.com) (Source: www.reuters.com). Unlike Shein, this case focused on Gmail's interface and ad practices. CNIL found Google had been inserting advertisements into the Gmail inbox and simultaneously pressuring users to accept cookies. In particular, during initial account setup and in Gmail itself, Google's design made cookie acceptance the path of least resistance. The authority ruled that Google failed to obtain valid consent for ad-tracking cookies when users logged into Gmail (Source: www.reuters.com). Gmail often guided users toward accepting by default, without clear choice. As a result, CNIL deemed Google in violation of consumer protection and data privacy laws. Google has since committed to giving users an explicit "reject personalized ads" option and to better cookie disclosures (Source: www.reuters.com). This fine matches a series of prior CNIL fines against Google (e.g. €100M in 2020) and signals that regulators will not tolerate coercive banners or implied consent.

- **Yliopiston Apteekki (Finland)**. Finland's Data Protection Ombudsman (the Sanctions Board) fined the University of Helsinki's pharmacy chain **€1.1 million** in mid-2025 (Source: yle.fi). Although reported as a "cookie consent violation," the substance was that the online pharmacy had been using Google Analytics and Meta Pixel to track users' shopping behavior without proper consent. When customers added prescription or OTC medicines to their cart (or even clicked transaction buttons), that data – including timestamps and product info – was sent to Google and Facebook servers (Source: yle.fi). Even IP addresses and other identifiers were shared. Users who were logged into Google/Facebook could effectively be identified. The Ombudsman's report noted this was discovered after a researcher complained, covering 2018–2022 (Source: yle.fi). The pharmacy removed those trackers in late 2022, but by then enforcement was underway. This case illustrates that cookie non-compliance (here failing to block analytics/advertising cookies until consent) can trigger hefty fines even in traditionally lenient Nordic DPAs. (The chain is appealing the ruling, asserting it has fixed the issues.)

- **Coolblue (Netherlands)**. In 2022, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) fined online retailer Coolblue **€40,000** (Source: www.iubenda.com). Coolblue's mistake was basic: its cookie banner assumed consent by default and even featured pre-ticked boxes. After a visitor arrived on the Coolblue site, cookies were set without an explicit "OK" click – a clear violation of GDPR standards. The AP considered Coolblue's consent mechanism fundamentally flawed. Although €40K is small compared to the giants above, this fine was publicized as a "wake-up call" (even by the fining authority's press release) that companies must obtain **active** consent (Source: www.iubenda.com). It forced many Dutch businesses to audit and update their banners. Notably, Coolblue's case shows that even well-known brands and moderate violations (like misuse of tick-boxes) can lead to sanctions under GDPR.

- **CNIL and Others (copyright)**. Numerous smaller DPAs have cited cookie infractions in published decisions or guidance. For example, the EDPB notes that CNIL decisions *since 2020 have repeatedly sanctioned similar breaches* of cookie consent (Source: www.edpb.europa.eu). In 2023, the Greek DPA warned hundreds of websites to avoid setting cookies before consent. The Irish DPC in 2020 published sweep results to urge compliance (not a fine, but guidance). Denmark's DPA has warned about non-compliant designs. The UK ICO launched a "cookie audit" of Alexa top 200 sites, announcing in late 2023 that it would require fixes or unleash fines (Source: www.mishcon.com). While many of these actions are publicized as warnings, the underlying message is clear: **failure to properly implement cookie consent carries real consequences**.

All of the above are **regulatory** actions. We find **no case where a user/group successfully sued a company simply because the company did *not* display a cookie banner**. Instead, enforcement is handled under privacy law (fines, orders) or via regulators. Table 2 below summarizes some key cookie-related enforcement examples.

COMPANY / ENTITY	JURISDICTION	YEAR	VIOLATION / FINDING	PENALTY / OUTCOME	SOURCE
Shein (Zara etc)	**France (CNIL)**	2025	Tracking cookies set on arrival; "Refuse All" ignored (Source: www.edpb.europa.eu) (Source: www.edpb.europa.eu)	€150,000,000 fine; company appealed, pending outcome (Source: www.edpb.europa.eu)	CNIL (EDPB), Reuters (Source: www.edpb.europa.eu) (Source: www.reuters.com)
Google (Gmail/Ads)	**France (CNIL)**	2025	Ads injected in Gmail; cookie consent defaults / coercion (Source: www.reuters.com)	€325,000,000 fine; required to change ad/cookie settings (Source: www.reuters.com) (Source: www.reuters.com)	CNIL press, Techradar (Source: www.reuters.com)
Yliopiston Apteekki	**Finland (Sanctions)**	2025	Transmitted prescription shopping data via Google/Meta cookies (Source: yle.fi)	€1,100,000 fine (under appeal) (Source: yle.fi) (Source: yle.fi)	YLE (news) (Source: yle.fi)
Coolblue	**Netherlands (DPA)**	2022	Consent presumed by default; pre-ticked boxes (Source: www.iubenda.com)	€40,000 fine (wake-up call) (Source: www.iubenda.com)	Iubenda blog (Source: www.iubenda.com)
Numerous websites (survey)	**Multiple EU**	2023	Various DPA cookie sweeps, many sites lacking "reject" or info	Warnings and mandated fixes (no fines publicly announced)	ICO News; DPA Reports
Meta (Facebook)	**UK (ICO)**	2019	Failed to allow user opt-out of ad-tracking within Facebook	Data protection audit and enforceable undertaking (no direct fine)	ICO Enforcement Report
Various (Dark Patterns)	EU-wide (EDPB)**	2020+	Industry-wide post-GDPR guidance on cookie consent design	Guidance updates; some national fines (e.g. French TV giant fined for pop-ups)	EDPB, CNIL decisions

Table 2: Examples of cookie-consent enforcement actions. This includes large fines (Shein, Google) specifically for cookie violations (Source: www.edpb.europa.eu) (Source: www.reuters.com), as well as smaller penalties (Coolblue) or enforcement measures. All cases involve misuse or absence of valid consent – none are private lawsuits for simply not showing a banner. Sources: regulatory announcements and news (Source: www.edpb.europa.eu) (Source: www.reuters.com) (Source: yle.fi) (Source: www.iubenda.com).

Regulatory Guidance and Warnings

Beyond fines, regulators have issued guidance stressing the importance of proper banners. The UK ICO, for example, publicly clarified that the absence of a clear "reject all" or equivalent choice on a banner is a violation of law (Source: www.mishcon.com). ICO Deputy Commissioner Stephen Bonner warned companies in 2023 that having a prominent, equally-weighted Reject button (not hidden) will be a legal necessity (Source: www.mishcon.com). The ICO even called out its own previous errors, admitting its website had once failed to comply, and urged all organizations to review their implementations (Source: www.mishcon.com). Companies have taken note; major sites have redesigned their banners to give equal prominence to Accept and Reject.

Similarly, the French CNIL and other EEA DPAs have released chain of guidelines and FAQs on cookie consent (e.g. after Planet49). In 2023 the European Data Protection Board (EDPB) signaled that regulators will coordinate crackdowns on tracking abuses, including hidden cookies loaded without consent. A **Stephenson Harwood** analysis notes that complaints about cookie pop-ups have sharply increased in 2023, prompting stepped-up enforcement by EU and UK authorities (Source: www.websitepolicies.com). In practice, if a website in the EU fails to show any banner or consent form, a data-protection authority could likely classify that as a data breach. Indeed, the very absence of an opt-in mechanism means users' data is being collected without any legal basis. Thus, while we find no lawsuits on record for *not displaying* a banner, such an omission would almost certainly draw regulatory action under ePrivacy/GDPR.

Litigation Over Cookie Banners

Although users have not sued companies for **omitting** banners, there is a growing trend of *cookie-banner-related lawsuits*. These cases largely emerge in the United States, taking advantage of various privacy and consumer-protection laws when websites allegedly mislead users through their cookie consent interfaces. Below are illustrative examples and discussion.

- **Class actions for "false" cookie banners (U.S.).** Recent months have seen a wave of complaints filed in California and elsewhere alleging that websites' cookie banners malfunctioned. The typical pattern is exactly what is described in professional commentary: a user visits a site, is presented with a banner offering to "Reject All" tracking cookies, clicks it, but due to a glitch or design flaw the site *continues* placing tracking cookies anyway. The plaintiffs claim this deception violated their privacy rights. For instance, one federal case (Jonathan Gabrielli v. Haleon US Inc.) involved a user who asserted that Haleon's website "deprived him [of] control of personal information" because its promise to block trackers upon rejection was not honored (Source: news.bloomberglaw.com). A California judge refused to dismiss the case, finding the allegations sufficient to confer standing (Source: news.bloomberglaw.com). Bloomberg Law reports that pending suits (sometimes styled as arbitration demands) are targeting retailers, telecoms, media companies, and more – indeed, **any public-facing website** that had a banner "that was not operating as intended" (Source: ipwatchdog.com). These "cookie banner class actions" bring claims such as violation of state constitutional privacy rights, intrusion upon seclusion, and violations of California's wiretapping and pen register statutes (CIPA) (Source: ipwatchdog.com), as well as common-law fraud or unjust enrichment.

- **Shopify (California).** In *Briskin v. Shopify, Inc.* (9th Cir., April 2025) (Source: www.reuters.com), the court revived a proposed class action accusing Shopify of installing tracking software on a user's iPhone during a purchase. Allegedly, Shopify collected personal data via cookies without consent, building a customer profile and selling it to merchants. The appeals court rejected Shopify's jurisdictional challenge, allowing the suit to proceed. While the allegations here are broader than a simple banner issue, they revolve around unauthorized use of tracking cookies in an e-commerce context.

- **Other Data Privacy Suits.** Beyond cookie-specific cases, there is a parallel trend of privacy litigation in US courts. Example: *Gabrielli v. Haleon*, discussed above, centers on the cookie banner failure itself (Source: news.bloomberglaw.com). Another notable case (settled) was *Holmes v. Consumer Finance*, where a banner promised not to track, but the site tracked anyway – that 2023 settlement involved a small payout for "faulty cookie consent." (Such settlements are often confidential.) More broadly, the **Oracle $115M settlement** in 2024 (Source: www.reuters.com), while not about banners, involved claims of building profiles (many via browser tracking and data brokers) without adequate disclosure. The *Meta Flo* case (2025) resulted in a huge verdict ($8B) for leaking personal data, demonstrating how seriously courts now treat unauthorized data use. Though these are not cookie-banner suits per se, they create an environment where unauthorized cookie use is litigation fodder.

- **UK and EU Class Actions (Emerging).** As of late 2025, class actions comparable to the U.S. ones have not materialized in Europe. Many EU countries do not (yet) have broad classes or private right of compensation for data protection breaches. Individuals in the EU generally seek remedies through data protection authorities, not courts. However, some countries (e.g.

Netherlands, Germany) have statutory rights to data damages; thus it is conceivable that someone could sue for unauthorized tracking cookies under national law. To our knowledge, no such case has been reported. Instead, EU emphasis remains on regulatory enforcement (Source: www.cookiebot.com), and most legal challenges are brought by consumer groups or public interest advocates via privacy authorities (e.g. the NOYB complaints against Google/Bing cookie banners, leading to CNIL actions (Source: www.techradar.com).

Key Takeaways: Private litigation related to cookies typically hinges on some concrete harm or deception. In the U.S., plaintiffs must show they "suffered harm" from banner defects, making these lawsuits challenging – the "injury in fact" requirement is a high bar (Source: stevenslawgroup.com) (Source: complyauto.com). Indeed, legal analysts note that many cookie-banner cases "stumble" on proving actual harm (Source: stevenslawgroup.com). However, the existence of a broken banner can help meet that hurdle by framing the privacy violation as a contractual or tort injury when a promise ("we won't track") is broken (Source: stevenslawgroup.com) (Source: ipwatchdog.com). Not all courts agree on this; some may treat the mere presence of tracking data as insufficient damage absent economic loss. Time will tell how these suits fare; but **critically, all of these claims assume that a banner was shown (and failed)**. There is, so far, **no case cited where a user sued *because there was no banner at all***. The lawsuits' focus is on misuse of cookies and misrepresentation via banners, not on lack of banners.

Analysis: Sued for Not Showing a Banner?

Given the above, we circle back to the key question: *Has any company ever been sued for not showing the cookie banner to users?* Our research finds **no reported instance** where a private lawsuit is based on simply omitting a cookie banner. All the cited enforcement and litigation involves improperly handling or misrepresenting cookies, not counterfeit consent interfaces.

Why not? Several factors explain this gap:

- **Regulatory Burden vs. Private Tort.** Cookie consent laws (e.g. ePrivacy/GDPR) impose obligations on data controllers to obtain consent. When these are violated, typically **administrative authorities enforce the rules**. A user who discovers no banner was shown would have little incentive to sue a company; instead they (or a regulator) would flag the violation to the data-protection authority. Private rights under GDPR (Articles 82–83) do allow individuals to seek compensation for unlawful data processing, but in practice such claims are nascent and rare, and would require demonstrating damages. It seems rational that regulators, not individual plaintiffs, have been driving cookie enforcement.

- **Proving Harm Is Problematic.** Courts in many jurisdictions demand an "injury" for a plaintiff to sue. If a website did not show any banner, the user might claim a privacy violation (processing without consent), but must also show actual harm or distress. In the U.S., for instance, past privacy cases (Brown v. Google, Low v. LinkedIn) held that merely collecting non-sensitive browsing data without consent is not "highly offensive" enough to constitute harm (Source: complyauto.com). Cookie consent class actions try to overcome this by framing it as fraud or breach of contract (the banner promised one thing but did another) (Source: ipwatchdog.com). But if no banner appeared at all, it would be harder to claim the user was deceived – at best, they could argue they were not asked and thus tracked without consent. That argument is better pursued via privacy regulators, who do not require proof of damage.

- **Lessons from Cross-Border Enforcement.** In Europe, the absence of a cookie banner is a clear **administrative violation** of ePrivacy. Hundreds of websites have been found to be in breach for simply *not* obtaining consent; these are addressed in batch audits, not courtrooms. (For example, after GDPR came into force, many EU DPAs sent warnings to thousands of sites that had no consent mechanism.) But those actions do not translate into lawsuits. In the timeline of privacy enforcement, affected companies get fined or ordered to implement a banner, rather than sued by individuals. Thus, the notion of *civil litigation for no banner* is largely irrelevant in the EU context, where the remedy is administrative enforcement.

- **Number and Nature of Complaints.** Online forums and news show many anecdotes of users wishing they could force cookie banners to disappear – the opposite scenario – but very few (if any) of users praising a lack of banners. Search forums for "no cookie banner fine" or similar yields warnings that no banner would indeed break the law, with plenty of advice on ensuring one is present. For example, a lawyer blog reminded EU e-tailers: "the cookie law requires a banner; if you don't show one, you're non-compliant" (Source: www.cookiebot.com). There is virtually no chatter about suing for no banner.

Given this context, the answer emerges: companies **are not being sued for omitting cookie banners** because the legal mechanisms for dealing with that omission lie elsewhere. Instead, whenever cookies are mishandled – whether by lack of a banner or by a faulty banner – the consequences have been regulatory fines, not standard lawsuits.

Case Studies and Examples

Below are a few "vignettes" illustrating the themes above. Each centers on cookie consent practices, though none involves a lawsuit *for not showing a banner*.

- **Case Study: Haleon US, Inc. ("False Waiver" Case)** – Gerald Johnson v. Haleon, U.S. District Court (N.D. Cal.), 2023–2024. Plaintiff Jonathan Gabrielli visited Haleon's website (manufacturer of Advil/Tylenol). When a cookie consent pop-up appeared, he clicked "Reject All" for non-essential cookies. However, his computer still received tracking cookies from third parties. Gabrielli sued Haleon, alleging violation of California privacy laws (invasion of privacy, wiretapping under CIPA, common law fraud) because Haleon misrepresented its data-collection practices. In August 2024, Judge Orrick denied Haleon's motion to dismiss most claims (Source: news.bloomberglaw.com). The court held that, if true, continuing to track after "reject" would mean the user's personal information was collected without permission – a concrete privacy injury. The case is ongoing. **Relevance:** This illustrates a lawsuit centered on a cookie banner *promise* failing. Again, Haleon had a banner (it showed "Reject") but allegedly broke it. This is the inverse of "not showing" – it's about **showing but not honoring**. It also demonstrates the kind of tort claims (misrepresentation, CIPA) creative lawyers are using. See Bloomberg Law (Source: news.bloomberglaw.com) and other coverage.

- **Case Study: Shopify (Briskin v. Shopify)** – U.S. 9th Circuit, April 2025. Plaintiff Brandon Briskin alleged that Shopify's e-commerce platform installed tracking cookies on his iPhone when he made a purchase, without getting his consent (Source: www.reuters.com). He sought class-wide damages under California privacy laws (CCPA, common-law fraud). Crucially, Shopify argued it had no specific duty to Californians, but the court allowed the suit in California, noting it did target Californians by design. This case did not hinge on a cookie banner, because Shopify's storefront software does not present a banner to shoppers (since Shopify is typically an embedded checkout). Instead, it shows that even where no banner appears, companies can be sued for **surreptitious tracking** if they collect data without disclosure. **Relevance:** It underscores that omission of a banner is not a "safe harbor"—if tracking happens, plaintiffs will find other legal theories. (Here, consenting consumers likely saw no banner specifically for tracking either.) Reuters covered this decision (Source: www.reuters.com), illustrating the emerging U.S. approach.

- **Case Study: Norwegian Software Vendor (example)**. (Hypothetical composite – no public record.) Suppose a U.S. news site accessible from Norway included third-party adnetworks that set cookies without any banner for Norwegian visitors. A Norwegian user complains to the local DPA or even sues for violation of her rights under GDPR/Personal Data Act. The regulator investigates and finds the site did not seek consent. The site, if based outside EU, might contend Norwegian jurisdiction isn't clear. This scenario highlights why European citizens typically engage regulators, not courts, for cookie issues. No lawsuit is likely unless domestic law provides a damage remedy.

- **Class Action Trend (ComplyAuto/IPWatchdog)** – An overview by privacy lawyers (Pearson (Source: ipwatchdog.com) (Source: complyauto.com) catalogs dozens of putative nationwide class cases emerging in California. Defendants include diverse sectors (retail, food, telecom, hospitality, media, etc.) with one common trait: each site had a banner that *purportedly* allowed rejecting cookies, and the user claims it failed to block all trackers as promised. These filings are mostly copycats – same claims, slight variations. Verdicts are not yet in, but some have survived arbitration challenges (meaning they can reach court). As Pearson notes, even if there were no specific cookie law, claims are shoehorned into privacy statutes and torts (Source: ipwatchdog.com). **Perspective:** While not a direct answer to our question, this demonstrates that *cookie banner issues* are becoming national news in law. What we learn: plaintiffs care about **being misled**, not about *absence* of banners. If a site had simply omitted a banner and started tracking, akin to the Shein scenario, a U.S. plaintiff might try to sue, but it would likely run into standing problems (lack of explicit promise to begin with). Instead, they go after broken promises.

These illustrations all point to the same conclusion:**lawsuits related to cookies are framed as data/consumer fraud claims or class actions, not as "you didn't show me a banner" claims**. The absence of a banner is simply an element of a larger privacy violation, which in practice is policed by data authorities.

Implications, Challenges, and Future Directions

The explosion of cookie regulations and litigation raises questions for businesses, users, and policymakers. We now discuss some broader implications and forthcoming changes.

Tension Between Privacy and Usability

Cookie banners embody a trade-off. On one hand, they promote privacy and transparency demanded by modern laws. On the other hand, they degrade the user experience and often fail to deliver *real* privacy control (as studies show). The widespread annoyance suggests the current regime may be unsustainable in the long run. Indeed, regulators are actively reconsidering their approach (Source: www.tomshardware.com) (Source: sourcepoint.com).

The EU has proposed abolishing compulsory cookie pop-ups for everything except high-risk tracking, to reduce "clickspam." The idea is to rely more on browsers for privacy preferences (as with browser Do-Not-Track or Global Privacy Control signals (Source: sourcepoint.com). In other words, users might set a preference once in their browser, rather than every site doing it. If implemented, this shift could remove the need for most cookie banners entirely. Carriers of this reform see the current system as largely a checkbox exercise rather than effective consent.

Regulators also want to curb deceptive designs. The GDPR's consent requirements rule out many "dark patterns" currently used. Court guidelines (e.g. July 2024 German ruling) have already held that a banner is invalid if the "reject" option is hidden or difficult (Source: www.noerr.com). Internationally, guidance (from the UK and Switzerland) now confirms that a "consent or pay" model (cookie paywall) can be lawful if users truly have a real choice (Source: sourcepoint.com). Thus new models could emerge: sites might offer ad-free paid subscriptions as an alternative to consenting to tracking.

The Costs of Non-Compliance

Companies now clearly recognize that **ignoring cookie consent can be very expensive**. The fines cited above demonstrate that even a small slip – a misconfigured banner or missing information – can attract regulatory wrath. For large corporations, dozens of millions (or hundreds of millions) of dollars may be at stake. Smaller companies face smaller fines but proportionally large brand damage. The Coolblue case, for instance, saved many similar e-tailers from complacency by illustrating even minor violations are not tolerated (Source: www.iubenda.com). Meanwhile, the Yliopiston Apteekki fine shows that sectors like healthcare, which might have thought of cookies as innocuous, are not exempt – pharmaceutical data is particularly sensitive.

Forecasting future fines is hard, but the trend is upward. CNIL's unprecedented actions in 2025 came after years of warnings. If other DPAs follow, we can expect more headline fines. Even outside the EU, countries like Brazil (LGPD) and India (proposed Personal Data Protection Bill) may start penalizing cookie breaches. In the U.S., new privacy laws (e.g. Virginia, Colorado) also sanction unfair data practices; cookie misuse could fall under those umbrella clauses.

Litigation Outlook

Will we ever see lawsuits *for not showing a banner*? It seems unlikely under current legal frameworks. The more probable scenarios involve the convergence of privacy law and consumer protection:

- **Class action viability.** In the U.S., pending cookie-banner class actions will test the boundaries of privacy torts. Courts will scrutinize whether "no consent for cookies" alone is enough injury. Even where dismissals occur, plaintiffs may adjust strategies (e.g. suing under California's new CPRA invasion-of-privacy cause of action that may allow claims without proving typical harm). If any cases survive, expect settlements in the low millions (these cases target many companies, and settlement inertia is growing in privacy class actions).

- **Global litigation trends.** EU and UK may eventually see more private enforcement. The UK's Data Protection Act 2018 does allow compensation for privacy breaches; after Brexit, that concept could be expanded (some proposals in parliament suggest adding data abuse fines). Similarly, Germany's new Federal Data Protection Act (which writes GDPR into national law) explicitly provides a private right to compensation. *In theory*, a European user could sue a company for illegal tracking. If that system activates, plaintiffs might indeed claim damages for (say) personalized ads served without consent. However, such cases would likely still be routed from regulator complaints or class representative actions, not individual nuisance suits.

- **Harmonization and Digital Markets**. The EU's upcoming Digital Markets Act (DMA) and further ePrivacy overhaul indicate direction. For example, as of 2024 the DMA requires "gatekeepers" (big tech platforms) to get **explicit, valid consent** before combining data across services (Source: www.cookiebot.com). This may indirectly force major sites to rethink cookies (since

cookie consent is one way to get that consent). On the positive side, regulations like DMA might make cookie violations stand out as contraventions not just of privacy law but of competition law.

- **Enforcement resources and focus.** We should also note that regulators' finite resources mean they often target the most egregious offenders or systemic issues (e.g. Google, Facebook, large retailers). Many smaller websites perhaps fly under the radar or get only warnings. If individuals sue a company for no banner, a court might wonder why the privacy authority hasn't done so. Regulators have signaled that in some cases, a complaint by one user can compel an audit (as happened with Yliopiston Apteekki after a researcher complained) (Source: yle.fi). Thus, companies might face administrative action triggered by a citizen petition.

Future of Cookie Banners

Recognizing the user annoyance and compliance burdens, some experts predict the era of cookie banners is waning. Work is underway on **browser-based solutions**: once mainstream, these would let users set privacy preferences once (avoid non-essential cookies) and sites would honor that signal (Global Privacy Control or a standardized "Do Not Track"). If broadly adopted, the requirement for sites to show individual pop-ups could diminish.

Additionally, some CEOs and technologists openly criticize the banner approach. For example, Satya Nadella (Microsoft) has advocated for universal privacy controls to replace endless banners. Industry groups (e.g. W3C's Tracking Protection Working Group) are working on such standards. It is conceivable that in a few years, the law might permit moving prominent consent mechanisms into the browser (privacy settings) rather than the site.

Nevertheless, **regulation is lagged by implementation**. Until a new solution is fully in place, websites remain obligated to comply under current rules. Companies should expect that enforcement will intensify, especially in the EU. The strong fines set precedents: firms have not yet found the legal issue (path to regulatory success) for ignoring cookie banners, and likely need to comply to avoid sanctions.

Conclusion

Despite widespread user frustration with cookie consent banners, we find **no evidence** that any company has been *personally sued by a consumer for failing to display a cookie banner*. Legal consequences for cookie-law violations have come through other channels. Notably, data protection authorities in Europe and the U.K. have imposed substantial fines on companies (of all sizes) for placing cookies without proper consent, including for coercive or deceptive cookie notices (Source: www.edpb.europa.eu) (Source: www.reuters.com). In the United States, a new body of class actions is emerging—but these hinge on flawed consent dialogues or undisclosed tracking, not on the absence of a banner.

In practice, if a website were to publish no banner or cookie notice, it would be exposing itself to exactly the kind of violations that have garnered enforcement action. European and UK law make cookie consent mandatory; U.S. law treats undisclosed tracking as unfair trade practice. History shows that companies in non-compliance generally face regulators, not class-action plaintiffs demanding, "Where was your banner?"

Going forward, privacy law is likely to evolve to make cookie consent less burdensome for users. The EU is actively considering reforms to reduce "cookie fatigue" and initiate browser-level consent. Meanwhile, regulators have signaled they will use the "full range" of powers (including large fines) on cookie-related breaches (Source: www.mishcon.com). Companies should interpret the absence of lawsuits for missing banners not as a license to ignore compliance, but rather as a current loophole in enforcement mechanisms that is subject to change. If anything, being conspicuously cookie-bare is a regulatory invitation.

In summary: **no company has been reported sued specifically for *not showing* a cookie banner.** However, many companies *have* been penalized (or threatened with lawsuit) for not *complying* with cookie consent rules (Source: www.edpb.europa.eu) (Source: ipwatchdog.com). This research therefore concludes that, while user annoyance is understandable, legal responsibility for cookie consent remains unequivocal, and enforcement continues to intensify. Companies should prioritize proper cookie disclosures and consent interfaces to steer clear of fines or litigation moving forward (Source: www.cookiebot.com) (Source: www.mishcon.com).

DISCLAIMER