INSIGHTS
Privacy Technology | SUMMER 2026

iab. LEGAL AFFAIRS & PUBLIC POLICY

CMPs, Server-Side, & CIPA: How newer technology can help with older laws

Introduction



Many businesses run on data, and data increasingly runs on consent. Collecting that consent is a challenge, as organizations must ensure that their practices meet local, national, and global privacy compliance. However, regulatory guidance, enforcement actions, and court rulings can immediately change what compliance looks like, sometimes overnight. The European Union continues to issue General Data Protection Regulation (GDPR) enforcement decisions that reshape how consent and data flows must be handled. Meanwhile, in the United States, new state privacy laws have been coming into effect nearly every quarter since 2023.

Though sometimes, even laws from over 50 years ago can show up in court cases, leading to a different interpretation and understanding of privacy laws that have rippling effects into data collection practices, as is the case with the California Invasion of Privacy Act (CIPA).

Navigating complex and ever-changing privacy laws is one of the main reasons organizations with online presences look towards the right technical solutions to keep up. This edition of Privacy Technology Insights explains how Consent Management Platforms (CMPs) and technologies like server-side tagging, in addition to good risk mitigation plans, can help navigate evolving regulations.

What are CMPs?

As a refresher, a CMP is a software solution that helps businesses manage the collection and documentation of user consent on their websites and apps. CMPs display consent notices, collect and store user choices, and integrate with downstream systems to support lawful data tracking and to communicate the permitted uses of that data.

Originally, consent management referred specifically to the healthcare industry whereas in the European Union, the digital landscape changed significantly when the EU Cookie Directive was enacted in May 2011. Websites were legally required to notify users that they used cookies. This resulted in the first wave of basic notification banners and plugins, but these tools were often rudimentary and merely informed users rather than collecting explicit consent. The adoption of the GDPR in 2018 began requiring explicit, affirmative opt-in consent before personal data could be processed. This led to the creation of solutions dedicated to displaying privacy banners and collecting consent.

What Is Consent?

In the digital advertising ecosystem, consent generally refers to a consumer's choice about whether and how a website or app may collect, use, or disclose information about them. The process of collecting, storing, and honoring user choices depends on the applicable law and the type of data processing involved.

An **opt-in** model requires the user to take an affirmative action, i.e., provide consent, before certain data collection or processing begins, while an **opt-out** model may permit processing unless the user asks for it to stop or exercises a specific privacy right. CMPs help operationalize these requirements by presenting the appropriate choices, recording the user's selection, and translating it into signals that other technologies can follow. We will use "consent" throughout this Insight to mean the opt-in/out status of the individual.

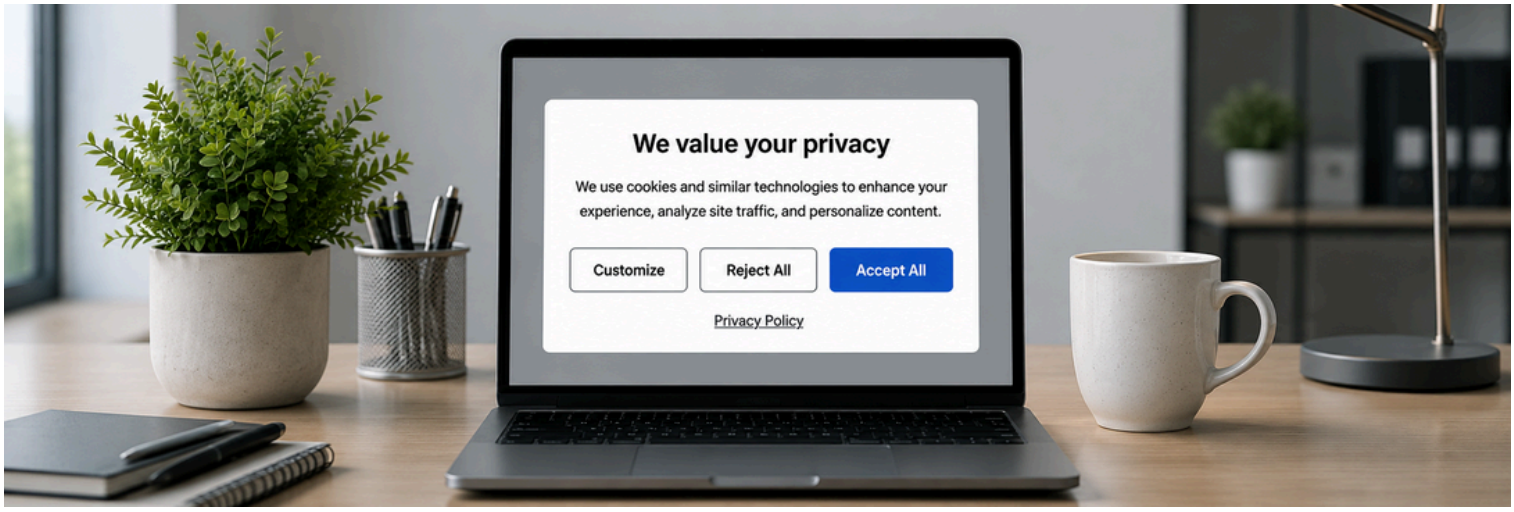
What are the "layers" to a typical CMP?

Most CMPs have three distinct layers: 1) what the user sees, 2) what's happening underneath the surface, and 3) what's happening behind the scenes, in addition to the logging of records:

The UI layer:

The UI layer is what the user sees when they navigate to your website, usually in the form of a consent banner. Banners should be configured to display information about the type of tracking technologies you have on your website. Additionally, the banner should provide users with the ability to choose the optional trackers to which they consent.

CMPs let you configure the consent experience depending on where the user is located. CMPs read the user's IP address and browser locale signals, meaning that you can ensure you are providing the correct choices and information to the user based on the regional or national regulation.



Logic and storage layer:

As the user interacts with the consent banner, the CMP maps user choices into defined purposes (analytics, ads, profiling) and records the outcome, along with a timestamp, a version number, and an identifier.

When a user accepts all or opts in to trackers and cookies, this layer collects the appropriate data and passes it along to the signal layer. When a user decides to opt out or reject all trackers or data collection, CMPs don't just delete that visit, it stores the information but sets key fields to zero. It's then on the CMP to purge existing 3rd-party cookies from the page and to suppress firing of signals. This also applies to any user using a Universal Opt-Out Mechanism (UOOM). Certain CMPs are also capable of using stored information across devices and platforms by connecting across all web, mobile, and CTV properties. This means that a user's choices are honored no matter what device or platform they use to access an organization's domains. However, this requires the user to be logged in and authenticated.

Signal layer:

The signal layer happens behind the scenes, turning the user's website visit into actional data. This is where third–party data sharing happens, passing along certain signals in the following order:

1. String encoding: Upon capturing the user's selection, the platform converts these preferences into a string, which is a machine-readable format of the metadata from the user's visit. The metadata includes what the user consented to, timestamps, and other data such as purpose-based permissions, bitfields, and CMP identifiers. Depending on the CMP, the user's location, the type of data, or other factors, a different string is used:

a. Transparency and Consent (TC) string: Primarily for areas under GDPR and ePrivacy jurisdiction, this string encodes user consent status for specific data processing purposes and advertising vendors in the EU.
b. Additional Consent (AC) string: Supplemental to the TC string that stores consent choices for Google-approved ad technology partners that are not registered on other approved vendor lists.
c. Google Consent Mode String: A simplified signal used natively by Google tags and analytics that translates user choices into binary states that is easily used by other Google systems and partners.
d. Global Privacy Platform (GPP) string: This string streamlines privacy, consent, and preference signals across a wide variety of global and regional frameworks to meet multiple regulatory requirements.
e. Multi-State Privacy Agreement (MSPA) string: Designed to align with the highest common denominator of U.S. state privacy laws, this string standardizes privacy choices to be used collectively rather than on a state-by-state basis.
f. US Privacy String: Used for state-level privacy laws in the United States, this condensed string communicates user choices regarding the sale or sharing of personal information. This string was depreciated in 2024 in favor of GPP strings, but still may be used by some CMPs.

2. Tag manager reading: Your website's tagging system reads the string on each page load via the CMP's Javascript API. The tag manager uses the string to decide on which tags to fire and to which third-party vendors based on the consent and preference choices of the user.
3. Ad calling: When your website's ad server makes an ad call to the supply-side platform (SSP), it is required to append the string to the request. SSPs automate the placement of ads on your website. If your ad server does not pass the string forward, every downstream vendor in the auction is effectively operating without the user's consent signal.
4. Bid requesting: The SSP broadcasts the ad bid request to potentially hundreds of demand-side platforms (DSPs), which are systems that allow advertisers to manage and operate their digital ad campaigns. Each DSP must parse the string and determine whether it holds a legitimate basis for the intended processing.
5. Upon receiving the bid request, the DSP checks if it has consent for different purposes, such as displaying personalized ads or creating an ad profile. If not, the DSP can determine whether or not to even bid on request or to bid without using personal data.

Records and auditability:

Across every stage of that process, the CMP should act as a persistent ledger, maintaining essential metadata such as the TC string, precise timestamps, platform versioning, and unique session or device identifiers. These logs serve as the primary defensive evidence required under some privacy laws, such as GDPR Article 7[1], and are increasingly being used in defense litigation for alleged violations of state privacy or wiretapping laws .

While regulatory bodies frequently demand these records during audits, their effectiveness is inextricably linked to the platform's implementation. Ensuring a CMP's logging capabilities is recommended when choosing a CMP.

What is server-side tagging?

As part of the collection of user data, websites use tags to track user behavior, organize content, or display specific content. Traditionally, tags are client-side, meaning that the tagging scripts run on the user's web browser. Server-side tagging runs those scripts on a separate server, sending all signals to the tagging manager first before being shared with third-parties. Not only does this provide a faster webpage experience for users, it also gives you more granular control over how tagging data is ingested and sent to third parties.

Server-side tagging has actually been around since the early days of the internet. Website activity tracking was strictly server-side. Companies analyzed raw HTTP server access logs to understand visitor counts, referrers, and basic device information. As web page technologies advanced, tracking switched to client-side, taking advantage of Javascript tags to better understand user habits. With that came an influx of third-party tags that were great for marketing teams and ad agencies, but eventually brought tagging technology into the light of privacy concerns.

Tagging managers are an important part of the consent process, sitting between the CMP and third-party vendors. Traditional or custom-made tagging managers use client-side execution because it is easy to implement and does not require complex infrastructure. However, since the tagging scripts run on the client's browser, third-party scripts can fire before being vetted by the CMP and the tagging manager, which is a compliance risk. Add in the growing usage of ad blockers and increasing restrictions on third-party cookies, and you have companies looking for solutions that take advantage of server-side tagging technology. Here's a breakdown of server-side tagging:



Browser event:

When a user intends to visit your webpage, the browser they are using sends a single HTTPS request to your domain and your domain only. This is known as an event. With client-side tagging, HTTPS requests would also be sent out to third-party vendors immediately from the user's browser, such as google-analytics.com or facebook.com, containing lots of event information. With server-side tagging, all collected information from the browser event is sent to a server container that can be connected to your CMP.

Consent enforcement:

Before any tagging data is forwarded, the server reads the consent signal. If a user has consented to analytics but not advertising, only the analytics tag fires. This enforcement happens server-side, meaning it cannot be bypassed by the user's browser state or overridden by a vendor script running client-side.

Data transformation:

Different vendors expect different tagging information. For example, Google Analytics wants the parameter of a webpage event, while Meta's Conversions API wants the webpage event with a hashed email. With server-side tagging, you can handle any data properties and translations in the tag manager, meaning that you can give third-party vendors exactly the information they need to be most effective without sharing anything unnecessary.

There are a few different types of transformation that server-side tagging tag managers do:

- Normalization: The first thing the server-side container does with an incoming event is normalise it into a standard internal format. Browser events arrive inconsistently depending on the device or browser provider, meaning that different tag setups send different field names, different casings, and different data types. The container resolves all of this into a single canonical event model before any other processing occurs.
- Enrichment: The tagging server can append data to the event that the browser alone could not reliably provide, such as accurate geolocation from the IP address, device classification, server-validated timestamps, and first-party identifier information. The information provided by the CMP and the tagging manager is more reliable than client-supplied values. For example, the user cannot manipulate their IP-derived country the same way they can manipulate a JavaScript variable.

- Redaction: One of the most critical parts of transformation is the removal of data before forwarding. Server-side tagging allows you to be extremely precise with what data each vendor is permitted to receive. Redaction includes truncating IP addresses before passing them to a vendor, hashing raw user IDs with pseudonymous tokens, or even deleting fields entirely.
- Schema mapping: Once the data has been normalized, enriched, and redacted, the event and event data is mapped into the specific format required by each third-party vendor. Every vendor typically has a different expected payload structure, essentially asking for different data or data formats. The server-side container handles data transformation centrally, so your engineering team defines the event once and the container maps it to each vendor's format, rather than each vendor's tag doing its own interpretation on the browser. This gives you greater control over which information is shared with each vendor without having to configure separate tags for every single vendor.

Server-to-server sharing:

Once the tagging information has properly gone through your tagging manager, information is shared to vendor APIs over server-to-server HTTP calls. Since third-party vendors never receive a request from the end user's browser, only from your tagging manager, the following happens:

- Vendor JavaScript never loads in the browser, so page performance improves and vendor scripts cannot access browser APIs (cookies, local storage) directly.
- Because calls are made from your server, you have a complete log of exactly what was sent to each vendor, with timestamps, which is a crucial audit trail for demonstrating compliance.
- Ad blockers and privacy-focused browsers have no mechanism to block these calls, since they originate from your infrastructure rather than the client.

Logging:

A good server-side tagging manager logs every vendor call made by the server-side container with full provenance: the original event, the string that authorised the call, the transformation steps applied, the final payload sent, the vendor endpoint, the HTTP response code, and a timestamp. The server-side log is what a publisher would produce in response to a regulatory investigation or litigation discovery request asking to demonstrate that consent was honoured.

Compliance considerations for CMPs and server-side tagging

It's extremely important to call out that using CMPs and server-side tagging managers do not automatically make your websites compliant. While these tools can help, what matters is that your implementation of the technologies are done so in a manner that meets the regulatory requirements of where your users are located. While many CMP providers are knowledgeable about privacy laws and regulatory developments, expertise can vary, and so it is critical that CMP implementation teams work with their legal counsel to validate the configuration of such tools. Compliance can be achieved or missed through configuration and governance during implementation.

However, compliance is not a one and done tweak to your practices. It must evolve, just as laws and regulations evolve. As you may know, over the past few years, California courts have been open to hearing plaintiffs' efforts to extend CIPA beyond its wiretapping origins. Hundreds of cases have been filed seeking statutory damages under CIPA, claiming that various modern technologies fall under the spirit of privacy invasion. The filed motions argue that these technologies allow companies or their third-party vendors to intercept[2] user interactions without consent. Different cases have brought up different website technologies, such as:

- third-party tracking pixels and software[3],
- cookies and identity profiles[4],
- application programming interfaces (APIs)[5],
- and website analytics[6].

These cases have brought up various arguments and theories regarding website technologies that are worth bringing up:

Dark patterns:

The term *dark pattern* is used to describe a user interface that technically offers user choice, but is designed in a way to influence the user towards a preferred outcome. For example, some websites may make the "accept all" button much larger and brighter in their consent notice in an effort to collect more information from a user. Other times, websites may make it more difficult to reject non-essential cookies. It's important to note that your CMP may not have parameters in place to ensure your consent banner does not feature a dark pattern, and even if it does, it's still on you to ensure that you are providing unbiased choices to your users.

Pre-consent firing:

When a website's tracking scripts execute and transmit user data on page load before the user has interacted with a cookie consent banner, this is known as *pre-consent firing*.

Under strict privacy laws like GDPR and CIPA, consent must be obtained prior to any data collection or interception. Whether this data collection is malicious or due to improper configuration of tagging scripts, regulatory bodies have not been shy to dish out fines for violations[7] and courts have not always been prone to dismiss claims.

Aiding and abetting:

The aiding and abetting theory has arisen from some CIPA class-action lawsuits, targeting companies that use third-party technologies such as live chat, session replay, or ad-tracking pixels. Plaintiffs have argued that any website running those software are aiding and abetting in allowing third parties to wiretap their conversation[8].

With these challenges, many organizations turn to privacy software like CMPs, not just to stay compliant, but to also ensure that the data they collect is still usable. Some techniques that you and your teams can use to take advantage of CMPs and server-side tagging to help protect yourself from any CIPA violation claims and continue collecting user data with the right consent are outlined in the next section.



Mitigating risk with CMPs and server-side tagging

Given the variances in the application of CIPA and the rest of the evolving privacy laws, even well-intentioned organizations can run into risks when it comes to collecting user data, even with consent collection in place. As such, the following practices can help mitigate some of that risk when used in combination with CMPs, server-side tagging managers, and qualified legal and privacy teams:

Be Transparent:

The first step towards compliance starts with being honest about your data collection practices. Not only is this a requirement in most data privacy laws, but it's also a crucial step to building and maintaining trust with your users.

You can use CMPs to provide transparent privacy notices that break down data collection into understandable and well-known categories (such as analytics and marketing). These notices can be dynamic, meaning that they automatically show when a user visits your website for the first time. Perhaps the most notable feature of CMPs, though, is easily providing users with the options for consenting to data collection. They also automatically track all of a user's choices, honoring their consent choice each time they visit your website in the future.
Clear, accurate disclosures about what is being tracked and honoring user choices are the first steps towards both compliance and building user trust.

Localize Consent:

Privacy laws vary greatly depending on where users are located. Given how easy it is to navigate to different webpages from anywhere, it's important to provide the right consent notices and options to users based on where they are visiting from. CMPs can simplify that struggle by automatically detecting a visitor's location and deploying the appropriate, legally required consent banner and language. You can manage multiple regional privacy laws simultaneously, ensuring that your users receive the correct notices and options that apply to where they are located.

Choose a CMP that has comprehensive coverage for various global privacy laws, helping ensure that any of your website visitors from around the world receive the proper consent notices and choices.

Keep Good Records:

Comprehensive recording-keeping is good advice for any business or industry, but particularly any business collecting user data. One of the most defensible approaches to all privacy laws is to operationalize consent and keep clean records.

A proper CMP proves its worth by helping you maintain clean, compliant data records through automating the collection, centralization, and verification of user consent. It eliminates manual tracking by providing a single source of truth for your user data collection operations. Every user interaction (consent, rejection, or partial choice) is recorded and stored in tamper-proof databases in the form of logs. These logs detail exactly what the user agreed to, when they did so (timestamps), and which valid regulation applied. With features like cross-device and cross-domain syncing, CMPs can retain authenticated users and securely link their preferences across multiple devices and domains, ensuring that consent records are recorded and updated consistently without fragmentation.

Tag managers can also provide extensive activity logs of what tagging information was shared, who it was shared with, and other event information. These logs are not only helpful for debugging or tracking performance, but can help prove compliant practices in the face of an audit.

Share Data Properly:

No matter what type of information you collect, it's important to understand with whom you are sharing that data. Since your webpage is the catalyst for collecting and sharing information, you are responsible for how that information is used. Consistently validating vendors, checking tags, and updating your cookie policies are all important steps to ensure proper data sharing transparency and practices.

Since CMPs and server-side tagging managers give you more control over how data is collected depending on consent, they enable you to ensure you share only the data you intend to share. You can remove sensitive information at the server before it ever reaches any third parties.

Standardize with TCF and GPP:

Recognizing that CMPs needed a common language to communicate consent signals across the broader advertising supply chain, the IAB developed the Transparency and Consent Framework (TCF).

The TCF is a standardized protocol for certain provisions of the ePrivacy Directive and the GDPR that defines how consent and legitimate interest signals are encoded and passed between publishers, CMPs, and third-party vendors such as advertising agencies and measurement providers. More recently, the IAB developed the Global Privacy Platform (GPP), which extends the TCF concept to the US through a single technical standard, the U.S. National Approach.

While voluntary, participation in IAB-registered frameworks can create a contractual and operational accountability chain. These standards bring together cross-industry partners to work together in their privacy practices, providing better experiences for users while maintaining proper compliance. Many CMP providers and third-party vendors utilize strings and formats, like the ones mentioned above, that have been set by the IIAB, not only making the process of sharing data more efficient, but also easier to do so in a manner that respects the privacy rights of users everywhere.

Conclusion

CIPA is just one of the many privacy laws that organizations collecting user data have to worry about, and the recent diverging rulings in California courts do not offer any clear distinction on how organizations should react. Rather than remain guessing and potentially face future allegations, it's best to partner with a CMP provider with experience navigating privacy legislation. Not all CMPs are created equal, so choosing a CMP provider that supports server-side tagging integration, as well as IAB's TCF and GPP, is highly recommended.

From a data protection perspective, CMPs and server-side tagging do not reduce your obligations. You remain the data controller and the one responsible for any data collected from your users. These technologies and tools give you greater capability to honour consent decisions programmatically and greater accountability because you hold the full event log. Regulators such as the CNIL have indicated that server-side configurations can be more privacy-respectful, but only if the consent enforcement logic is correctly implemented. A server-side container that fires all tags regardless of consent signal is no more compliant than a client-side one. No matter how great your privacy software is, no compliance tool eliminates all legal risk. Working with qualified legal counsel alongside your privacy tools is always recommended.

References

[1] Regulation (EU) 2016/679 (General Data Protection Regulation)
[2] CIPA (Penal Code § 631 et seq.)
[3] *Camplisson v. Adidas Am., Inc.*, 2025 WL 3228949 (S.D. Cal. Nov. 18, 2025).
[4] *Riganian v. LiveRamp Holdings, Inc.*, 791 F. Supp. 3d 1075, 1080–81, 1090–94 (N.D. Cal. 2025).
[5] Doe *v. Tenet Healthcare Corp.*, 789 F. Supp. 3d 814, 836–840 (E.D. Cal. 2025).
[6] *Smith v. Google, LLC*, 735 F. Supp. 3d 1188, 1193, 1196–1200 (N.D. Cal. 2024).
[7] *American Express fined €1.5 million by CNIL.*, Délibération SAN-2025-011 du 27 novembre 2025
[8] *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073 (C.D. Cal. July 15, 2021); *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021); *Johnson v. Blue Nile, Inc.*, 2021 WL 1312771 (N.D. Cal. Apr. 8, 2021).

Author



Michael Lanoie
Product Marketing Manager
Didomi