COMPLYAUTO

CNCDA California New Car Dealers Association CELEBRATING 100 YEARS

A Dealer Guide to Online Tracking & Cookie Consent Management

By Mark Sanborn and Chris Cleveland

April 2024





Table of Contents

1. Introduction
2. Background on Cookies and Similar Technologies
    A. Cookies
    B. Tracking Pixels
    C. Scripts
    D. Fingerprinting
    E. Other technologies
    F. Cookies as Covered Personal Information
3. Legal Theories Targeting Online Tracking Practices
    A. Wiretapping Claims under the California Invasion of Privacy Act
    B. Federal and Other State Wiretapping Claims
    C. State Laws Relating to Privacy and Personal Information
    D. FTC enforcement actions
    E. Video Privacy Protection Act ("VPPA")
4. Solutions and Approaches to Consider to Reduce Risk
    A. Cookie Consent Management
    B. Privacy Policy Disclosures and Transparency
    C. Advertising Providers, Service Providers, and Settings to Limit Data Use
    D. Arbitration and Class Action Waiver Strategy
    E. Practical Considerations and Recommended Steps for Dealers
    F. Businesses Fighting Back

Appendix 1: Website Cookie Compliance Checklist

Appendix 2: Website Cookie Screenshots

Copyright © 2024 ComplyAuto Privacy LLC. All rights reserved.

1. Introduction

In the rapidly evolving digital landscape, auto dealerships face a myriad of challenges and opportunities when it comes to engaging with customers online. The use of cookies, tracking technologies, and other online tools has become essential for understanding consumer behavior, optimizing marketing efforts, and delivering personalized experiences. However, the deployment of these technologies is not without risks, particularly in light of growing concerns over data privacy and the legal implications of wiretapping and personal data compliance.

This comprehensive guide aims to provide auto dealerships with the knowledge and strategies necessary to navigate the complex world of online tracking and data privacy.

By delving into the technical background, functionality, and dealership-specific use cases of cookies and tracking technologies, this guide will equip dealerships with a solid foundation for making informed decisions about their online practices.

The guide begins by exploring the various types of cookies and tracking technologies commonly used by dealerships, including first-party and third-party cookies, tracking pixels, scripts, fingerprinting, and other related technologies. It examines how these tools are employed to collect and analyze user data, personalize content, and streamline sales processes.

Next, the guide delves into the legal theories targeting online tracking practices, such as wiretapping claims under the California Invasion of Privacy Act ("CIPA"), similar laws in other states, and the Federal Wiretap Act. It also explores the application of state privacy laws, such as the California Consumer Privacy Act ("CCPA"), and their impact on the collection, use, and sharing of personal information obtained through online tracking. The guide also examines recent enforcement actions by the Federal Trade Commission ("FTC") and the potential applicability of the Video Privacy Protection Act ("VPPA") to dealership online practices.

Building upon this legal foundation, the guide provides practical solutions and approaches for dealerships to consider in order to reduce their legal risk. It delves into strategies for obtaining effective consumer consent, implementing transparent privacy policies, and managing vendor relationships. The guide also explores the potential benefits and drawbacks of implementing arbitration agreements and class action waivers.

Throughout the guide, readers will find practical considerations and recommended steps for dealerships to take in order to align their online practices with legal requirements and best practices. By providing a comprehensive overview of the legal landscape and offering actionable insights, this guide serves as an valuable resource for auto dealerships seeking to harness the power of online tracking while minimizing legal risk and protecting consumer privacy.

COMPLYAUTO

2. Background on Cookies and Similar Technologies

In today's digital landscape, auto dealerships increasingly rely on various online tools and technologies to engage customers, optimize marketing efforts, and streamline sales processes. Among these technologies are cookies and related tracking mechanisms, which have become essential for understanding consumer behavior and delivering personalized experiences online.

However, the use of these technologies is not without its challenges, particularly in light of growing concerns over data privacy and the legal implications of wiretapping and personal data compliance. This section will provide information about the technical background, functionality, and dealership-specific use cases of cookies and tracking technologies.

A. Cookies

A note about terms in this guide. In Section 2A, we introduce and define cookies alongside several distinct but related technologies that perform similar functions in the context of online tracking. These technologies, while technically different from cookies, share the common purpose/ability of collecting user data for various purposes, such as personalization, analytics, and targeted advertising.

To maintain clarity and conciseness throughout this guide, we will employ the term "cookies" as an umbrella term encompassing these additional technologies and website tracking technologies in general. This expanded scope allows us to discuss the overarching concepts, implications, and legal considerations surrounding online tracking without repeatedly listing each individual technology.

A website cookie is a small text file set by a website or server and stored on the user's computer by the web browser while the user is browsing (though they may be stored well after a user is done browsing the website that set the cookie). Cookies are designed to be a reliable mechanism for websites to remember stateful information (such as offering an online shopping cart) or to assist in recording the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). They can also be used to remember pieces of information that the user previously entered into form fields, such as names, and addresses. When the user revisits the website that initially placed the cookie, the browser transmits the cookie back to the website's servers and makes it available to scripts running in the browser, along with information the cookie collected and stored.[1]



[1] *See, e.g.*, Federal Trade Commission, Internet Cookies, https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies (archived at: https://perma.cc/7P8G-EN3G).

B. Tracking Pixels

Tracking pixels, also known as "pixel tags" and "web beacons," are small images or lines of code embedded on a website. Users cannot see the tracking pixel and may not know that they exist. Tracking pixels are used to track user behavior and the pixels can monitor and transmit various types of data from a webpage, including personal data, user interactions with a webpage, items purchased, and information entered into forms on the site. The information that the tracking pixel obtains can be used by the website owner for their internal purposes, it can also be shared with third parties such as marketing companies to target specific audiences and messages.[2]



C. Scripts

Website scripts, primarily written in JavaScript, are essential components of modern websites that enable interactivity, functionality, and data collection. Like cookies, these scripts can be first-party, created by the website owner, or third-party, provided by external services (like analytics platforms or marketing providers). Scripts can perform various tasks, such as handling user interactions (like loading accessibility tools), dynamically updating content, and tracking user behavior. Tracking scripts can gather information such as page views, clicks, form submissions, and user demographics.

Tag managers, like Google Tag Manager or Adobe Tag Manager, are tools that simplify the management and deployment of scripts on websites. Instead of directly embedding multiple scripts in the website's code, tag managers provide a centralized interface where website owners can configure and deploy various tags (scripts) without modifying the website's source code. When a user visits a website with a tag manager, the tag manager script loads along with the webpage and fires the configured scripts based on defined triggers and rules.

The tag manager then fires the configured tracking scripts based on defined triggers and rules. For example, a tracking script for an analytics platform may be triggered on every page view, while a marketing script may be triggered only on specific pages or when a user interacts with a particular element. The tag manager ensures that the appropriate scripts are executed at the right time and in the right context.

Tag managers provide a streamlined way to add, remove, or update tracking scripts without requiring direct code changes on the website. This enables website owners to quickly implement new tracking functionalities, test different scripts, and maintain a clean and organized codebase. Tag managers also offer features like version control, debugging tools, and user consent management, making it easier to comply with privacy regulations and give users control over their data, however this requires website owners to be proactive to ensure that their tag-manager consent settings are up-to-date.

---

[2] *See, e.g.,* Federal Trade Commission, Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking (archived at: https://perma.cc/6B26-ACTT).

D. Classification of Cookies, Pixels, and Scripts

Classification of Cookies, Pixels, and Scripts is important to understanding how they are used and how they should be treated in the context of wiretapping and personal information compliance. These technologies are first categorized by who places them or who is intended to receive information from them (first-party vs. third party), and secondly by their purpose. (The term "cookie" will be used in the generic context for the remainder of this section, as an umbrella term encompassing tracking technologies in general.)

I. First Party and Third Party Cookies

First-Party Cookies are those that are created or placed by the website that the user is visiting.

Third-Party Cookies are those that are created or placed by a third party. Third-party cookies may be used to transmit data to a third party that is not the website owner. Often third-party cookies are used to track the user's activities across different websites.

This guide uses a holistic approach to define if a cookie is classified as "first-party" or "third-party" including the domain that creates the cookie; the cookie's domain attribute; and the domain of the server to which network requests that transmit information related to the cookie are sent. Accordingly, under this approach, even cookies with a first-party domain attribute may be classified as a "third-party cookie" if the cookie is set by, used by, or shared with a third party.

Note that it is possible to disguise a third-party cookie as a first-party script on a website, and dealers need to ensure that their website companies and other vendors notify them about what cookies and scripts are loaded on the website and how they are used so they can be properly classified.

II. Cookie Purpose Categories

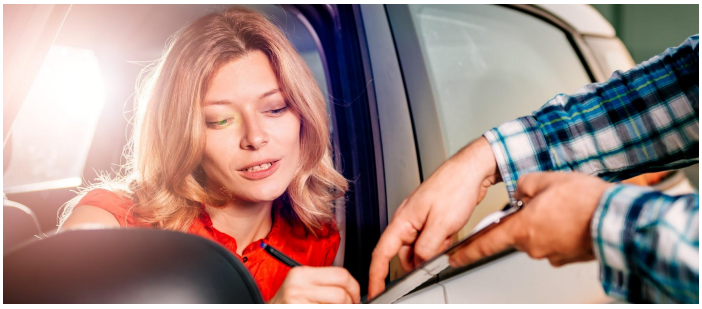
There are two basic categories of cookies, essential, and nonessential cookies.

Essential Cookies are critical for the functioning of a website. These cookies enable basic features such as page navigation, access to secure areas of the website, and setting region information. Essential cookies are typically used to maintain a user's session, store authentication information, enable website shopping cart carts, comply with state or federal laws (e.g., accessibility or cookies preferences), and ensure the security of transactions. Without these cookies, a website may not work, or may not be able to provide certain basic services or features, and its performance may be affected.

Nonessential Cookies are those that are not strictly necessary for the basic functioning of a website but are used to enhance the user experience or collect data for analytics, advertising, or other purposes. These cookies often enable "optional" website features or third-party integrations, such as live chat modules, social media sharing buttons, or personalized content recommendations. It is important to note that while nonessential cookies contribute to the overall functionality and user experience of a website, they are not critical for the website to load and function properly. In the absence of these cookies, the website will still be accessible, but certain features or enhancements may not be available or may have limited functionality. While the website may not operate as smoothly without some of these optional functions, the website will still load.

Nonessential cookies can be further subcategorized as follows:

- Functional Cookies: These cookies allow websites to remember choices made by the user, such as language preferences, login details, or region selection, to provide a more personalized experience. These cookies also allow optional functionality, like chat modules, payment calculators, and service scheduling tools, to be personalized or function correctly. Functional cookies are also used to improve the functionality of the site, such as by tracking errors.



- Marketing Cookies: Marketing cookies consist of two subcategories of cookies:
  - Analytics Cookies. These cookies that collect and transmit analytics and statistical information about how visitors use a website. These cookies help website owners understand how visitors interact with their site, but without tracking users across websites. The information gathered may include the number of visitors to the site, the pages they visited, the average time spent on the site, and the referring websites. This data is then used to improve the website's performance, content, and user experience. By analyzing visitor behavior, website owners can identify areas that need improvement, optimize their site for better engagement, and make data-driven decisions to enhance their online presence. It is important to note that while classified under a marketing umbrella in this guide, not all analytics cookies are used for marketing or advertising purposes.
  - Targeting Cookies. Also known as targeted advertising cookies and cross-context behavioral advertising cookies, these cookies are used to deliver advertisements that are more relevant to users based on their interests and browsing behavior. These cookies collect information about a user's online activities (including by uniquely identifying the user and/or user's browser and device), such as the websites they visit, the pages they view, and the links they click. This data is then used to create a profile of the user's interests, which allows advertisers to display targeted ads that are more likely to be of interest to the individual. They are also used to limit the number of times an ad is shown and to help measure the effectiveness of advertising campaigns. Targeting cookies can also be used for retargeting, where ads for previously viewed products or services follow the user across different websites. The purpose of targeting cookies is to improve the effectiveness of online advertising by showing users ads that are more aligned with their preferences and interests.

Some cookies are temporary, and deleted after the user's session ends ("Session cookies"), and other cookies remain on the user's device for a predetermined length of time, beyond the user's session ("Persistent cookies").[3] Pixels are generally marketing and analytics, but it is possible for them to be functional in certain circumstances.

Cookies can be managed and deleted through browser settings, but as noted above, this may impact the functionality of certain websites.

[3] *See, e.g.*, Federal Trade Commission, Internet Cookies, https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies (archived at: https://perma.cc/7P8G-EN3G).

A breakdown of the types of cookies appears in the table below:

	Cookie Purpose Name	Other Common Names	Definition / Examples
	Essential	Strictly Necessary	Required to enable essential website functions. They are necessary for (among other things) secure site access, maintaining shopping cart contents, and ensuring compliance with state or federal regulations regarding accessibility and cookie preferences.
	Functional	Preference	Not essential for basic website functionality but enables functionality for website features and enhancements. Remembers visitor preferences, choices, and login credentials. These cookies store visitor preferences, choices, and login credentials, enable error reporting, and facilitate optional features such as chat module interaction.
Marketing Cookies	Analytics	Performance or Statistics	First-party & third-party analytics and statistics cookies. These cookies collect and transmit statistical data about visitor interactions within a single website, enabling owners to analyze user behavior, optimize performance, and make data-driven enhancements to content and user experience.
	Targeting	Advertising, Marketing, or Tracking	A.K.A targeted advertising, cross-context behavioral advertising, and social media cookies. These cookies collect and share user data (including personal information) with third-parties and across websites to build interest profiles, deliver personalized advertisements, limit ad repetition, measure campaign effectiveness, enable social media sharing and login, and facilitate retargeting.



E. Other Technologies

In the complex landscape of online privacy and data protection, various technologies and website features beyond cookies can have significant implications for tracking, wiretapping, and compliance with personal information laws. Among these technologies are fingerprinting, website chat modules, which enable real-time communication between visitors and website operators; session replay tools that record and analyze user interactions; and geotargeting and geofencing techniques that deliver location-based content or services.

a. Fingerprinting

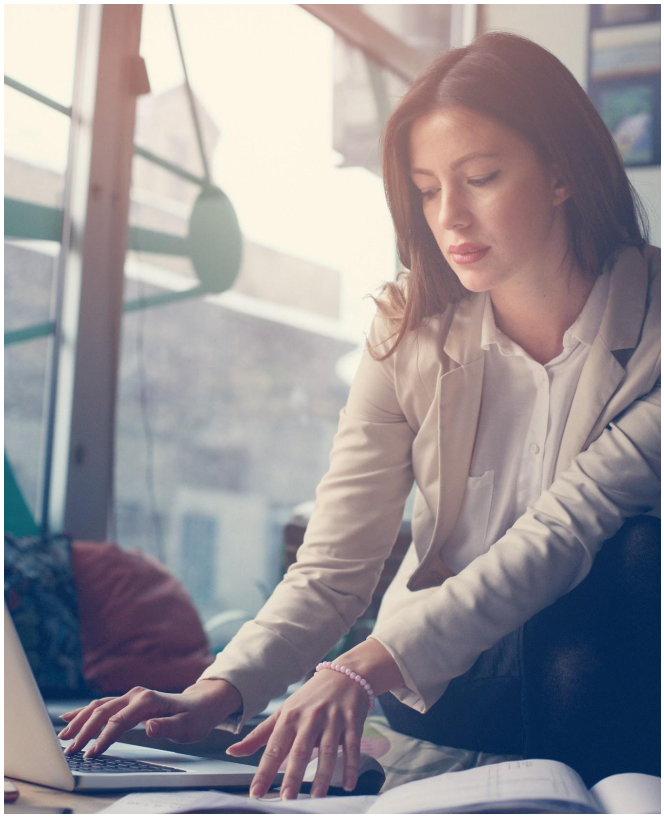
Fingerprinting, in the context of online tracking and web analytics, refers to a technique used to uniquely identify a user's device or browser without relying on traditional tracking methods such as cookies that often involve generating a unique identifier that is stored in a cookie or other persistent storage. This technique involves collecting a variety of data points and characteristics about a user's device, browser, and system configuration to create a unique "fingerprint" that can be used to recognize and track the user across different websites and browsing sessions.

The data points collected during fingerprinting may include:

- Browser information: Browser type, version, user agent string, and installed plugins.
- Device information: Screen resolution, color depth, device memory, and hardware configuration.
- System information: Operating system, installed fonts, and time zone.
- Network information: IP address, connection type, and network speed.
- Canvas fingerprinting: Rendering a graphic using the HTML5 canvas element and analyzing the resulting pixel data.

By combining some or all of these various data points, a unique fingerprint can be generated that has a high probability of identifying a specific device or browser. Even if individual data points change, such as the IP address or browser version, the overall combination of characteristics remains relatively stable, allowing for consistent tracking.

Fingerprinting is often used as an alternative or complementary tracking method to cookies, particularly in scenarios where cookies are blocked, deleted, or not supported. This makes it more challenging for users to opt-out of tracking or maintain their privacy, as fingerprinting can be harder to detect and harder to stop because traditional methods for maintaining privacy (like blocking third-party cookies) will not work or are less effective. Fingerprinting is generally third-party but it is possible that it could be used in the first-party context as well.

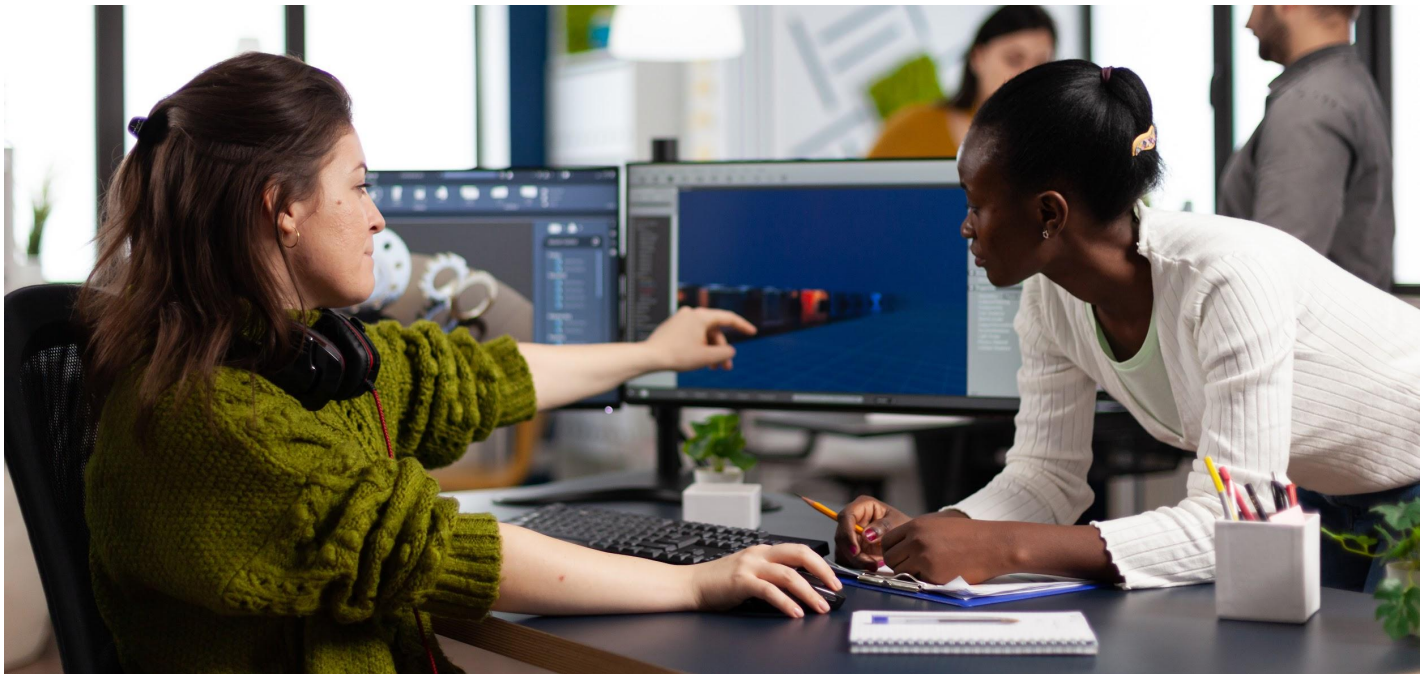


b. Chat modules

A website chat module, often referred to as a chat widget or live chat, is an interactive feature integrated into websites that allows visitors to communicate in real-time with company representatives, customer service agents, or automated chatbots. This tool is designed to provide instant support, information, or responses to inquiries that website visitors may have. Chat modules save and record communications and can collect data about customer interactions, preferences, and frequently asked questions, which can be used for analytics and improving customer service strategies. Dealers should be careful with their implementation of chat modules, as discussed in the legal theory section of this guide, they are among the targets of lawsuits and demand letters for wiretapping. FCA and truckstop.com were sued in separate lawsuits filed in May 2023 and January 2024, respectively, for wiretapping in connection with chat modules they employed on their websites.

c. Session replay

Session replay is a technology used in web analytics and user experience optimization, where the interactions of a user with a website are recorded and replayed. This technology captures mouse movements, clicks, scrolls, keystrokes, and sometimes even browser window size changes, effectively recreating the user's journey through the site. The purpose of session replay is to gain a deeper understanding of user behavior, identify usability issues, and optimize the website design for better user engagement and conversion. Session replay is capable of collecting sensitive user information, thus care must be taken to maintain user privacy and comply with data protection regulations. A dealership might use session replay to understand why users are abandoning a particular page, such as a vehicle details page or financing application. By observing the recorded sessions, the dealership can identify issues like confusing navigation, slow-loading content, or unclear calls-to-action, and make improvements accordingly. Some popular session replay vendors in the automotive industry include Quantum Metric, Navilytics, and Hotjar.



d. Geotargeting & Geofencing

Geotargeting and geofencing are two location-based marketing strategies that leverage user location data to deliver more relevant content, advertising, or experiences.

Geotargeting involves tailoring content, advertising, and offers to users based on their general geographic location, such as country, region, city, or postal code. This is typically achieved by using IP addresses, GPS data, or other location-based information to determine a user's location. This technique is widely used in online marketing, where advertisers can show different content or ads to users based on their location. For instance, a dealership might create ads tailored to specific regions or localities. For instance, they might target areas with higher incomes for luxury car models or focus on regions where certain car types, like SUVs or electric vehicles, are popular. Dealers might also target areas near competitors to attract customers through competitive pricing, promotions, or unique selling propositions. Geotargeting allows marketers to create more personalized and relevant experiences, increasing the effectiveness of their campaigns by catering to local preferences, languages, and market conditions.

Geofencing, on the other hand, is a more precise and area-specific approach. It involves creating a virtual geographic boundary or "fence" around a specific location using GPS or RFID technology. When a user's mobile device enters or exits this defined area, it triggers an action, such as sending a push notification, SMS, or targeted advertisement to the user's device. Geofencing is commonly used in proximity marketing, where businesses target potential customers who are near a physical store or event. For example, a dealership may set up a virtual boundary around their dealership or even around competitors' locations, dealerships can send targeted advertisements and promotions to potential customers' smartphones when they enter the geofenced area. For instance, if someone is browsing cars at another dealership, they might receive a notification about a special offer at a nearby dealership. Additionally, Geofencing can provide valuable data on customer behavior, such as how often a customer visits the dealership, the average duration of their visit, and which areas of the lot they spend the most time in. This information can be used to improve sales strategies and customer service. Geofencing is particularly effective for local marketing, driving foot traffic, and enhancing customer engagement through timely and location-specific messaging.



e. Call Recording & A.I. Monitoring

AI Call Monitoring refers to the use of Artificial Intelligence ("AI") technologies to analyze and evaluate voice communications, typically in call centers or customer service interactions. This technology leverages advanced algorithms and machine learning techniques to process large volumes of call data. It can transcribe audio into text, detect key phrases, assess caller sentiment, identify compliance issues, and provide insights into customer service performance.

AI call monitoring can identify keywords and phrases that indicate a customer's interest or concern, such as "financing options" or "trade-in value," allowing dealerships to tailor their response and follow-up accordingly. The technology can also evaluate an agent's tone, pace, and language, providing feedback and coaching opportunities to improve sales and customer service skills. Some AI call monitoring vendors in the automotive industry include CallRevu, Car Wars, and Marchex. By leveraging AI call monitoring, dealerships can gain a deeper understanding of their customers' needs, analyze their phone-based interactions.

F. Cookies as Covered "personal information"

Cookies can be considered personal information under privacy laws. Taking the California Consumer Privacy Act ("CCPA") as a prime example, the law explicitly categorizes "unique identifiers" as "personal information."[4] This definition explicitly encompasses cookies, beacons, pixel tags, device IDs, IP addresses, and similar technologies that can be used to identify a particular consumer or device over time and across different services.[5] The operative word here is "can," which highlights the technology's capability rather than its current use. This distinction is very important. Using "can" in this context prevents companies from circumventing their privacy obligations by simply not activating certain tracking and identification features until they choose to do so, which would otherwise allow them to identify and track consumers surreptitiously.

The Federal Trade Commission ("FTC") has mirrored this stance in its recent enforcement actions against healthcare companies GoodRx[6] and BetterHelp,[7] defining personal information in nearly identical terms as the CCPA's definition above. The FTC specifically mentioned "persistent identifiers" that include cookies and the like. Therefore, at least from the FTC and California perspective, it is clear: the potential of these cookies to track and identify a unique individual is enough to classify them as protected personal information.

Moreover, several other state privacy laws have begun to specifically regulate the "targeted advertising" or "cross-context behavioral advertising" byproduct of cookie tracking.[8] Some even require businesses to honor "global privacy controls" or "do not track" signals, which automatically opt users out of such tracking.[9] This reflects a growing legislative trend towards giving consumers more control over their online privacy and the use of their personal data.

Automobile dealers are also considered "financial institutions" for purposes of the federal Gramm-Leach-Bliley Act ("GLBA") due to their providing loans or leases for vehicles. The GLBA addresses the collection and use of nonpublic personal information ("NPI") obtained in connection with financial products. The GLBA explicitly states that information collected through "cookies" and web tracking devices is potentially NPI.[10]

---

[4] California Civil Code § 1798.140(v)(1)(A).
[5] California Civil Code § 1798.140(aj).
[6] GoodRx is an online platform that tracks the price movements of prescription drug medication of over 75,000 various pharmacies. According to the FTC complaint, GoodRx violated the FTC Act by sharing consumers' sensitive information to advertising companies like Facebook, Google, and Criteo, including prescription medication, personal health information, and contact information.
[7] BetterHelp is an online platform that provides patients with access to online mental health services, such as counseling and therapy, by using web-based interactions, phone, and SMS text messaging. BetterHelp violated the FTC Act by collecting, using, and disclosing consumers' information without receiving their consent. Furthermore, the consumers' health information was shared for advertising or advertising-related purposes.
[8] As of this writing, the following states have enacted personal data laws that reference "targeted advertising" or "cross-context behavioral advertising": California, Colorado, Connecticut, Delaware, Iowa, Indiana, Montana, Oregon, Tennessee, Texas, Utah, New Jersey, and Virginia.
[9] As of this writing, the following states have enacted personal data laws that reference browser settings, extensions, global setting or other technology that enables consumers to opt out of the controller's processing of the consumer's personal data: California, Delaware, Iowa, Montana, New Jersey, and Oregon.
[10] 12 C.F.R. § 1016.3(q)(2)(i)(F).

The GLBA's definition of NPI is broader than simply information obtained from credit applications or financing documents because it also encompasses any information collected from a consumer in connection with a financial transaction application. In the context of digital advertising, this includes seemingly non-sensitive data such as (1) lease versus finance preferences, (2) monthly payment quotes or other information from payment calculators, (3) income prediction, (4) credit score estimation, and (5) financial capacity—information that can be, and is often, collected through online tracking and behavioral profiling technologies.

Thus to the extent that cookies or other website technologies are transmitting information covered by the GLBA to, or the information is being intercepted by, a third party that could pose concerns and liability for the dealer. In the healthcare context, The Department of Health and Human Services ("HHS") has specifically called out website tracking features as potentially a violation of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") if those technologies receive individually identifiable health information.[11] HHS states that individually identifiable health information might be disclosed if the user's visit to the website is to seek information about a health condition the user has. While GLBA is a different regulation than HIPAA, the message is clear that enforcement agencies are taking the perceived threat of tracking technologies seriously.

Dealers must ensure that they are complying with GLBA to the extent that cookies are transmitting nonpublic personal information to third parties.

G. Practical Use Cases

This section provides an overview of the various use cases for cookies, scripts, pixels, and fingerprinting in the context of automobile dealership websites. It discusses how these technologies are employed by dealerships and their vendors to enhance user experience, track visitor behavior, optimize marketing efforts, and streamline operations.

a. Cookie Use Cases

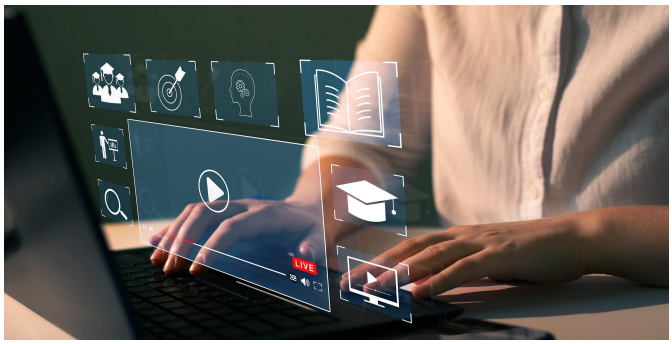
Auto dealerships leverage website cookies for various use cases to enhance customer experience and streamline their online operations. Cookies are placed on every dealership website by the website provider (e.g., Dealer.com or CDK) as well as many vendors that perform marketing, advertising, and analytics services for dealers. For example, cookies can be used to remember a visitor's preferences, such as their preferred language or vehicle search criteria, making it easier for them to navigate the site and find relevant information. Cookies can also be employed to track user behavior, allowing dealerships to analyze which pages are most popular, how long visitors spend on each page, and where they navigate after leaving the site. This data can be used to optimize the website's layout, content, and functionality. Additionally, dealerships can utilize cookies for retargeting, serving personalized ads to users who have previously visited their site, showcasing specific vehicles or offers that align with their interests. Cookies can also be used to support third-party tools, such as chat platforms or financing calculators, providing a seamless and convenient user experience.

[11] U.S. Department of Health & Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, HHS.gov (2024) https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html?mkt_tok=MTM4LUVaTS0wNDIAAAGR9qhTZM4p0cB8DTt1YNN8zpNMJAb6fRYH4j4I06JBzC0luY-t-4QaIqFRXxTK4O0qD4kiKeP9Nl_3Xi3jqD5DGAHuZ6K__h6FA2c_p8NLrqb2 (archived at: https://perma.cc/QB7R-3MND).

Google Ads, a robust online advertising platform, is an extremely common source of advertising cookies used by dealers to create and display targeted ads to users across Google's vast network of websites and apps. Google Ads provides dealerships with a variety of ad formats, including search ads, display ads, and video ads, allowing them to choose the most effective format for their marketing goals. Search ads appear at the top of Google search results when users search for relevant keywords, such as "new cars" or "used SUVs." Display ads, on the other hand, are visually engaging banner ads that appear on websites within the Google Display Network, which includes millions of websites across various industries and topics. Video ads can be showcased on YouTube and other video partner sites, capturing the attention of users who consume video content.

One of the key advantages of Google Ads for automobile dealerships is its advanced targeting capabilities. Dealerships can target their ads based on a wide range of criteria, such as geographic location, user interests, demographics, and even the specific pages or content users are viewing. For example, a dealership can target ads for luxury vehicles to users who have previously visited websites related to high-end products or have shown an interest in luxury travel. This level of targeting allows dealerships to reach the right audience with the right message, increasing the relevance and effectiveness of their ads.

To track the performance of their Google Ads campaigns, dealerships can use conversion tracking. This involves placing a small piece of code, known as a conversion tracking tag, on specific pages of the dealer's website, such as the "Thank You" page after a form submission or the confirmation page after an appointment is made. When a user clicks on a dealership's Google ad and completes the desired action on the dealer's website, the conversion tracking tag allows the dealership to attribute the conversion to the specific ad and campaign. This data provides valuable insights into the effectiveness of their advertising efforts, enabling dealerships to make data-driven decisions to optimize their ad spend and targeting strategies. By continuously monitoring and refining their Google Ads campaigns, automobile dealerships can maximize their return on investment and drive more qualified leads and sales through this powerful online advertising platform.



b. Scripts Use Cases

Dealership website vendors employ various scripts to enhance functionality and user experience on auto dealer websites. These scripts power features such as chat widgets, service schedulers, and payment calculators. For example, LivePerson and Gubaggoo provide scripts that enable live chat and messaging capabilities, allowing dealerships to communicate with potential customers in real-time. Companies like Xtime offer scripts for service scheduling widgets, making it convenient for customers to book appointments online. Payment calculator scripts, provided by vendors like AutoGravity, help customers estimate their monthly payments and explore financing options. Other scripts, such as those from inventory management providers like AutoSweet and vAuto, display and manage vehicle inventory on the dealership's website. By integrating these scripts, dealerships can offer a more interactive and user-friendly experience, ultimately improving customer engagement and streamlining the car-buying process.

c. Pixel Use Cases

Some notable vendors that use of tracking pixels in the dealership website context include Google Ads, Meta (Facebook) which uses tracking pixels to measure conversions and optimize ad campaigns, Google Analytics which employs tracking pixels to gather website usage data and track conversions, Dealer.com which uses tracking pixels for website analytics, ad tracking, and remarketing, and Dealer Inspire which uses tracking pixels for user behavior analysis and targeted advertising.

The Meta Pixel, formerly known as the Facebook Pixel, is probably the most well-known tracking pixel, and is a powerful tool used by dealers to enhance their digital marketing efforts and gain valuable insights into user behavior. By installing a small piece of code on their website, dealerships can track the actions of visitors who land on their site from Meta ads or organic posts. This data, which includes page views, vehicle views, form submissions, and other specific events, helps dealerships understand user interests and engagement with their content.

One of the key advantages of the Meta Pixel is its ability to enable retargeting. Dealerships can create Custom Audiences based on website visitor behavior, allowing them to display relevant ads to users who have shown interest in specific vehicle models or have started but not completed a form submission. This targeted approach increases the likelihood of users returning to the website and taking the desired action, such as requesting a test drive or making a purchase.

Furthermore, the Meta Pixel empowers dealerships to create Lookalike Audiences, which are groups of users who share similar characteristics and behaviors to the dealership's existing website visitors or customers. By targeting these Lookalike Audiences, dealerships can expand their reach and attract new potential customers who are more likely to be interested in their offerings. The pixel also enables conversion tracking, allowing dealerships to measure the effectiveness of their Meta ads in driving specific actions, such as vehicle purchases or service appointments.

d. Fingerprinting Use Cases

Dealership websites may use fingerprinting techniques, often through third-party vendors, to identify and track website visitors. However, the specific vendors a dealership works with and the particular fingerprinting methods used can vary significantly. Many dealership website providers offer a range of tools and integrations, and fingerprinting techniques can be included in different types of services. Additionally, fingerprinting is often not explicitly disclosed, as it happens in the background and doesn't require user input like cookies do.



3. Legal Theories Targeting Online Tracking Practices

In recent years, including as recently as 2024 (the year of this guide), dealerships and automobile manufacturers have found themselves at the center of legal claims regarding their use of cookies and related technologies on their websites. These cases typically allege improper recording or interception of information sent by website users, or improper selling of personal information in violation of state privacy laws. Notably, dealerships and manufacturers have faced legal claims not only in states where they physically operate but also based on state law in states where individuals have accessed their websites from.[1] This cross-jurisdictional aspect of online tracking has added a layer of complexity and uncertainty to the legal landscape, as dealers must navigate a patchwork of state-specific privacy laws and regulations. Since 2023 to the date of this guide there have been over 44 wiretapping lawsuits filed in California, and over 100 nationwide, in connection with cookies and pixels, this number does not include demand letters, meaning the actual number of claims is likely much higher.

As a result, it has become increasingly important for dealerships to understand the legal implications of their online tracking practices and take steps to ensure compliance with relevant laws and industry best practices. This chapter discusses some of the legal theories used against dealers and online businesses in connection with their use of cookies.

[1] A dealership in New Jersey was recently sued based on the California wiretapping laws. *See also, Rodriguez v. Ford Motor Co. et al.*, 3:23-CV-00598 (S.D. Cal. Apr. 3, 2023).

A. Wiretapping Claims under the California Invasion of Privacy Act

There has been an uptick in litigation (including class actions) brought under the The California Invasion of Privacy Act (Cal. Penal Code § 630 et seq.) ("CIPA") alleging that online tracking tools (whether it be cookies, tracking pixels, session replay tools, or chat modules) constitute illegal "wiretapping" or recording of user activities and communications without consent. The interpretation and application of CIPA in relation to cookies and other tracking technologies is still a developing area of law. However, the perceived uncertainty is something that plaintiffs' attorneys have capitalized on.



The litigation has focused on alleging liability under three main sections of CIPA: Section 631(a), which prohibits the interception of the contents of communications in transit; Section 632(a), requiring all-party consent for using a device to eavesdrop or record a confidential communication; and Section 638.51, related to the use of a "pen register" or "trap-and-trace device" without a court order. Under these sections, website

operators and third parties that receive such communications or information could potentially be held liable for using cookies and other online trackers, or otherwise recording website visit information, especially in scenarios where these technologies are used to offer services like live chat or session replay, or where they collect information that could reveal details about an individual, such as their location or browsing activity. Indeed, the Ninth Circuit, in an unpublished opinion, has indicated that Section 631 requires prior express consent from all parties to the communication before obtaining the contents of the communication.[2] In that case, the Court held that wiretapping does apply to internet tracking and that consent must be obtained before the tracking begins.

State laws like the CIPA protect residents and place requirements on parties who want to record communications. Whether it is audio or text-based, all parties to the recorded communication need to provide consent if at least one of them is from California no matter where the other parties are located. This means that businesses anywhere in the country could be sued for violations of CIPA in connection with communications with someone in California.

CIPA provides a private right of action under Section 637.2 which allows recovery of statutory damages of $5,000 per violation, or treble damages, whichever is higher. The potential damages can be large in any given case as the number of plaintiffs increase and as the number of alleged instances of tracking increases (each instance of tracking, including of the same user, can constitute a violation).

B. Federal and Other State Wiretapping Claims

14 states (including California) require all parties to consent to the recording or monitoring of a communication. Plaintiffs' lawyers in these other states have begun to take the same approach to wiretapping as the California plaintiffs' lawyers have.



One example is a 2022 appellate case, *Popa v. Harriet Carter Gifts, Inc.*[3] in the Third Circuit involving Pennsylvania state wiretapping laws. In that case the plaintiff visited the website of Harriet Carter Gifts, an online retailer. When the plaintiff's browser loaded the retailer's website, the website told the plaintiff's browser to send a separate "GET" request to NaviStone, a marketing company used by Harriet Carter Gifts. NaviStone's server used a JavaScript code to place a cookie on plaintiff's browser and began sending information to NaviStone about plaintiff's activities on the Harriet Carter website. Plaintiff alleged that NaviStone violated the wiretapping law by intercepting her communications with Harriet Carter Gifts, and that Harriet Carter Gifts violated the law by procuring NaviStone to intercept her communications.

[2] *Javier v. Assurance IQ, LLC,* No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022).
[3] *Popa v. Harriet Carter Gifts, Inc.,* 52 F.4th 121, 123 (3d Cir. 2022).

The Court of Appeal held that deploying this type of software and placing cookies to send data about a website visitor's behavior constitutes interception for purposes of the Pennsylvania wiretapping law. However the Court left open the question of whether the plaintiff provided consent to the interception and tracking.

Similarly, federal law sets a baseline of protection against wiretapping in all 50 states. The Wiretap Act (18 U.S.C. § 2510, et seq.) prohibits (among other things) the unauthorized "interception" of an "electronic communication".[4] The Wiretap Act is a "one-party" consent law, meaning that only one party to the communication needs to consent to the interception.[5]

However, the Wiretap Act does not define the term "party" and courts are split on whether surreptitious duplication of website requests, and placing of cookies and/or tracking information by third parties renders the third party a "party" to the communication.[6]



C. State Laws Relating to Privacy and Personal Information

Any state laws that provide rights and protections to its own state residents could be used as a launching pad for these types of claims if they are violated by out-of-state parties. A prime example would be state personal data laws that address the concept of the sale of personal information and the use of targeted advertising. Cookies and other technologies can be used to collect personal information, including unique identifiers, and dealers' collection, use, and sharing of that information likely is subject to state privacy laws.

i. "Sale" or "Sharing" of Information

As dealers navigate the evolving landscape of consumer privacy laws, it's crucial to understand how different states approach the sale of personal information and the use of targeted advertising. While most state privacy laws address these issues, the specific definitions and requirements can vary significantly.

One key distinction among state laws is how they define the "sale" of personal information. In some states, such as Virginia and Utah, a "sale" is limited to situations where personal information is exchanged for monetary consideration. This means that if a dealer receives payment in exchange for sharing consumer data with a third party, it would be considered a sale under these laws.

However, other states such as California, Connecticut, Colorado, Montana, and Texas, have a more expansive definition of a "sale." In these states, a sale includes not just exchanges for money but also exchanges for other valuable consideration. This broader definition means that if a dealer receives any benefit or advantage by sharing consumer data, even if no money changes hands, it will be considered a "sale."

---

[4] 18 U.S.C. § 2511(1)(a)–(e).
[5] 18 U.S.C. § 2511(1)(d).
[6] See, e.g., *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (discussing differing approaches taken by First, Seventh, and Third Circuits, and following the approach taken by the First and Seventh Circuits that that simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception.)

Most state privacy laws discuss the sale of personal information and the use of targeted advertising. In the CCPA, California goes even further and states that sharing personal information for cross-contextual behavioral advertising (targeted advertising) constitutes sharing (which is akin to a sale) and is thus subject to the provisions of the CCPA. In states like Virginia that limit the sale to monetary consideration, they still provide consumers to opt out of target advertising.

Furthermore, California's laws introduce the concept of "sharing" personal information, which is particularly relevant for businesses engaged in targeted advertising. The CCPA defines "sharing" as transferring personal information to a third party for the purpose of cross-contextual behavioral advertising, also known as targeted advertising. This type of advertising involves tracking a consumer's behavior across multiple websites or apps to deliver more personalized advertisements. In California, sharing personal information for targeted advertising is treated similarly to a sale and is subject to the same requirements and consumer rights.

While not all states explicitly mention "sharing" in their privacy laws, many still address targeted advertising. For example, under Virginia's Consumer Data Protection Act ("VCDPA"), consumers have the right to opt out of targeted advertising, even though the law limits the definition of a "sale" to exchanges for monetary consideration.

Retargeting cookies such as third-party retargeting scripts and pixels including Google Ads and the Meta Pixel are examples of targeted advertising and cross-contextual behavioral advertising. Dealers should be aware of the presence of these types of cookies on their websites and consider whether these cookies are selling user information, and/or whether the dealer needs to provide a user an ability to opt out of targeted advertising.

It is therefore critical for dealers to understand that if they or their vendors use cookies or other technologies on the dealer's website that collect or disclose personal information, they are subject to strict legal requirements. Failure to comply with applicable state privacy laws can result in severe consequences, including substantial fines, legal action, and reputational damage. It's important to note that even if a dealer is not physically located in a state with such privacy laws, it may still be required to comply if it collects or processes the personal information of residents from those states. To mitigate these risks, it is imperative that dealers take proactive steps to ensure compliance, such as reviewing data collection and sharing practices, providing clear privacy notices, implementing required opt-out mechanisms, maintaining records of consumer requests, training employees, and considering legal or privacy consulting services.

Potential pitfalls of deploying cookies before the user records their preferences

To the extent that the interception of communications (or data in the case of pen registers or trap-and-trace devices), or the sharing or selling is occurring prior to the consumer recording their preferences (giving consent) on a website, this is potentially problematic because once the information is provided to a third party, it may be difficult or impossible for the dealer to update the consumer's preferences or delete the information, and in the case of wiretapping claims, the violation has arguably already occurred, and the concept of retroactive consent is not likely a viable argument. In the case of selling or sharing, the technical limitations posed

by the interactions with third party tracking devices compound the difficulty. For instance, a third-party marketing cookie that activates before a consumer opts out enables the third party to commence tracking and potentially gather personal information. Even if the consumer subsequently opts out, the third party might have already associated the information from the cookie or tracking device with an existing consumer profile. Consequently, any later opt-out requests might not be fully effective. The dealer, in attempting to communicate the opt-out, may only be able to transmit an IP address, while the third party may have linked the data to a profile that is unassociated with that IP address.

ii. Honoring GPC signals and DNT signals

GPC (Global Privacy Control) and DNT (Do Not Track) are both mechanisms designed to give users control over their online privacy, but they differ in their implementation. From a technical standpoint, GPC and DNT differ in how they communicate users' privacy preferences to websites and online services. GPC is a newer standard that is available in compatible browsers, extensions, or tools that allow a user to configure settings that signal the user's desire to opt-out of the sale or sharing of their personal information. On the other hand, DNT is an older mechanism that is used to express a user's preference not to be tracked online. While both technologies aim to enhance user privacy, GPC has gained more traction recently due to its more specific focus and requirement that the user specify exactly what the user consents to, whereas DNT, despite being widely supported by browsers, lacks specificity.

Privacy laws in states like California and Colorado require a business's website to honor GPC signals that meet the technical requirements stated in the applicable laws. In California, under the CCPA there is a mandate for businesses to respect GPC signals as a method for consumers to express their opt-out preferences for the sale or sharing of their personal information. This includes honoring DNT signals as an equivalent to opt-out preference signals. If a consumer from California activates a GPC or DNT signal on their browser, businesses are required to treat this action as a valid request to stop selling or sharing their personal data.

Colorado's approach, as dictated by the Colorado Privacy Act ("CPA"), also emphasizes the importance of honoring GPC signals. Starting July 1, 2024, businesses in Colorado are required to allow consumers to opt out of data processing for targeted advertising or sales through a universal opt-out mechanism, such as GPC signals. The Colorado Attorney General will provide technical specifications for this mechanism, which businesses must adhere to.

For businesses that are not physically located in California or Colorado but engage with residents of these states, it is crucial to understand and implement mechanisms to honor these opt-out signals. This effectively requires the business to block all cookies and tracking devices that collect personal information that is sold (or shared in the case of California) with third parties when an opt-out preference signal is received. This ensures compliance with state laws and demonstrates a commitment to respecting consumer privacy preferences.

The California Online Privacy Protection Act ("CalOPPA"),[7] a law that predates the CCPA, mandates that commercial websites collecting personal information must post a privacy policy containing specific elements. Two crucial aspects of CalOPPA are the requirement to disclose the privacy policy's effective date and to state how the website responds to DNT signals.

[7] Cal. Bus. & Prof. Code §§ 22575-22579.

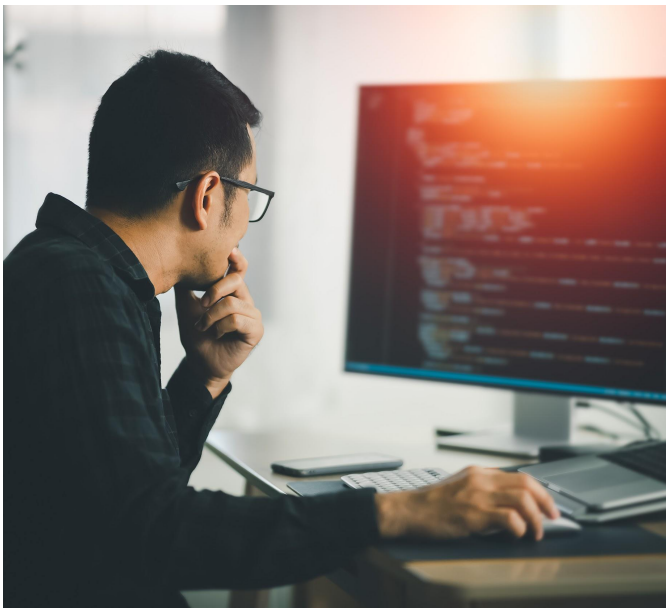


Before the CCPA's enactment, many website owners included a generic statement in their privacy policy, indicating that their website did not respond to DNT signals due to the lack of a standardized method for processing these signals. However, with the introduction of the CCPA and the California Attorney General's enforcement position that DNT signals must be honored as opt-outs, dealers who have not removed this statement from their privacy policy are likely in violation of California law. To ensure compliance, dealers should also confirm that their privacy policy includes an effective date that is updated whenever the policy undergoes revisions.

D. FTC enforcement actions

The FTC has used its Section 5 authority to target businesses that it claims have engaged in unfair and deceptive acts or practices ("UDAP") in connection with online tracking and collection of consumers' personal information. One such example is the case that the FTC filed against Kochava Inc.[8] Kochava is a data broker that the FTC alleges gathers sensitive personal data from consumers and then sells the data to its own customers. It also alleges that Kochava provides a software development kit to application developers, and it collects data from the applications that are developed. All of this is allegedly done without consumer consent, ability to opt out, and without appropriate safeguards. Kochava is also the target of a CIPA case.[9] Additionally, the FTC recently sent out a letter to tax companies notifying them that tracking consumers or using confidential information without consent is a UDAP.[10]

The FTC has also called out the use of "dark patterns" which are design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.[11] Examples of dark patterns cited by the FTC include design practices that hide or delay disclosure of material information, and design elements that obscure or subvert privacy choices. (Dark patterns are discussed further in Section 4.) Regarding privacy choices, the FTC notes that dark patterns may confuse consumers about the privacy choices that they have online, or what the effect of the choices may mean. Specific dark pattern privacy practices called out by the FTC include presenting illusory choices that nudge consumers to increased data sharing, bundling consent, defaulting to increased sharing, and place options to accept cookies more prominently than the option to decline.[12]



[8] *Federal Trade Commission v. Kochava Inc.,* No. 2:22-cv-00377-BLW (D. Idaho June 5, 2023).
[9] *See Greenley v. Kochava, Inc.,* No. 22-CV-01327-BAS-AHG, 2023 WL 4833466, at *1 (S.D. Cal. July 27, 2023).
[10] Federal Trade Commission, "FTC Warns Tax Preparation Companies About Misuse of Consumer Data" (Sept. 2023), available at: https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-warns-tax-preparation-companies-about-misuse-consumer-data (archived at https://perma.cc/X4XC-L22Q).
[11] Federal Trade Commission, "Bringing Dark Patterns to Light," at 2 (2022) (archived at: https://perma.cc/G7QG-ZRJE).
[12] *Id.* at 15-16.

.

In the GoodRX and BetterHelp cases mentioned above, the FTC's focused on the non-consensual use of cookies and pixel technology for targeted advertising. Central to these enforcement actions was the concept that health information was shared with third parties like Facebook and Google without proper consent, which the FTC defines as "Affirmative Express Consent" (see below). This standard of consent effectively disqualifies cookie consent banners that are crafted to coerce user acceptance of tracking cookies or making it difficult or impossible to decline. The FTC's definition, while detailed, is crucial and is provided below for clarity:

> Affirmative express consent means any freely given, specific, informed and unambiguous indication of an individual's wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual, apart from any "privacy policy," "terms of service," "terms of use," or other similar document, of all information material to the provision of consent. Acceptance of a general or broad terms of use or similar document that contains descriptions of agreement by the individual along with other, unrelated information, does not constitute Affirmative Express Consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute Affirmative Express Consent. Likewise, agreement obtained through use of user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, does not constitute Affirmative Express Consent.

Dark patterns fail to meet the FTC's criteria for consent. The reasoning is straightforward: there is no true consent without the presence of a clear and voluntary choice.



E. Video Privacy Protection Act ("VPPA")

Another legal theory to be aware of is the VPPA,[13] which was originally enacted in the 1980s to ensure the confidentiality of customer information gathered from video rental services. Despite the decline of video rental stores, the statute has recently seen renewed interest in enterprising plaintiffs' attorneys who are attempting to use the statute's relatively broad terms to apply to website tracking and disclosure of personal information.

One such case is a proposed class action lawsuit that accuses GameStop of sharing consumers' personal data with Facebook without consent, breaching the VPPA.[14] The suit claims that GameStop's website uses a Facebook tracking pixel to collect visitor information, including game purchases. This data, combined with Facebook IDs, allegedly allows identification of individuals and their gaming choices. The case argues that GameStop, by matching customer lists and website activity, targets consumers with ads but fails to obtain necessary consent for such data sharing. In addition, Dealer.com was sued in 2022 in a class action case alleging violation of the VPPA in connection with alleged use of the Facebook (Meta) Pixel and video content hosted by Dealer.com.[15]

---

[13] 18 U.S.C. § 2710.
[14] *Alejandro Aldana et al v. GameStop Inc.*, No. 1:22-cv-07063 (S.D.N.Y. filed Aug. 18, 2022).
[15] *Jesse Cantu v. Dealer Dot Com, Inc.*, No. 3:22-cv-1938-BEN-MSB (S.D. Cal. filed Dec. 8, 2022).



Key to understanding the VPPA's application are the definitions of "video tape service provider," "personally identifiable information," and "consumer." A "video tape service provider" includes any entity involved in the business of renting, selling, or delivering pre-recorded video cassette tapes or similar audiovisual materials, which courts have interpreted to include online video content but not live streaming content. The term "consumer" typically refers to might be colloquially considered a “subscriber,” namely: a renter, purchaser, or subscriber of goods or services from a provider, with courts often requiring an ongoing relationship with the provider. What is considered to be "Personally identifiable information" under the VPPA has evolved over time, encompassing information that identifies a person as having requested or obtained specific video materials or services from a provider, and might include state definitions such as under the CCPA. There is a split in court opinions regarding what constitutes PII, with some courts considering device IDs and GPS coordinates as PII, while others do not regard IP addresses, browser settings, and device IDs as PII.

In the evolving legal landscape, there's an ongoing debate around the definition of a "consumer" (or subscriber) and whether a website qualifies as a "Video tape service provider" under the VPPA. Some argue that a website isn't a video provider if its primary focus isn't on delivering audiovisual content. Presently, courts seem to interpret the VPPA as mainly applicable to businesses where video content is the primary product, rather than supplementary, such as promotional videos. Also, there's a growing view that to be a "subscriber" under VPPA, there might be requirements like subscription or login to access videos.

For businesses like car dealerships, this interpretation suggests that videos showcasing product features or akin to traditional commercials may not fall under VPPA. However, if a dealership ventures into creating regular video content like a vlog or webcast accessible on their website, this could potentially trigger VPPA considerations. It's prudent for dealerships to carefully assess the nature and scope of their video content, being mindful of evolving legal interpretations and potential VPPA implications before expanding or introducing new video offerings.

4. Solutions and Approaches to Consider to Reduce Risk

This section provides practical solutions and strategies to navigate the complex landscape of cookie consent management and mitigate legal risks associated with the application of wiretapping laws to common internet functions. Key recommendations include implementing comprehensive privacy policies, maintaining accurate cookie inventories, utilizing compliant cookie consent banners, employing cookie and script blocking techniques, obtaining proactive consent for website widgets, and ensuring proper vendor management.

A. Cookie Consent Management

Many of the legal theories targeting cookies (namely personal information collection and sharing, and wiretapping-related issues) can be mitigated by obtaining effective consumer consent and providing proper opt-out options. This section will give a high-level overview of some factors to consider when considering cookie consent management strategies.

a. Consent as strategy

Consent serves as a crucial defense against wiretapping claims under CIPA and against allegations involving the use of pen registers and trap-and-trace devices. Even for websites that currently do not engage in practices that have been alleged to constitute wiretapping or employing pen registers/trap-and-trace devices, it is prudent to disclose the potential for such data sharing. This forward-looking approach accounts for possible changes in operational practices and ensures ongoing compliance.

While state privacy laws universally adopt an "opt-out" approach for the sale of personal information and targeted advertising, the inherent technical limitations and practical considerations associated with this method can prove challenging, if not insurmountable. Furthermore, the FTC's stance, as articulated in the GoodRX and BetterHelp cases, indicates a clear preference for prior express consent.

From a practical standpoint, the 'opt-out' method in the context of cookie tracking is fundamentally flawed. The majority of cookie technologies employed by websites initiate data collection and tracking prior to providing consumers with a genuine opportunity to decline, and many such technologies lack the capacity to support an "after-the-fact" opt-out mechanism altogether. Even in instances where such functionality is available, it may be contingent upon the website having entered into service provider agreements or limited data use agreements, which may not be applicable to all users of the website (refer to Section C for a more in-depth discussion).



Consequently, if a consumer subsequently opts out, a third party with whom the data has been shared may have already associated the information gathered from the cookie or tracking device with an existing consumer profile. As a result, any subsequent opt-out requests may not be entirely effective in preventing further data collection or use. Moreover, in the context of wiretapping, courts have suggested that consent obtained after the commencement of recording or tracking is not considered valid. This implies that the opt-out approach could potentially expose a dealer to wiretapping claims. Given these considerations, it is evident that relying solely on an opt-out mechanism for cookie tracking and data sharing may not only be technically challenging but also may be legally inadequate.



The most effective method to obtain consent is through affirmative express, informed consent, distinctly separate from other agreements or disclosures (see definition in Section 3). This approach should clearly articulate the specifics of what the user is consenting to, thereby ensuring transparency and understanding. While courts have yet to provide a definitive stance on the validity of alternative consent methods in the wiretapping context, such as bundled consents or brief descriptions with supplementary links, these practices would likely be assessed on an individual basis. Given the varying legal interpretations and the evolving nature of the application of wiretapping laws in the digital context, a conservative approach prioritizing clear and separate consent is advisable to mitigate legal risks and uphold user trust.

Consent can also help simplify opt-out compliance. State privacy laws, such as the CCPA, have specific requirements for notices and rights to opt-out, including the recognition of opt-out preference signals, or limit the sharing of personal information. For example, the CCPA requires organizations that sell personal information or share it for cross-context behavioral advertising to provide at least two designated methods for users to submit opt-out requests or requests to limit the use of their personal information.[1] Under the CCPA, selling or sharing personal information does not occur when the consumer directs the business to disclose the information.[2] Thus if a business obtains prior express consent from a consumer to disclose the information, the business will not need to treat it as a sale or sharing of the information. However, consent must be informed and is not valid if it is buried in a lengthy terms of use document, or is obtained through a dark pattern.[3]

Additionally, the VPPA has specific conditions pertaining to how consent can be obtained and how long it lasts. For a video tape service provider to legally share a consumer's personally identifiable information, they must obtain the consumer's informed, written consent. This consent must be clearly distinct from other legal or financial agreements involving the consumer. The consent can be obtained either at the time the information is to be disclosed or in advance for a predetermined period, not exceeding two years, or until the consumer decides to withdraw their consent. Furthermore, it's mandatory for the provider to offer a clear and conspicuous option for the consumer to revoke their consent.[4]

[1] Cal. Code Regs. tit. 11, § 7026(a).
[2] Cal. Civ. Code § 1798.140(ad)(2), (ah)(2).
[3] Cal. Civ. Code § 1798.140(h).
[4] 18 U.S.C. § 2710.

b. Dark patterns void consent

As noted previously, if consent is not valid or properly obtained, then the consent is void. Use of dark patterns is likely to render consent void, several dark patterns are described below.

i. Framing bias

Framing bias as a dark pattern in web design manipulates users' choices by presenting options in a way that highlights the positive aspects of one choice over others, often leading users towards a decision that they might not have made if presented neutrally. For example, a subscription service website might prominently display and extol the benefits of a premium plan in comparison to a basic plan, using persuasive language, highlighted buttons, and strategic placement to make the premium option appear more advantageous. This technique plays on cognitive biases, subtly influencing decision-making by framing one choice as more beneficial, regardless of its actual value or relevance to the user's needs.

ii. Default settings

The dark pattern of default settings involves pre-selecting options in a user interface in a way that benefits the service provider, or presenting an illusory choice that nudges the consumer toward increased data sharing, often at the expense of the user's best interests or preferences. These default settings are typically designed to opt users into certain choices, like sharing personal data, or accepting cookies and tracking, without explicit consent. Users, often rushing through processes or not fully understanding the implications, may inadvertently agree to these settings and may not realize the effect of the settings, or may not realize that other options exist. This tactic relies on user inattention or inertia, banking on the likelihood that many will not take the time to change the defaults, thereby leading to outcomes that favor the organization, such as increased data collection.

iii. Accept-only

"Accept-only" describes a dark pattern cookie consent banner that only offers an option to accept cookies, without a straightforward way to refuse them. This design intentionally makes it difficult, time-consuming, or impossible for users to reject cookies, often by hiding the refuse option in complex settings or not providing it at all. As a result, users are coerced into accepting cookies to proceed, effectively bypassing genuine consent. This approach manipulates the user's choice, exploiting their desire for quick website access, and often leads to higher rates of consent for cookie tracking than would occur with a fair, balanced choice.



iv. Confirm-shaming

Confirm shaming is a dark pattern where the refusal option in a prompt or request is worded in a way that shames or guilt-trips the user for choosing it. Often encountered in subscription pop-ups or opt-out situations, this tactic uses negative or condescending language for the opt-out choice, like "No, I don't want to save money" or "I prefer to stay uninformed," as opposed to a neutral or positive affirmation. This manipulative technique preys on the user's emotions, particularly their fear of missing out or feeling judged, to coerce them into making a decision that they might not have made under a neutral presentation, such as signing up for a newsletter or accepting a special offer.

v. Other dark patterns

The FTC has identified other practices[5] that constitute dark patterns, summarized here:

- Design elements that induce false beliefs, such as advertisements deceptively formatted to look like independent, editorial content, and purportedly neutral comparison-shopping sites that actually rank companies based on compensation.
- Design elements that hide or delay disclosure of material information, such as burying key limitations of a product or service in dense terms of service documents or adding hidden fees that only appear late in the checkout process (drip pricing). This makes it hard for consumers to comparison shop.
- Design elements that lead to unauthorized charges, such as tricking people into paying for goods/services they didn't intend to buy, making it easy to sign up for subscriptions but very difficult to cancel, and automatically charging consumers after a free trial ends without clearly disclosing the terms.
- Design elements that obscure or subvert privacy choices, such as interfaces that make it difficult to opt out of data collection/sharing, repeatedly prompt consumers to select privacy-invasive options, highlight choices that maximize data collection while greying out privacy-protective options, or include default settings that enable extensive tracking. Some dark patterns also trick consumers into sharing more personal information than they intended.

c. Cookie Consent Banners

When a user visits a website, a cookie consent banner should be displayed prominently, clearly indicating its purpose of providing information about privacy and cookies, and should have a direct link to the privacy policy. The banner should inform users, in plain language, that cookies are used for tracking purposes and that the collected data may be shared with third parties. It should also explain the consequences of accepting or denying cookies, ensuring that users can make an informed decision. The buttons for a consumer to accept or decline cookies should be symmetrical and the design of the banner and the language within it should be neutral, in order to avoid allegations of dark patterns.

To cater to a diverse audience, the banner should be designed to support translation into common foreign languages. Indeed, the CCPA regulations require the disclosures mandated by the rules be available in all languages in which the business is conducted at the business.[6] Additionally, if the website falls under the jurisdiction of the CCPA, the banner must include a "Notice at Collection" and a privacy choices link. Furthermore, the banner should be programmed to recognize and respond to GPC signals, notifying users that their preferences have been recorded.

This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our Privacy policy

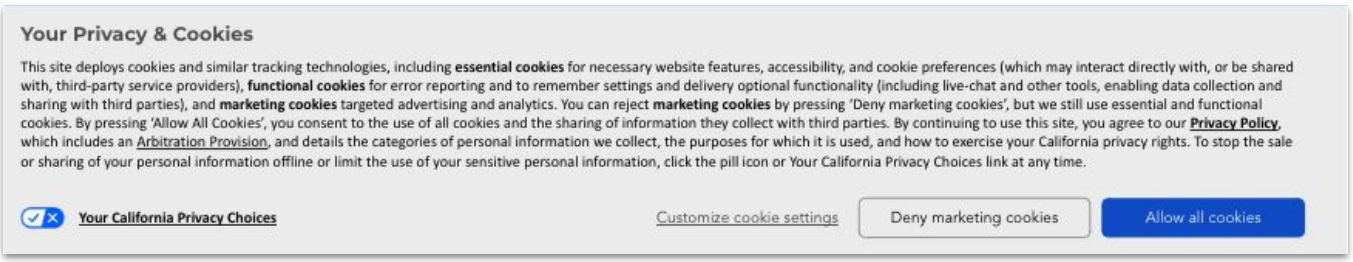
Manage cookies Accept all

[5] Federal Trade Commission, Bringing Dark Patterns to Light: An FTC Workshop (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (archived at https://perma.cc/C2CU-4WTP).

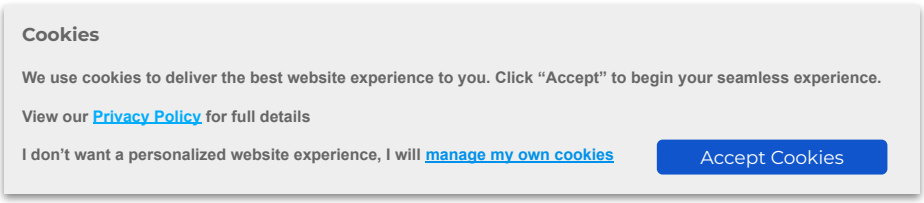
[6] Cal. Code Regs. tit. 11, § 7003(b)(2).

To prioritize user privacy, the banner script should prevent the activation of marketing cookies until the user explicitly accepts them. A more conservative approach, aligned with the European Union's General Data Protection Regulation ("GDPR"), would be to block all non-essential cookies until the user provides consent. However, in the United States, the primary concern is typically focused on cookies that collect and share information with third parties which can typically be managed without blocking cookies to the extent required by GDPR. A recommended best practice is to also have a cookie settings link that will allow users to customize their cookie settings.

Lastly, to ensure accessibility and usability, the cookie consent banner should be optimized for seamless loading on both desktop and mobile browsers. This optimization ensures that all users, regardless of their device, can easily access and interact with the banner, making informed decisions about their privacy preferences. A template banner is provided below as an example:



An example of a dark pattern cookie banner is below:



The following are some notes on the dark pattern banner:

- Consent language does not include any information about the types of cookies used or data collected/shared. This would not constitute valid consent.
- Privacy policy is not clear and conspicuous and is not hyperlinked.
- Banner uses the following dark patterns:
    - Accept-only, does not provide a meaningful opportunity to decline.
    - Confirm shaming by phrasing link to manage preferences in negative terms.
    - Subverts privacy choices and hides material information about data collection, tracking, etc.
- Website operator may be sharing or selling data and personal information without disclosure.
- The website may be loading cookies before the user can manage their preferences, thus defaulting to the "Accept" choice.

d. Effects of Blocking or Delaying the Loading of Cookies

Delaying or blocking cookies before a user explicitly accepts their use can potentially impact a dealer's analytics data and ability to retarget (potential) customers. It is estimated that approximately 20-30% of users decline cookies. While data for users who fail to interact with a cookie banner is less readily available, it is rational to assume that such users account for a modest increase in that percentage.

The level of risk a dealer is willing to tolerate determines how their website is configured to deploy cookies. This guide recommends delaying marketing cookies until the user accepts them. Under this approach, if a user declines to accept, or fails to interact with the banner, targeted advertising and analytics cookies will not load, resulting in decreased website statistics visibility, online advertising performance metrics, lead attribution, conversions, and audience reach. A dealer with a higher risk tolerance might choose to load analytics cookies before the user interacts with the banner. While this approach will have less of an impact on the dealer's analytics, it will increase their risk of potential wiretapping or personal information claims. See also the call out in section 3.C.i of this guide.

It is crucial to recognize that the discussion in this guide is not purely about legal compliance; there are practical business impacts that a dealer might experience based on the decisions they make with the information presented. Dealers might also face pressure or dire warnings from vendors they use to activate their marketing efforts. However, it is important to keep in mind that some of these vendors have a financial interest in increased use of analytics based on their compensation formulas. Therefore, while their input is valuable, dealers should also evaluate these issues with input from sources that are not financially interested in the continued use of marketing cookies. Dealers should strongly consider asking their vendors for written indemnification from claims related to online tracking, targeted advertising, and analytics. Additionally, dealers should assess whether a modest decrease in analytics tracking will result in a decrease in revenue or sales, and if so, to what extent. Dealers might conclude that adopting a more conservative risk approach is worth the potential reduction in website statistics visibility.



B. Privacy Policy Disclosures and Transparency

When it comes to cookie consent management, having an up-to-date and comprehensive privacy policy is crucial. The contents of privacy policies are driven by state and federal laws, though at a minimum a privacy policy should include information pertaining to the following key elements: (1) the types of personal information collected from users, such as names, addresses, email addresses, and payment details; (2) how the collected information is used, shared, and disclosed to third parties; (3) the security measures in place to protect user data from unauthorized access or breaches; (4) the user's rights regarding their personal information, including the ability to access, correct, or delete their data; (5) the company's data retention practices and how long user information is kept; (6) information on the use of cookies and other tracking technologies; (7) a clear explanation of how users can opt-out of data collection or sharing; (8) details on how the company complies with relevant state and federal privacy laws; and (9) contact information for users to reach out with privacy-related questions or concerns.

This policy should be prominently displayed on the dealer website and clearly referenced and linked within the cookie consent banner. By doing so, you are effectively notifying users that additional terms apply to the personal information collected by or transmitted through your website. This approach puts the user on notice to review those terms and conditions.

Incorporating the privacy policy and including a direct link to it in the cookie banner strengthens the argument that the user's consent choices are informed by the privacy policy's contents. In other words, by consenting to the use of cookies, the user is also agreeing to the terms outlined in the referenced privacy policy.

However, it is essential to understand that a comprehensive privacy policy alone is not a panacea. Website owners must exercise caution and seek guidance to ensure compliance with applicable laws and regulations. If important disclosures are hidden within a lengthy privacy policy or if the policy attempts to obtain consent without making the disclosure clear and conspicuous to the user, such practices are unlikely to be considered valid and may not withstand legal scrutiny.

To mitigate these risks, it is advisable to conduct a thorough review of your website's data practices and create a data map that identifies the types of personal information collected, the purposes for which it is used, and the third parties with whom it is shared. This data mapping exercise will help you ensure that your privacy policy accurately reflects your data practices and that you are not inadvertently collecting or sharing personal information in ways that are not disclosed to users.

Dealers should also ensure that any chat bots or widgets incorporated into their website include a clear disclosure within the widget itself, informing users that their conversations may be subject to monitoring or recording by both the dealer and the third-party chat provider. Furthermore, if the third-party provider intends to use the information collected through the chat for any purpose beyond facilitating communication with the dealer or providing the chat service, it is imperative that this information be explicitly disclosed. This disclosure should be prominently displayed not only within the chat widget but also in the dealer's comprehensive privacy policy.



Furthermore, it is crucial to maintain proper vendor management when dealing with third parties that have access to user data collected through your website. This includes carefully vetting vendors, establishing contractual safeguards to protect user data, and regularly monitoring their compliance with your privacy policy and applicable laws. By doing so, you can demonstrate a commitment to protecting user privacy and mitigate the risk of unauthorized data access or misuse by third parties.

While incorporating a privacy policy and linking to it in the cookie consent banner is an important aspect of cookie consent management, it is not a substitute for clear, conspicuous, and legally compliant disclosures and consent practices. A well-crafted privacy policy, along with proper disclosures and thoughtful consent management, can help companies avoid legal liability related to wiretapping, pen registers, cookies, and online tracking technology. By clearly outlining the types of data collected, the purposes for which it is used, and the parties with whom it is shared, a privacy policy ensures transparency and informed consent from users.

Website owners must work closely with legal experts to ensure that their privacy policies and data practices are transparent, easily understandable, and fully compliant with applicable laws and regulations. By doing so, they can build trust with their users and minimize the risk of legal and reputational harm

Below is an excerpt of a template privacy policy disclosure that discusses disclosure of information with third parties, dealers should consider their own data sharing practices when creating a privacy policy:

Disclosure of Personal Information to Third Parties

Categories of Personal Information Disclosed for a Business Purpose or Sold to Third Parties	Categories of Third Parties to Whom the Information was Disclosed	Categories of Third Parties to Whom the Information was Sold or Shared for Cross-context Behavioral Advertising
Audio / Video / Visual / Electronic such as photographs, recorded calls, voicemails, and online & electronic communications, such as those made via a live or automated online chat module.	Software Vendors, Claims & Benefits Administrators, Professional Service Companies, Attorneys & Law Firms, Social Media Networks	Software Vendors
Commercial such as vehicles, products, services, and repairs purchased, obtained or considered; personal property records (e.g., vehicle titles and registration cards); or other purchasing or consuming histories or tendencies.	Insurance Brokers (non-health related), Auctions & Wholesalers, Software Vendors, Check Guarantee Companies, Digital Retailers & eCommerce Platforms, Government Entities, Payment Processors & Gateways, Records Management Companies, Repair & Sublet Facilities, Transportation Companies, Professional Service Companies, Attorneys & Law Firms, Debt Collection Agencies & Repossession Companies, Website and Hosting Providers, Auditors & Consultants, Social Media Networks	Advertising Networks & Marketing Agencies, Data Brokers & Analytics Providers, Vehicle Manufacturers, Reputation Management Companies, Financial Institutions, F&I Product Providers & Administrators

C. Advertising Providers, Service Providers, and Settings to Limit Data Use

When configuring advertising and analytics providers for a website, it is important to be aware of the data processing options available to ensure compliance with privacy regulations and respect for user preferences. Advertising and analytics providers have varying options that allow website owners to customize how data that is sent to the providers is used by the provider. Two major providers, Meta and Google, offer customizable settings.

Meta's Limited Data Use ("LDU") feature enables businesses to restrict how Meta processes data from users. When it is activated, Meta will treat the data as a service provider. The Limited Data Use option is only available for information from users in California, Colorado, and Connecticut, and is not available for all Meta products in each of those states, though it does apply to the Meta Pixel.[7] Similarly, Google provides restricted data processing options and custom settings within Google Analytics. These controls allow website owners to limit how Google uses data collected from their sites.[8]

Google also allows advertisers to opt-in to the applicable data protection/data processing terms under which Google agrees to be a service provider for data collected under state privacy laws, and agrees to certain restrictions on its processing of data. In addition, the privacy controls in Google Analytics allow advertisers to customize the settings used for their data, one such control is IP address masking which a user's IP address is not logged or stored. Dealers should consult with their counsel regarding the benefits that opting into the service provider arrangements might have in regards to potential wiretapping claims, especially regarding claims of a dealer aiding and abetting wiretapping.

It is important to note that these settings require the dealer to take affirmative steps to opt in, including signing supplemental data processing agreements. However, using these settings, along with a dealer's own data practices, can help ensure that the dealer is not selling the data to the analytics partner. In addition, dealers who choose a higher risk approach to cookie management, such as by loading analytics before a user provides affirmative consent, should consult with their counsel to see if activation of features such as LDU, or use of Google Privacy Controls, or similar features can minimize the dealer's risk of claims relating to wiretapping and misuse of personal data.

Dealers should be aware of their contractual obligations to their franchisors ("OEMs") and OEM-mandated vendors regarding advertising, analytics, and the sharing of personal information. These agreements often require dealers to represent that they have obtained consent from individuals whose information is being shared. Dealers should ensure the accuracy of these representations and, if necessary, modify contracts and/or data management practices accordingly.

It is crucial to note that while these options offer increased control over data processing, they may not be available for all products or users. Some of these features only apply to users residing in certain states, or to whose personal information is subject to state data privacy laws. Thus, even if a dealer has activated these settings, it is possible that some of the users to its website will not have the settings applied to them. Therefore, dealers should always consider broader cookie consent management practices. Dealers should also carefully review the terms and conditions of their chosen advertising and analytics providers to ensure they are taking the necessary steps to safeguard user privacy.

---

[7] "Meta Business Help Center, About Limited Data Use," available at: https://www.facebook.com/business/help/1151133471911882 (last accessed March 20, 2024).

[8] "Helping Advertisers, Publishers, and Partners Comply with US States Privacy Laws," Google, https://business.safety.google/rdp/ (archived at: https://perma.cc/2DYB-HYEZ). "Privacy controls in Google Analytics," https://support.google.com/analytics/answer/9019185?hl=en#zippy=%2Cin-this-article (archived at: https://perma.cc/JX6S-T3PM).

D. Arbitration and Class Action Waiver Strategy

Implementing terms of use on websites, including arbitration provisions and class action waivers, can be an effective strategy for dealers to mitigate the risk of litigation. Arbitration clauses, often seen in purchase and lease contracts, require that any disputes arising from the use of the website be resolved through arbitration, a process that takes place outside of the court system and on an individual basis, rather than through class action lawsuits. By mandating individual arbitration, organizations can potentially avoid the substantial damages and costs often associated with class action suits, which can lead to significant cost savings.

Arbitration, while generally more expensive than traditional court fees, offers several advantages over litigation. The process is often more efficient, with streamlined procedures and limited discovery, which can result in faster resolution of disputes. However, it is important to note that the legal requirements for drafting enforceable arbitration clauses and class action waivers can vary significantly from state to state.

Given the complex legal landscape surrounding these provisions, it is crucial for organizations to seek the guidance of experienced legal professionals when crafting their terms of use. Legal experts can help ensure that the arbitration clauses and class action waivers are legally sound, enforceable, and tailored to the specific needs and circumstances of the organization. By working closely with legal counsel, organizations can develop robust terms of use that effectively protect their interests while complying with applicable laws and regulations.

Here are some guidelines to keep in mind when implementing an arbitration agreement:

1. Users must be adequately notified of the agreement's existence. Courts are more likely to enforce agreements when users explicitly agree to the terms or when a conspicuous notice is provided, informing users that their use of the website is governed by an arbitration agreement. Burying the notice within the website or solely including it in a terms of use document linked at the bottom of the webpage may reduce the likelihood of enforceability.
2. To increase the chances of a court enforcing the arbitration agreement, the terms should be balanced and apply mutually for both the dealership and the user. Avoiding terms that are unreasonably favorable to the dealership can help ensure the agreement's enforceability.
3. The arbitration agreement should clearly reference the applicable rules governing the arbitration process. Many arbitration administrators, such as the American Arbitration Association, make their rules publicly available online. It is important to note that identifying the applicable rules does not necessarily require the arbitration to be administered by that specific administrator. By providing information about the governing rules, users can better understand the procedures that will apply to their claims.
4. The agreement should outline the process for initiating an arbitration. This information is often provided in the applicable rules, which can help clarify the arbitration process for all parties involved.
5. It is crucial for dealerships to promptly enforce their arbitration agreements when disputes arise. Failure to do so may result in the dealership being deemed to have waived its right to arbitrate. To preserve their rights, dealers should involve counsel as soon as a dispute arises and inform them of the existence of the arbitration agreement. By taking swift action, dealers can ensure that their rights are protected and that the arbitration agreement is properly enforced.

E. Practical Considerations and Recommended Steps for Dealers

1. Privacy Policy

As described above, a comprehensive and legally compliant privacy policy is a fundamental requirement for any organization operating in today's digital landscape. It is essential to ensure that the privacy policy aligns with the relevant state and federal laws and regulations. By dedicating resources to develop and maintain a strong privacy policy, dealers can foster trust with their customers, mitigate legal risks, and demonstrate their commitment to data privacy and security.



2. Cookie inventory

Maintaining an accurate and up-to-date inventory of cookies is a crucial step for dealers to ensure compliance with privacy regulations and provide transparent disclosures to their users. This inventory should encompass all cookies utilized on their websites, as well as their respective purposes and durations.

By regularly auditing and documenting their cookie inventory, dealers can manage their data collection practices and ensure that their privacy policy accurately reflects the cookies in use. This inventory serves as a foundation for providing clear and comprehensive information to users about the types of cookies employed, their functions, and the data they collect. Moreover, a well-maintained cookie inventory enables dealers to promptly identify and address any potential compliance issues, demonstrate due diligence, and respond to user inquiries or regulatory requirements with confidence.

3. Cookie consent banner

As discussed above, Dealerships are strongly advised to implement a cookie consent banner on their website to inform users about the use of cookies and provide them with the option to either accept or decline these tracking technologies.

4. Cookie and script blocking

To ensure compliance with data protection regulations and respect users' privacy preferences, it is advisable for website operators to implement a cookie banner that prevents the deployment of marketing cookies until the user provides explicit consent. This approach aligns with the principle of user control and transparency in data collection practices, it also avoids potential technical limitations of after-the-fact opt-outs, and is consistent with legal theories advocated by some courts.

From a technical perspective, when a website initially loads cookies and subsequently provides users with the option to opt out, updating the user's preferences may prove challenging or even unfeasible if the data has already been shared with third-party providers (e.g., Google or Meta). The successful implementation of such an opt-out feature might be contingent upon the website having opted in to Limited Data Use or restricted data processing agreements with the provider, and the user being covered under the applicable terms.

Furthermore, the user's after-the-fact opt-out request may necessitate specific technical capabilities on the website's part, such as the integration of appropriate code or Application Programming Interface (“API”) connections. For instance, the Google Deletion API enables websites to request the removal of user data from Google's systems. However, the availability and implementation of these technical solutions are not universal across all websites.

Additionally, in the wiretapping context, courts have suggested that retroactive consent—consent obtained after the commencement of recording or tracking—is not considered valid.[9] This means that prior express consent is required. The FTC has adopted a similar stance regarding the use of cookies to collect personal information for advertising purposes, emphasizing the importance of obtaining consent before initiating any data collection or tracking activities.

From a technical perspective, achieving this objective of delaying the deployment of marketing cookies until the user provides explicit consent requires strategic placement of the cookie banner script within the website's source code. Specifically, the script should be positioned at the top of the header section to effectively block the execution of third-party cookies, scripts, and tag managers, such as Meta pixel and Google Analytics, until the user actively selects their preferred cookie and tracking settings.

Implementing this best practice necessitates close collaboration among various stakeholders, including the IT department, marketing team, and website providers. These parties must work together to ensure the proper integration of the cookie banner and the successful blocking of third-party elements prior to user consent.

To streamline the implementation process and ensure compliance, website operators may consider engaging the services of third-party compliance vendors. These specialized providers can offer expertise and solutions tailored to the specific requirements of the website, helping to efficiently and effectively implement the cookie banner and manage user preferences in accordance with regulatory standards.

5. Proactive consent in website widgets

When implementing interactive features on their websites, such as chatbots, dealers should prioritize user privacy by incorporating separate consent mechanisms and disclosures. These features may involve the tracking, collection, or recording of personal information exchanged during user interactions.

To ensure transparency and compliance, dealers should integrate prominent notices within the relevant widgets or interfaces, informing users about the potential monitoring, tracking, or recording of their communications. Ideally, these notices should be accompanied by a consent process, allowing users to make informed decisions about engaging with the feature and granting permission for their data to be processed as described. By proactively providing clear disclosures and obtaining consent, dealers demonstrate their commitment to respecting user privacy and adhering to applicable data protection regulations and reduce their legal risk.

A template general website disclosure regarding chat widgets and session replay appears below:

Chat Modules

We (or our third-party vendors on our behalf) may collect certain categories of personal information from you when you use our interactive chat module. In addition to the information you may enter into the chat box or live chat feature, the categories of personal information include, but are not limited to, name, phone number, email, mailing address, and other identifiers you may provide. Additionally, we (or our third-party vendors on our behalf) may also store any transcripts from such conversations and link those transcripts with your personal information. We (or our third-party vendors on our behalf) may also collect information from you to perform data analytics and thereby enhance your experience and help improve the functionality of our tools and digital advertising in an effort to present to you only relevant products and services. Such information includes, but is not limited to, geolocation, IP address, pixel tags, browsing history, viewing behavior, clicks, online activity, and other analytics. By interacting with the chat module, you understand and agree that we may use this data to communicate with you about our products and services. You also consent to our collection and analysis of all personal information provided as part of the chat module and understand that we utilize a vendor to process, analyze, and store the content of the chat on our behalf. By using the chat module, you are consenting to us disclosing and sharing with the chat module vendor any information (including personal information) you provide.

Use of Session Replay Tools

We (or our third-party vendors on our behalf) may collect certain categories of personal information from you when you interact with our website(s) or application(s) through the use of session replay tools. Session replay is a tool that recreates your sessions from our websites or applications (including visual elements), giving us (or our third-party vendors on our behalf) a better understanding of how you interact with our websites and applications to help maximize the customer's experience. Session replay tools that we may utilize include, but are not limited to, video-like playback, error tracking integration, application performance monitoring (APM) integration, real user monitoring (RUM) session timeline, and speed controls. Depending on your interaction with our website (e.g. when you complete a "Contact Us" form), the categories of personal information we may also capture include, but are not limited to, name, phone number, email, mailing address, and other identifiers that you may provide. By interacting with our website(s) or application(s), you are consenting to us (or our third-party vendors on our behalf) capturing any interactions and any information (including personal information) you provide.

[9] *See, e.g., Javier v. Assurance IQ, LLC,* No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022).

Dealers should collaborate with their widget providers to ensure that appropriate disclosures are also included within the widget itself. It is important to note that a conservative cookie policy or banner can sometimes prevent widgets from loading automatically. In such cases, it may be possible to allow users to click on the specific area of the webpage where the widget would have appeared, thereby activating the widget or script manually. In conjunction with this user-initiated activation, a disclosure can be displayed before the widget loads, enhancing the consent process and providing additional notice to the user. By implementing these measures, dealers can strengthen their compliance efforts and provide users with greater control over their data and interactions with the website's features.

6. Vendor management

Maintaining a comprehensive inventory of vendors accessing, collecting, or receiving information from their website is a critical responsibility for dealers. This inventory should include a thorough assessment of each vendor's data practices, ensuring that they align with the dealer's own privacy policies and comply with relevant regulations.

To establish trust and mitigate potential risks, dealers must conduct due diligence on their vendors, verifying that they are competent operators with robust data protection measures in place. This process involves evaluating the vendors' security protocols, data handling procedures, and privacy policies to ensure that they meet or exceed industry standards. Dealers should also ensure that there are appropriate contractual terms in place with vendors that obligate vendors to limit the use of data obtained from the dealer, and to safeguard that data. By actively monitoring and managing their vendor relationships, dealers can demonstrate a strong commitment to safeguarding user information and maintain accountability throughout their data ecosystem.

Moreover, dealers must update their privacy policy when they start using a vendor that collects, shares, or processes new categories of information. For instance, if a dealer previously did not collect biometric data but begins doing so or engages a vendor who collects such information (e.g., fingerprints, facial recognition, or voice recognition), the dealer's privacy policy will need to be revised to include this new category of data. The updated policy should disclose whether the biometric information is shared, sold, or used for targeted advertising purposes. Dealers could consider working with a vendor to assist in streamlining updates to their privacy policy. By keeping their privacy policy current and accurately reflecting the types of data collected and how it is used, dealers can maintain transparency and comply with legal requirements.



E. Businesses Fighting Back

The wiretapping laws forming the basis of the new wave of internet wiretapping cases are attempting to apply these laws in ways that could significantly impact the general operation of websites.

Many businesses have responded to the federal lawsuits by filing motions to dismiss the complaints (motions to dismiss are not always an option in state courts). While some have been successful, courts often allow plaintiffs to amend their lawsuits, and most cases settle before the issues can be resolved by a court or jury, and before those trial court decisions can be finalized by an appellate court. This has led to a lack of clear legal precedent on the matter.

A recent case in a California Federal Court illustrates a different approach. L'Occitane, a business facing thousands of wiretapping arbitration cases filed by a single law firm, is initiating an offensive fight against that law firm alleging that the firm is involved in a conspiracy to fabricate thousands of fraudulent claims related to the CIPA and wiretapping. L'Occitane's complaint seeks to halt the legal claims pursued by the law firm and requests that the court declare CIPA unconstitutional.[10] The outcome of this case, and cases like it, could have significant implications for businesses operating online and the future interpretation of wiretapping laws in the context of the modern internet. If courts uphold the claims that use of analytics and other cookies without express consent are wiretapping, it could move the U.S. toward a GDPR-style consent requirement, necessitating the use of more intrusive cookie banners and reduced analytics data.



The aggressive litigation approach taken by L'Occitane is costly and time-consuming, and thus may not be feasible for all businesses, particularly businesses that do not have the same litigation budgets as multinational corporations. Consequently, it is advisable for dealers to take a proactive and cautious approach to minimize the risk of becoming targets of such claims.

Another legal theory cited by a California Federal District Court also identified a potential area of attack to CIPA claims. In *Javier v. Assurance IQ, LLC,* 649 F. Supp. 3d 891, 898 (N.D. Cal. 2023), the plaintiff alleged that Assurance IQ used a third party software company to monitor his interaction with Assurance IQ's website including monitoring keystrokes and eavesdropping on his communications without consent. He filed a lawsuit under CIPA. The defendants filed a motion to dismiss, in considering the motion to dismiss District Court suggested that some services are so ubiquitous on the internet that they might not be considered a third party for purposes of wiretapping.[11] If that argument is adopted, it might mean that certain ubiquitous services, such as Google Analytics, would not be considered wiretapping under CIPA.

---

[10] *L'Occitane Inc. v. Zimmerman Reed LLP, No. 2:24-cv-01103 (C.D. Cal. Feb. 8, 2024).*
[11] *Id. at 900.*

Appendix 1: Website Cookie Compliance Checklist

Use this checklist to evaluate key elements of your dealership website for cookie compliance. Please note that this list is not exhaustive, and additional measures may be necessary to ensure full compliance.

Cookies

- ❑ 1. Cookie banner loads when users visit the website.
- ❑ 2. Cookie banner contains link to privacy policy.
- ❑ 3. Cookie banner has symmetrical accept and decline options.
- ❑ 4. Cookie banner discloses types and uses cookie and tracking technologies, including third-party sharing.
- ❑ 5. Marketing cookies are blocked until the user accepts the banner.
- ❑ 6. Cookie banner avoids dark patterns to obtain consent.
- ❑ 7. Banner displays CCPA notices if applicable.
- ❑ 8. Cookie banner is programmed to recognize GPC and DNT signals and provide users with notice that the signal has been recognized.
- ❑ 9. Cookie banner provides translation options.
- ❑ 10. Dealer conducts periodic cookie and tracking technology inventory.

Website in General

- ❑ 1. Website features that collect personal information or unique identifiers, such as chatbots, are disclosed in the privacy policy and have consent/disclosures integrated into the feature itself.
- ❑ 2. Website elements are designed with a "privacy-by-design" approach, by embedding privacy considerations into the design and architecture of the website.
- ❑ 3. Provides notice of arbitration agreement in privacy policy (may be in cookie banner if conspicuous).

Privacy Policy and Personal Information

- ❑ 1. Privacy policy discloses categories of personal information collected.
- ❑ 2. Privacy policy discloses categories of third parties with whom personal information is shared or sold.
- ❑ 3. Privacy policy provides information about how a user can opt out of the sale of their personal information.
- ❑ 4. Privacy policy and website provides information or portal for users to submit requests regarding their personal information as required by applicable law (e.g., requests to know, requests to correct, etc.)
- ❑ 5. Dealer conducts vendor due diligence to ensure that vendors have appropriate safeguards to protect customer information and that vendors limit the use of personal information received from the dealer.
- ❑ 6. Dealer has contracts with vendors (including marketing companies and third parties that place features or widgets on websites) that limit the vendors' use of personal information and that ensure that vendors have appropriate safeguards and data security practices.
- ❑ 7. The dealer itself has appropriate data security, physical and technical safeguards, and access controls to protect against unauthorized access to personal data and to comply with applicable law.
- ❑ 8. Privacy policy includes agreement to arbitrate disputes.

Appendix 2: Website Cookie Screenshots

A website visitor can view the cookies that a webpage is using with just a few clicks in their web browser. This section provides instructions on how to view the cookies and includes some pertinent screenshots. The process for accessing and viewing cookies varies slightly depending on the web browser being used, but generally involves opening the browser settings, navigating to the privacy or security section, and selecting the option to view or manage cookies.

A. Steps to View a Website's Cookies

Step One: Navigate to the webpage that you wish to view the cookies for.

Step Two: Right click on the webpage and select "Inspect" (some browsers call this "Inspect Element" or use a similar phrase. This will open the developer view of the webpage, often as a sidebar within the existing window, or in a new window.

Step Three: Click "Application" at the top of the developer view. You might need to click the arrow button to see this option.

Step Four: In the "Storage" section in the Application view. Click "Cookies."

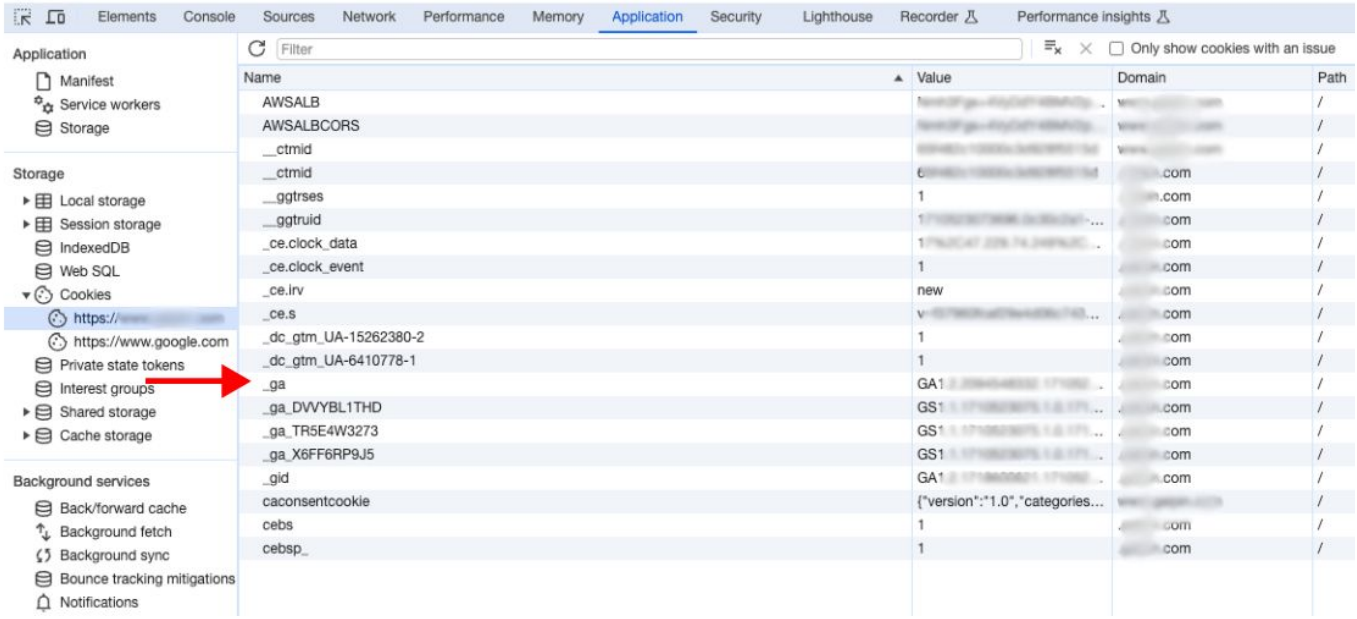
Step Five: Typically one or more domains will appear in a drop-down list. The most relevant cookies will be found in the domain for the website that you're visiting. Click the domain you are interested in and the list of cookies will appear in the window.

Once you are viewing the cookies, it can be difficult to make sense of the various letters and numbers, the screenshots on the next page point out a few relevant points and illustrate the effect of a cookie blocking banner.

Appendix 2: Website Cookie Screenshots

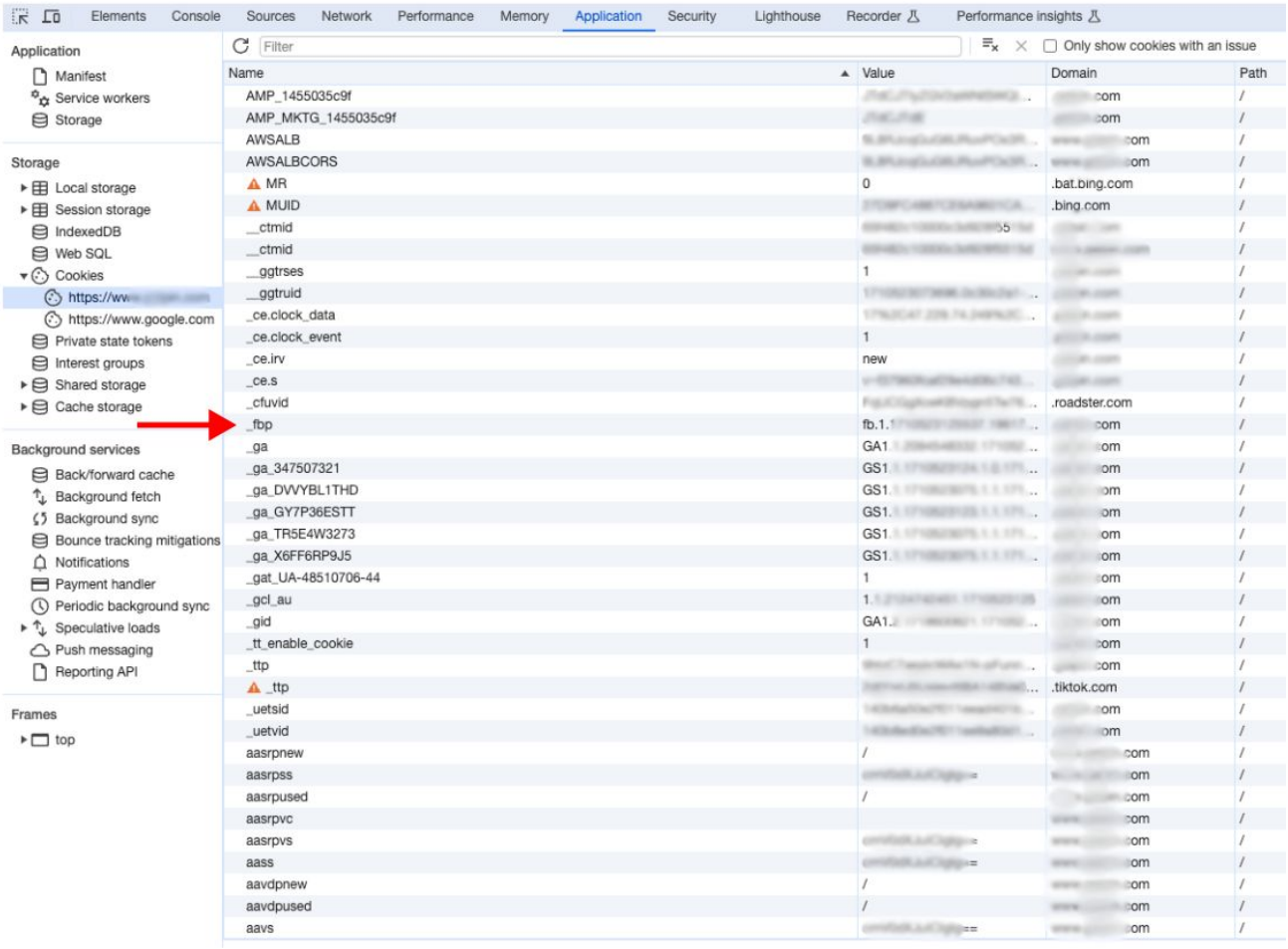
B. Representative Screenshots

The image below, is a view of a dealership website with identifying information blurred out. This website has been configured to block targeting cookies but to load analytics and functional cookies. This image shows the cookies that have loaded before the user accepts or declines the cookie banner. The cookies that begin with "_ga" (noted with the red arrow) signify Google Analytics cookies.



The next image shows the additional cookies that are set once the user accepts all cookies via the cookie banner. Note the new cookie "_fbp" (noted with the red arrow) that has appeared; this is the Meta Pixel. This tracking pixel was initially blocked but once the user accepted cookies, it was activated. If the user declined cookies, the view would remain the same as in the image above.

Appendix 2: Website Cookie Screenshots



The domain column indicates the domain that set the cookie. The blurred domains are the dealer's website domain. Interestingly, the Meta Pixel indicates that it was set by the dealer's domain, however as discussed in the guide, we know that with the Meta Pixel, data is transmitted directly to Meta/Facebook. Thus, even though it appears to be set by the dealer, it is in fact a third-party cookie. This can be verified by inspecting the "Network" tab, which would reveal a network request sending information to the Facebook.com or Meta.com domain.

About the authors



Mark Sanborn
Senior Product & Regulatory Counsel

With over a decade of experience in the automotive industry, Mark has served as both outside counsel and in-house counsel for a wide variety of dealers groups, and has developed a nuanced understanding of both the operational and legal challenges facing dealerships. Mark joined ComplyAuto in 2024.



Christopher Cleveland
Co-Founder & CEO

Chris Cleveland, CEO and Co-Founder of ComplyAuto, has over a decade of experience in automotive regulatory compliance. At Galpin, he led the compliance team through over 40 routine audits across various domains, including sales, finance, and information security. At ComplyAuto, he leverages his dealership expertise to develop software solutions that mitigate dealership legal risks. Chris lives in Utah with his family.

An innovative hub of former dealership employees, techies, compliance experts, and lawyers, ComplyAuto is known for bringing cutting edge technology to the market and disrupting how dealerships do business. Whether it's HR, employee and customer safety, privacy and cybersecurity, or F&I, sales and advertising, ComplyAuto offers a suite of cloud-based solutions that help dealerships focus on what they do best - sell and service vehicles. With 10,000 dealerships across the country and endorsements from 40+ state dealer associations, ComplyAuto is the leading regulatory compliance organization in the US.

CNCDA
California New Car Dealers Association

For 100 years, CNCDA has protected and promoted the interests of California's franchised dealers. We provide top-notch compliance and educational resources for our new car and truck dealer members. As the nation's largest state association of franchised dealers with nearly 1,200 members, CNCDA is highly active, ensuring our collective voice is heard in Sacramento.

COMPLYAUTO

CNCDA California New Car Dealers Association CELEBRATING 100 YEARS

A Dealer Guide to Online Tracking & Cookie Consent Management

