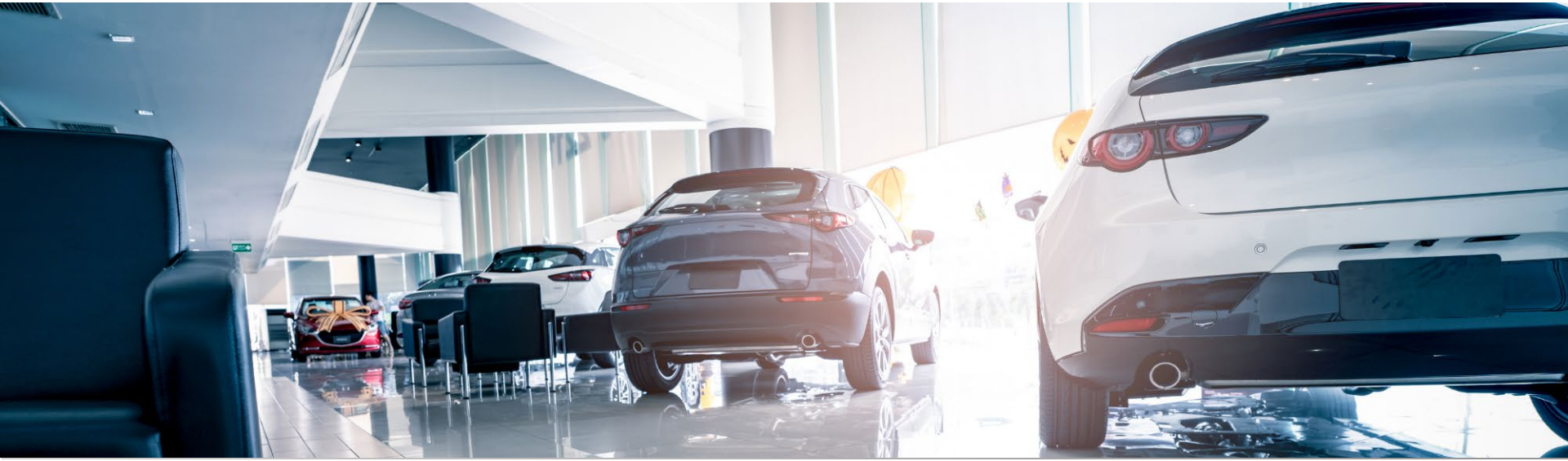


Website Compliance for Dealerships: Litigation and Regulatory Risks Are Growing

Thursday, February 26, 2026

Upcoming Webinar Schedule

March 5

A Dealer's Playbook for Handling Complaints

with LaBonte Law Group

March 12

Dominate AI Search with Reputation or Get Left Behind

with DAS Technology

Visit www.gnyada.com/events to register

Lincoln Tech Career Fair

LTI Queens Campus, New York City

Thursday, March 12, 2026:

- 10 AM – 1:30 PM
- 6 PM – 8 PM

Discover New Talent!

Connect with qualified Lincoln Tech students and conduct on the spot interviews. Find your next auto tech!

For more details, please reach out to Jeremy Mercado at 718.746.5900 or jeremy@gnyada.com.

COMPLYAUTO

GNYADA
Greater New York Automobile Dealers Association

Website Compliance for Dealerships: Litigation and Regulatory Risks Are Growing

February 26, 2026

Presenter

Brad Miller

CEO and Chief Legal Officer

16+ years at NADA - Chief Regulatory Counsel

Legal Disclaimer and Notice

This presentation is intended to be used as a compliance aid. Reasonable efforts have been made to ensure the accuracy and completeness of the following subject matter. No express or implied warranty is provided respecting the information contained in this presentation. **The following material is not legal advice and should not be construed as (nor used as a substitute for) legal advice.** If legal advice is required, the services of a competent professional should be sought. Each dealer must rely on its own expertise and knowledge of law when using the material provided.

By Dealers. For Dealers.

#1 Recommended compliance solution

10,000+ Active dealers across all 50 states

43/50 State dealer association endorsements

200+ Years of combined experience in the automotive industry

Many staff are former dealership employees and even more have worked in the automotive industry

Agenda

- Background and Overview
- Legal Theories & Potential Risks
  - Practical Implications
  - Regulatory Enforcement
- Strategies and Solutions to Avoid Becoming a Target
- AI Cookie Classification

COMPLYAUTO

Background and Overview

Dealer Website Evolution

- Dealer websites have become the center of online commerce/digital retailing.
- Today’s dealership websites do far more than show inventory. They capture leads, process financing pre-qualifications, and offer chat-based support.
- Each interaction generates valuable behavioral data. This data flow turns a passive website into a real-time customer profiling engine—posing serious privacy and compliance challenges.

Business and Legal Implications of Online Tracking

- The data collected—credit info, chat interactions, browsing behavior—is often sensitive and personally identifiable.
- If shared with third-party advertisers or OEMs without informed consent, dealerships risk lawsuits, reputational harm, and regulatory action.
- Loss of control over data can also dilute competitive advantage.

What Are Cookies and Tracking Technologies?

- Cookies store user info like session data or preferences.
- But modern tracking includes invisible pixels, JavaScript-based scripts, and session replay tools that log clicks, hovers, and even keystrokes.
- These tools operate silently in the background, often without the user’s knowledge.

Key Tracking Tools (Pixels, Scripts, Session Replay, Chat)

- **Pixels**: Track user activity and send data to third parties like Meta.
- **Scripts**: Collect interaction data; may continue to operate after a page loads.
- **Session Replay**: Records a user's session for analytic playback.
- **Chat Modules**: May record personal communications and send transcripts to external vendors.
- These tools are embedded deep in dealer websites, frequently without proper consent mechanisms.
- These are often bundled with advertising and analytics services. Though sometimes labeled as "cookies," they go far beyond simple site preference tracking and are central to most wiretapping and privacy claims.

Cookie/Script/Pixel Purpose Overview

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, enabling shopping cart, 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 enable error reporting, and facilitate optional features such as chat module interaction.
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, Tracking	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, and facilitate retargeting.

Marketing

*Pixels are typically Analytics or Targeting

What is the Practical Impact of Consent?

- There is more going on with your websites than you may realize.
- It’s a bit complicated to decipher, but very easy to see.
- Remember - its publicly available to anyone on the internet.
- Work with your website vendors to learn more, but here’s a sample….
  (random and anonymized)

COMPLYAUTO

How Can You Determine What is Happening on your Sites?

- There is more going on with your websites than you may realize.
- It’s a bit complicated to decipher, but very easy to see.
- Remember - its publicly available to anyone on the internet.
- Work with your website vendors to learn more, but here’s a sample….
  (random and anonymized)

COMPLYAUTO

Note That...

- There was a cookie banner on that site, but..
  - All these cookies and scripts were running before any consent was given (or required)
- Determining what is set in your domain can be complicated - and may be an indication of practices someone is trying to disguise
- You also need to understand website structure
  - iFrames? (chatbots, other tools?)
  - Subdomains? - Have their own policies, or follow yours?

Legal Theories & Potential Risks

Legal Issues

Various Website Tracking Tools Raise a Number of Complicated Legal Issues:

- State Private (increasingly class action) Lawsuits
- Federal Private Lawsuits
- State Privacy Law Issues
- Federal UDAP Enforcement
- State UDAP Enforcement

Legal Theories Asserted Vary

- **Federal Wiretapping - Violation of federal wiretapping laws by using third-party cookies to track consumer activities and share information without consent.**
- **FTC Act Section 5 or State (UDAP) - collecting & sharing sensitive information via tracking and advertising cookies/tech. without consumer consent/ banner doesn't work as stated and/or privacy policy is deceptive.**
- **State Wiretapping & "Pen Register" Surveillance (hundreds of lawsuits filed recently).**
- **Recording Communications without all parties' consent Tracking cookies and chat modules violation of state laws that require consent of all parties to record "communications."**
- **State Privacy Laws - Violations of specific state privacy laws**
- **Common Law Claims -** Invasion of privacy;Intrusion upon seclusion; common law fraud, deceit, and/or misrepresentation; unjust enrichment; and trespass to chattels.

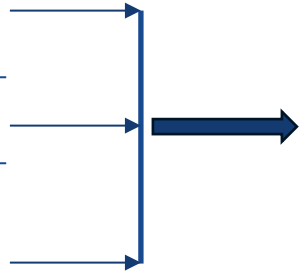
COMPLYAUTO

Isn’t “Wiretapping” Just an Issue in California?

- No - Majority of cases are still from CA law firms, but many defendants are not from CA.
- *Briskin* case - opens new doors to extraterritorial application
- “Highest” risk jurisdictions as of today? - CA, PA, IL, FL
  - One of the reasons we provide Geofencing tools in our software
- Increasingly using “tester plaintiffs
- Thousands of demand letters all over the country - including to dealers

State And Federal Statutes

Statute	Penalties	Conduct Regulated
California's Invasion of Privacy Act ("CIPA")	$5,000 per violation	• Interception of communication "content" (Wiretap) • Collection of "addressing" information (Pen Register/Trap and Trace)
California's Confidentiality of Medical Information Act ("CMIA")	$1,000 plus per violation	• Disclosure and/or negligent maintenance of confidential medical information
California Consumer Privacy Act ("CCPA")	$100 - $750 per violation	• Inadequate protection of personal information
California Unfair Competition Law ("UCL")	Profit disgorgement	• Unfair, unlawful, and/or fraudulent business practices
Federal Video Privacy Protection Act ("VPPA")	$2,500 per violation	• Unauthorized sharing of video watching information
Federal Wiretap Act	$100 - $1,000 per violation	• Interception of communication "content"
Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA")	$1,000 per day	• Interception of communication "content"



Not just a California issue; nearly every state has some version of a wiretap statute

Wiretapping/CIPA Foundations

- The California Invasion of Privacy Act (CIPA) prohibits the interception of communications, or recording of confidential communications, or use of a pen register or trap and trace device without the consent of all parties.
- Plaintiffs increasingly allege that chat tools and behavioral trackers qualify as unlawful surveillance.
- Similar claims arise under the federal Wiretap Act and state-level equivalents (e.g., PA, FL, IL).
- **CIPA is Not Just Limited to California:**
  - CA residents suing out-of-state businesses (including dealers) based on CA law.
  - "Tester" plaintiffs that work with certain law firms to visit websites seeking violations.

Expanding Claims: UDAP & State Privacy Law Theories

- Even in states without wiretapping statutes, plaintiffs invoke UDAP (Unfair and Deceptive Acts and Practices) laws. These claims argue that consent banners, disclosures, or vendor behavior mislead consumers or misrepresent privacy safeguards.
- Regulators are beginning to treat misleading banner design as a deceptive trade practice.
- Regulators are also waking up to the fact that many cookie banners and website privacy policies lack required notices and consumer options required under state privacy laws
  - CPPA Honda enforcement action
  - New York Attorney General Guidance
  - Oregon Attorney General Investigations

The Rise of Class Actions

- To date, the majority of claims have been individual claims, seeking statutory damages
- Recently - a number of class action claims have been filed, and many are currently working their way through the courts
- In general - tied to UDAP (state or federal) and based on the allegation that the banner/privacy policy/terms of use were deceptive
    - That is - the banner did not function as it claims it did
- Of course if successful, this changes the risk calculus materially
- Automotive retail is a key target: plaintiffs are suing not just dealers, but also their website providers, inventory listing services, and finance companies.

Practical Implications

Practical Implications

- Lots of people want this data
  - Dealer themselves
  - OEMs
  - Vendors
  - Marketing Companies
  - Big Data Companies
- There can be a tradeoff that dealers need to understand - providing a choice means some people will choose “no”
- Implementing a compliant banner WILL have an impact on data collected

The Numbers

There is still plenty of data to make good marketing decisions.

63% ACCEPT ALL COOKIES

19% ACCEPT SOME

18% REJECT

Baby Boomers have highest rejection

GenZ & Millenials have the highest acceptance

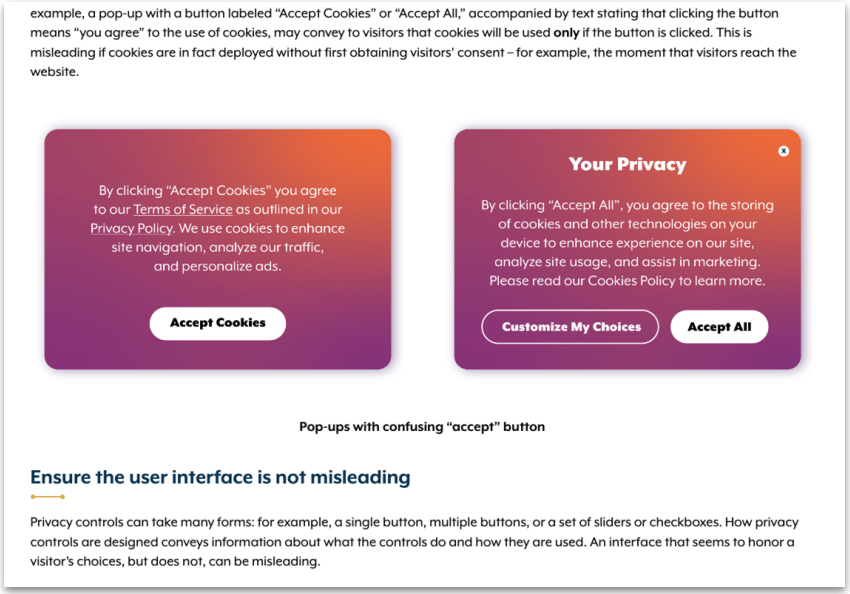
Some Third Parties Are Pressuring Dealers

- Compliance means some consumers opt out
- Marketing companies lose access to certain data
- As a result, many are:
  - Trying to obfuscate or hide retargeting cookies, and/or
  - Pressuring dealers to weaken or eliminate compliant consent tools
- As a Dealer - ask:
  - Why does that matter to them? Does it really matter to you?
  - Why are they asking you to increase your legal exposure.
- Note also - many of these companies share this information with the OEM

Regulatory Enforcement

NY AG Guidance

- On July 30, 2024, the Attorney General James' office issued a comprehensive guide on cookie consent banners which includes a business guide - "Business Guide to Website Privacy Controls"
- Lays out specific "dos and don'ts" and "mistakes to avoid"
- The guidance is consistent with ComplyAuto's guidance on these issues including:
  - Categorization of cookies/tags
  - Blocking cookies prior to loading
  - Clarity of language and choices
  - Avoiding "dark patterns"



example, a pop-up with a button labeled "Accept Cookies" or "Accept All," accompanied by text stating that clicking the button means "you agree" to the use of cookies, may convey to visitors that cookies will be used **only** if the button is clicked. This is misleading if cookies are in fact deployed without first obtaining visitors' consent – for example, the moment that visitors reach the website.

By clicking "Accept Cookies" you agree to our Terms of Service as outlined in our Privacy Policy. We use cookies to enhance site navigation, analyze our traffic, and personalize ads.

Accept Cookies

Your Privacy

By clicking "Accept All", you agree to the storing of cookies and other technologies on your device to enhance experience on our site, analyze site usage, and assist in marketing. Please read our Cookies Policy to learn more.

Customize My Choices | Accept All

Pop-ups with confusing "accept" button

Ensure the user interface is not misleading

Privacy controls can take many forms: for example, a single button, multiple buttons, or a set of sliders or checkboxes. How privacy controls are designed conveys information about what the controls do and how they are used. An interface that seems to honor a visitor's choices, but does not, can be misleading.

COMPLYAUTO

NY AG Guidance - Impact?

- First clear AG guidance of its kind
  - What does this mean for potential enforcement?
- New York does not yet have a omnibus state privacy law
  - There is no specific state wiretapping or recording statute cited
- The AG cites to generalized "privacy" concerns under UDAP. The Guide states:

  However, businesses' privacy-related practices and statements are subject to New York's consumer protection laws. These laws, which prohibit businesses from engaging in deceptive acts and practices, effectively require that websites' representations concerning consumer privacy be truthful and not misleading. This means that statements about when and how website visitors are tracked should be accurate, and privacy controls should work as described.

State Law Regulatory Implications Growing

Now - 19 states that have omnibus state privacy laws

- Almost all address retargeting cookies
- Generally require you to provide an opt-out (separate from your banner)
- Implications under state data processing requirements for prohibiting the “sale” of such information
  - Must properly handle consumer data requests
  - Must also oversee third party vendors
    - Just like you must obtain contract amendments from vendors under GLB, you must obtain different contract amendments under state laws
      - And they can vary by state
- Bottom line - these laws, and the implications of cookies under them, can be very complicated
- And now, states are starting to enforce….

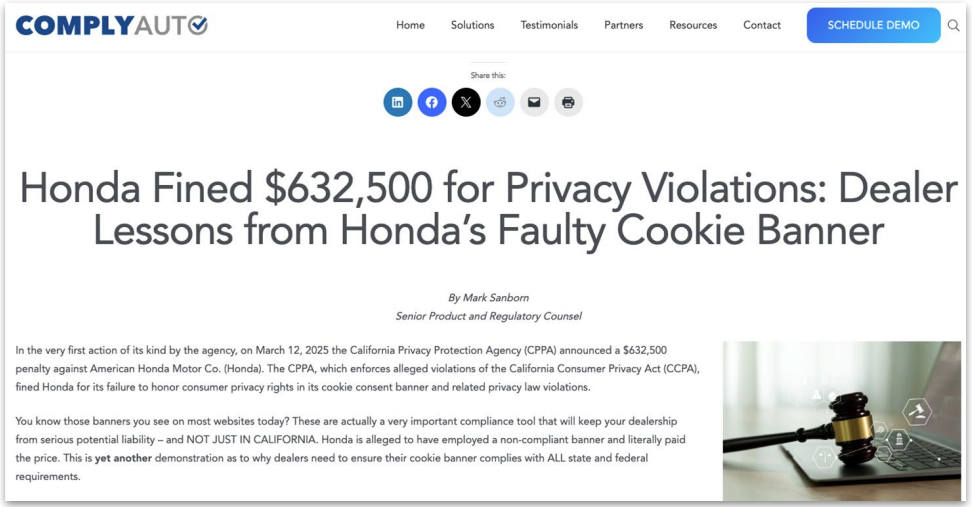
COMPLYAUTO

California CCPA Enforcement - Honda Motor Co.

In first action of its kind - CPPA (state enforcement agency) fined Honda over $632,000

March 12, 2025

- **Non-compliant cookie banner**
- **Improperly handled consumer data requests**
- **Failure to oversee third party vendors**



COMPLYAUTO

Home Solutions Testimonials Partners Resources Contact SCHEDULE DEMO

Share this:

Honda Fined $632,500 for Privacy Violations: Dealer Lessons from Honda's Faulty Cookie Banner

By Mark Sanborn
Senior Product and Regulatory Counsel

In the very first action of its kind by the agency, on March 12, 2025 the California Privacy Protection Agency (CPPA) announced a $632,500 penalty against American Honda Motor Co. (Honda). The CPPA, which enforces alleged violations of the California Consumer Privacy Act (CCPA), fined Honda for its failure to honor consumer privacy rights in its cookie consent banner and related privacy law violations.

You know those banners you see on most websites today? These are actually a very important compliance tool that will keep your dealership from serious potential liability – and NOT JUST IN CALIFORNIA. Honda is alleged to have employed a non-compliant banner and literally paid the price. This is **yet another** demonstration as to why dealers need to ensure their cookie banner complies with ALL state and federal requirements.

Recent FTC Cookie Consent Actions (UDAP)

FTC Notice of Penalty Offenses to GLBA-Covered Entities

- FTC sent a notice[1] to several GLBA-covered businesses (primarily tax prep) regarding collection of confidential consumer information without express informed consent, including by use of tracking technologies (cookies, pixels, etc.)

Consumer Consent to Targeting and Advertising Cookies

- *FTC v. GoodRx* (Feb. 2023) - GoodRx violated the FTC Act by collecting, using, and selling consumers' sensitive information to advertising companies like Facebook, Google, and Criteo, including prescription medication, personal health information, and contact information.
- *FTC v. BetterHelp* (July 2023) - BetterHelp violated the FTC Act by collecting, using, and selling consumers' sensitive information without receiving their consent. Furthermore, the consumers' health information was shared for advertising or advertising-related purposes.

[1] https://resources.complyauto.com/privacy/resources/7b75a27a-daad-4bad-af63-820654c655fa.pdf

9th Circuit: *Briskin v. Shopify* – Jurisdiction Over Companies Placing Cookies

- The 9th Cir. ruled in Briskin v. Shopify (Apr. 21, 2025) that placing tracking cookies on a device located in a state establishes personal jurisdiction in that state—even without other business contacts.
- Shopify was sued by a California resident over cookies collecting browsing and device data without clear consent.
- The court found that interacting with a user's device located in California was sufficient "purposeful direction," allowing California courts to hear the case.

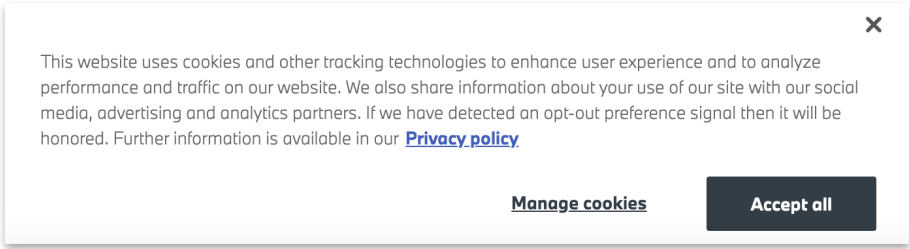
Key Takeaway: Any business, including out-of-state dealers and vendors, can be hauled into court wherever a tracked user resides.

This potentially opens the floodgates for CIPA claims against defendants located outside of California.

COMPLYAUTO

Beware of Dark Patterns!

- Not all cookie banners are created equal; both state Attorneys General and the FTC have warned against the use of “dark patterns” in cookie consent banners (CA has outright banned certain dark patterns)
- Dark patterns, in the context of cookie consent banners, are design practices that are meant to trick users into conceding their privacy rights or “nudge” them into accepting cookies.
- Examples include the use of small fonts, lack of options besides accepting cookies, manipulative designs, and obscuring key information.
- Dark Patterns are considered a UDAP violation and will not satisfy “express and informed consent”



Lastly …. A Note about “Email Cookies”

- A newer topic at issue in lawsuits this year is email pixel tracking, also known as “spy pixels.”
- Email tracking pixels are similar to web pixels but are embedded in emails rather than websites
- Basis is unclear - seems to be focused on claims coming out of Florida
- Work with email vendors to address

Strategies and Solutions to Avoid Becoming a Target

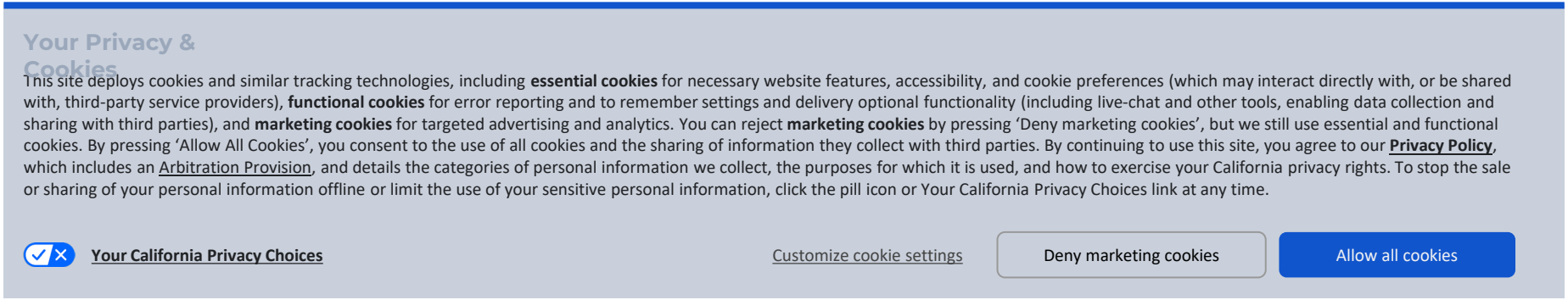
(Hint: Get Consent)

Solutions to These Various Issues

Cookie Consent Banner and Comprehensive Privacy Policy

- **Cookie Banners** - A ***compliant*** cookie consent banner prevents marketing cookies and tracking pixels from loading until a consumer consents to it by clicking "accept." Obtaining clear consent is fundamental to addressing all these issues. Banner should include a link to the privacy policy to ensure that users are also well-informed about the specifics of data collection and usage.
- **Privacy Policy** - These should disclose website tools that collect and share information, detailing exactly what categories of information are collected and who they are shared with. Consider adding chat module and session replay tool disclosures in the privacy policy. Consider arbitration agreement.
- **Disclosure in chat module** - Work with chat module providers to include a conspicuous disclosure that notifies consumers that sensitive information sent in the module may be shared with third parties.

Cookie “Banner”



- Auto blocks all marketing cookies until user accepts banner.
- Provides notice of sharing with third parties.
- Has translation options upon deployment.
- User consents to hyperlinked Privacy Policy and receives notice of arbitration provision.
- Allows user ability to customize settings.
- Geofencing is available to serve up to residents in certain states

COMPLYAUTO

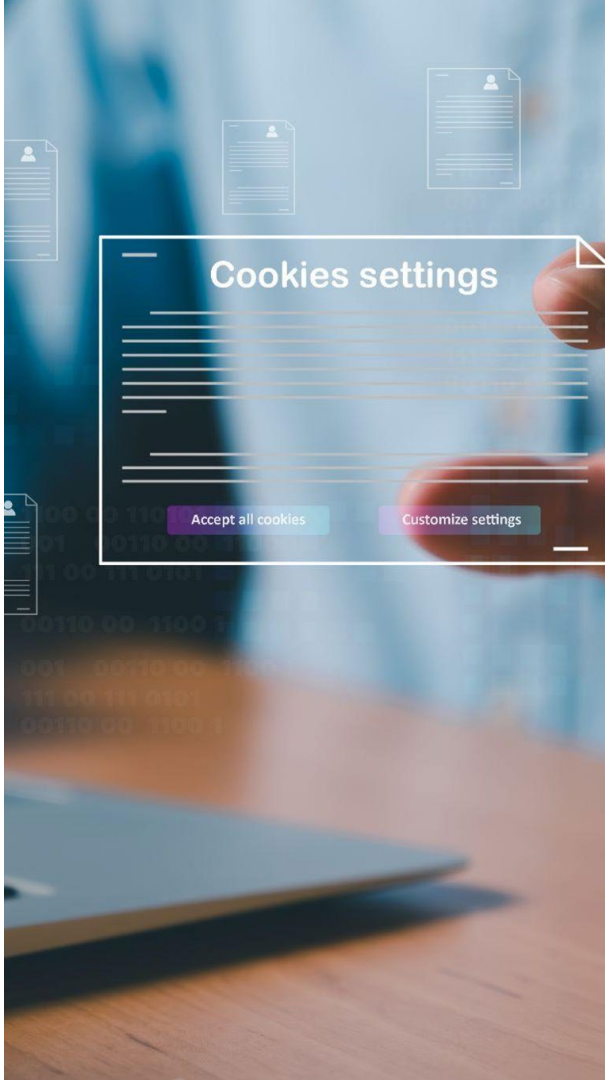
What Can Dealers (and others) Do To Protect Themselves?

- **Consent** - Obtain affirmative, express consent of users to allow collection of their data. Remember that this consent cannot be coerced, confusing, or limited.
- **Policies -** Draft and update a valid and comprehensive Privacy Policy
- **Practices:**
  - Understand what is happening on your own websites!
  - Route the Data Through You: Do not allow providers to receive user data directly—intercepting it before it reaches you, the intended recipient. Instead, route it through your business' systems/servers first.
  - Limit the Content Recorded: Dismissal is more likely if your provider only records basic information rather than interactions exposing more personal details.
- **Contracts** - Ensure all provider agreements specifically state that the provider won't sell or share the data or use it without express consent
  - This means, chat modules, website providers, OEMs, website tools, schedulers, any third party.

COMPLYAUTO

What Else Can You Do?

- Ask your website vendors what is happening on your sites and why.
  - Often, just asking can illuminate a number of issues
- Ensure you have a compliant cookie banner that is tied properly to your DSAR and privacy policy.
- Make a corporate decision - involve marketing and legal to reach a balance **in terms of functionality and your state and legal posture.**



Bottom Line For Dealers

It's NOT JUST CALIFORNIA! - ALL DEALERS NATIONWIDE NEED A PROPER BANNER

- Other states have wiretapping statutes
  - And Federal Wiretap Act
  - PA, IL, FL in particular are "higher risk" (MA case 12/24)
- CIPA - brought against dealers nationwide
  - *Briskin* - makes that even more likely
    - CIPA/CCPA?/Other Privacy and consumer protection laws?
- Plaintiffs bar is continuing to be "creative" (rise in email pixel cases)
- State Privacy Laws are an *independent* source of risk - But remember, this is not *just* a state privacy law issue

Bottom Line For Dealers - (continued)

All Dealers Need A Banner That Works!

- Having a “sham” banner creates more risks than not having one at all
  - Rise of class actions ties to deception in banners and privacy policies
  - This highlights the need for the banner and policy to work together and be clear and accurate
- Consider a website “Terms of Service” that covers this and other legal issues.
  - A contract - may wish to consult your attorney
- Litigation and Regulatory Risk aside
  - You **NEED** to know what is happening on your websites.
  - It’s a critical business responsibility of the dealership

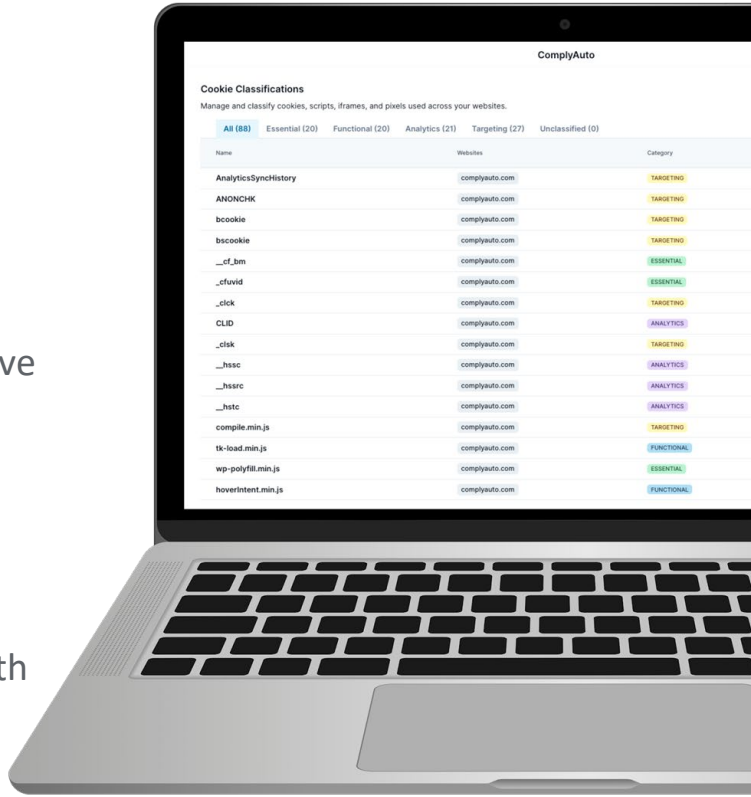
COMPLYAUTO

COMPLYAUTO PRIVACY

AI Cookie Classification & Control

Gain granular visibility and control over what loads on your website.

- **Scan & Categorize:** AI identifies and classifies cookies into Essential, Functional, Analytics, or Targeting categories.
- **Review Queue:** Flags 'Needs Review' items so you can approve classifications or block risky scripts before they load.
- **Granular Dashboard Control:** Disable specific cookies or scripts directly from the ComplyAuto dashboard—no coding required.
- **Auto-Blocking:** Automatically blocks cookies on websites with failed or incomplete scans to ensure safety.



COMPLYAUTO

Privacy

FTC Safeguards, Cybersecurity
& Privacy Rights Management

Safety

Environmental Health & Safety

Guardian

F&I, Sales,
and Advertising Compliance

Workforce

HR Policies & Training

ComplyCrypt

Secure end-to-end encrypted messaging

DealCheck Ai

AI Powered Deal Audits

Questions?

We’re here to help! Questions?

Brad Miller

CEO/Chief Legal Officer

brad.miller@complyauto.com

Schedule a demo

10,000+ active dealers across all 50 states

43/50 state dealer association endorsements

NADA AFFINITY PROVIDER

COMPLYAUTO

COMPLYAUTO

By Dealers. For Dealers.