COMPLYAUTO

Oregon Auto Dealers Assn Webinar:

Oregon Consumer Privacy Act and Cookie Banner Update

June 20, 2024

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.

Presenter

Brad Miller

Chief Compliance/
Regulatory Officer
Head of Legal

16+ years
Chief Regulatory Counsel
National Automobile Dealers
Association

COMPLYAUTO

Agenda

I. Oregon Consumer Privacy Act (OCPA)

II. Cookies / Related Tracking Technologies

   A. Overview

   B. Legal Framework and Legal Theories

   C. Strategies and Solutions to Avoid Becoming a Target

   D. Practical Considerations - Effects of Limiting Marketing Cookies

III. Q&A

COMPLYAUTO

I. Oregon Consumer Privacy Act

Oregon Consumer Privacy Act

On July 18, 2023, Oregon governor Tina Kotek signed the Oregon Consumer Privacy Act (the Oregon Consumer Privacy Act or "OCPA")

- Oregon is the 18th state to enact comprehensive data privacy legislation.
- The OCPA will take effect on July 1, 2024.
- It does NOT contain a private right of action.
- The Oregon AG has exclusive authority to enforce violations.
- However, 30 day right to cure - until 1/1/2026
- The AG may seek civil penalties of $7,500 per violation.

To Whom Does the Oregon Consumer Privacy Act apply?

Transparency and disclosure obligations on a "controller" (an individual or legal entity who, "alone or jointly with another person, determines the purposes and means for processing personal data") who either: (1) conducts business in Oregon; or (2) produces products or services that are targeted to the residents of Oregon; **and** that during a calendar year:

- controls or processes personal data of not less than 100,000 Oregon residents, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- controls or processes personal data of not less than 25,000 Oregon residents and derives more than 25 percent of its gross revenue from the sale of personal data.

Notably, the OCPA does not have a revenue threshold for entities to be subject to privacy obligations.

It also does not apply to certain classes of data, including consumer credit-reporting data, employment-related information, and data processed pursuant to GLBA.

What Rights Does the OCPA Grant to Consumers?

OCPA grants Oregon "consumers" (individuals not in a commercial or employment context), certain access and control rights concerning their personal data. Including the right to request to:

- confirm whether the controller is processing the consumer's personal data;
- obtain a copy of the consumer's personal data (i.e., data portability);
- correct inaccurate personal data of the consumer;
- delete personal data about the consumer;
- disclose, at the controller's discretion, the list of third parties to whom the controller has disclosed the consumer's, or any consumer's personal data;
- opt out of the processing of the consumer's personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer (profiling); and
- revoke previously given consent to process the consumer's personal data, which must be honored within 15 days of receiving the request.

COMPLYAUTO

How Must A Controller Honor Those Rights?

- A controller must respond to consumer requests to exercise their rights within 45 days.
- The controller may extend that time period for an additional 45 days when reasonably necessary considering the complexity and number of the consumer's requests, but must notify the consumer.
- Controllers must provide information once every 12 months without charge
- Consumers can appeal the controller's refusal to take action on requests to exercise their rights.
- A controller must respond to an appeal in writing within 45 days and, if the appeal is denied, the controller must provide the consumer with a method for contacting the Oregon Attorney General.

What Data Does the OCPA Seek to Protect?

OCPA generally applies to "personal data." Personal data is defined as any information that is linked or reasonably linkable to a consumer or to a device that is reasonably linkable to a consumer.

The definition of personal data excludes de-identified data or publicly available information.

It also imposes certain duties and restrictions on “sensitive data,” which includes information such as:

- Race or ethnicity, national origin, citizenship or immigration status, status as transgender or nonbinary;
- Genetic or biometric data, or;
- specific geolocation data.

What Obligations Does the OCPA Impose on Controllers? - Privacy Policy

OCPA requires controllers to provide a reasonably accessible, clear, and meaningful privacy policy that includes:

- The categories of personal data and sensitive data processed;
- The purpose for processing personal data;
- The manner in which consumers may exercise their rights, including how a consumer may appeal;
- A list of the categories of data shared with third parties, the categories of third parties, and, to the extent possible, how each third party may process data;
- An active email address or other mechanism that the consumer may use to contact the controller;
- The express purpose for which the controller is collecting and processing personal data;
- Clearly and conspicuously discloses if the controller sells consumers' personal data to third parties or engages in targeted advertising, and provide consumers an opportunity to opt out;
- A mechanism to allow consumers to exercise their right to opt out via an opt-out preference signal;

What Obligations Does the OCPA Impose on Processors?

OCPA requires processors (that process personal data on behalf of a controller) to assist the controller in meeting its obligations under the act, including its obligations regarding consumer rights requests and security of data processing, and to enter into contracts with processors that must:

- clearly set forth instructions for processing personal data,
- the nature and purpose of processing, the type of data subject to processing, the duration of processing,
- and the parties' rights and obligations.
- include a duty of confidentiality and
- require that processors only engage subcontractors pursuant to a written contract that requires the subcontractor to meet the same obligations of the processor with respect to the personal data.
- processors must also delete or return personal data upon the controller's request.

Bottom Line for Dealers

- The OCPA will take effect on July 1, 2024.
- If you process 100,000 or more customer records in one calendar year, it may apply to you.
    - Likely to apply to most dealers - remember, it's not just the DMS/CRM.
- Dealers will need to ensure that their Privacy Policy is compliant
    - that will require some inquiry into business practices.
- The GLB exception could - but likely will not exempt dealers.
- This may restrict some uses of data,
    - particularly sensitive data (e.g. geolocation) and data obtained from third parties (OEM)
- There are a series of consumer rights that you will need to be ready to honor.
- You are going to need to review and revise third party contracts
- You should understand and review your cookie practices

COMPLYAUTO

Bottom Line for Dealers (cont.)

- Consent (an "opt-in") required to process “Sensitive Data”
  - Most categories would be in person/by implication
  - Geolocation data?
- Opt-Out Rights before “selling” personal data or “Targeted Advertising.”
  - The OCPA defines the "sale" of personal data as "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." As noted above, controllers must provide consumers with the ability to opt-out of the selling of their personal data.
  - The OCPA defines "targeted advertising" as "advertising that is selected for display to a consumer on the basis of personal data obtained from that consumer's activities over time and across one or more nonaffiliated websites or online applications and is used to predict the consumer's preferences or interests."
- Do you “sell” personal data? (broader than you may think)

COMPLYAUTO

Bottom Line for Dealers - Areas of Dealer Focus

- Right to obtain - ensure you have process to provide in an encrypted manner
- All requests - ensure you have a process to verify identity without making it overly complicated (dark pattern)
    - Verifying "authorized agent" requests (can be risky).
    - Sometimes state rules on POA and related reqs.
    - GPC/DNT
- Deletion requests - Be prepared for exceptions and state/federal record retention requirements and to be able to articulate those exceptions in responses to consumers
- Importance of conducting a vendor and data inventory (dealers may not realize how much data they collect/share)
- Tracking the "service provider" agreement requirement
- Definition of "sale" (OEMs, valuable consideration, etc.)
- Privacy Policy needs to be updated consistently based on new vendors, sharing practices, collection practices, etc.
- For individual consumer, determining which categories of info collected is very challenging without some sort of data mapping tool

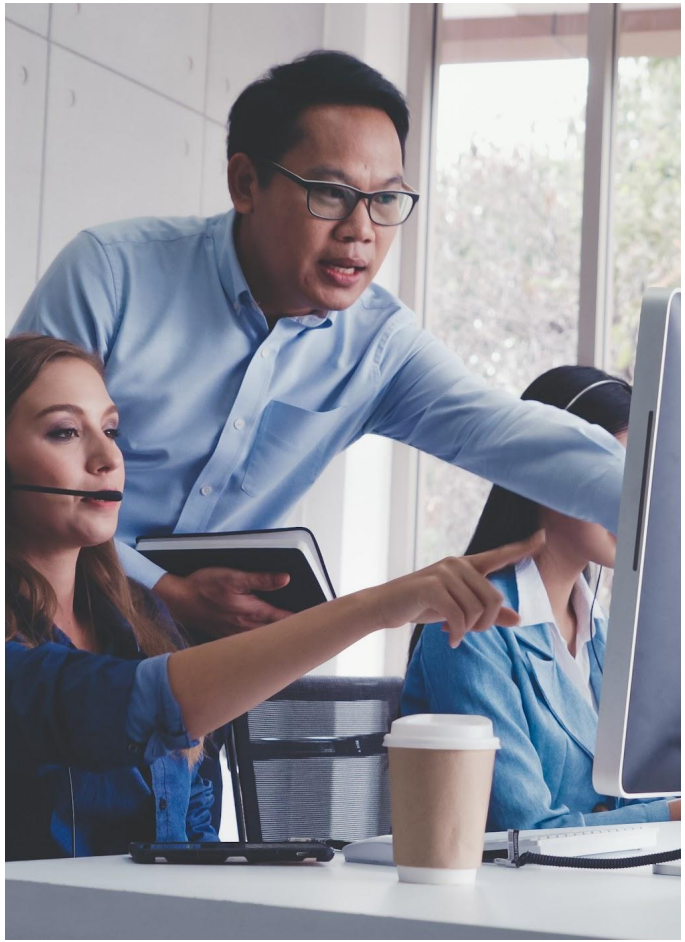
COMPLYAUTO

II. Background / Definitions of Cookies and Related Technologies

Cookies and Tracking Technologies - Overview

- Over the past few months, there has been a surge in lawsuits related to online tracking tech. Dealers are one of the latest industry targets, along with OEMs, website providers, and other automotive vendors.
- These claims have not been widely reported largely because the overwhelming majority settle before being publicized.
- Claims allege wiretapping and similar privacy violations in connection with common website tracking technologies like cookies, Google Analytics, Meta Pixel, and website chat modules.
- The merits of the arguments are often dubious, but the courts are currently split on how to handle these cases, and defending or settling these cases can be very expensive (similar to ADA cases).

COMPLYAUTO



Consent Banners:

What Are They and What Are the Potential Tradeoffs?

- The fundamental issue is what consumer consent will a dealer require before deploying analytics & retargeting cookies on a dealer website.
- Dealers must weigh the business vs legal risks. They could lose up to 40% of visibility into website traffic through tools like Google Analytics from high risk jurisdictions.
- Banners do <u>not</u> "eliminate" analytics or retargeting cookies. They simply ask the consumer for consent - and trends indicate that over 60% of customers accept all cookies.

COMPLYAUTO

Cookies

Definition

- A small text file created and set by a website or server and stored on the user's computer by the web browser while the user is browsing.

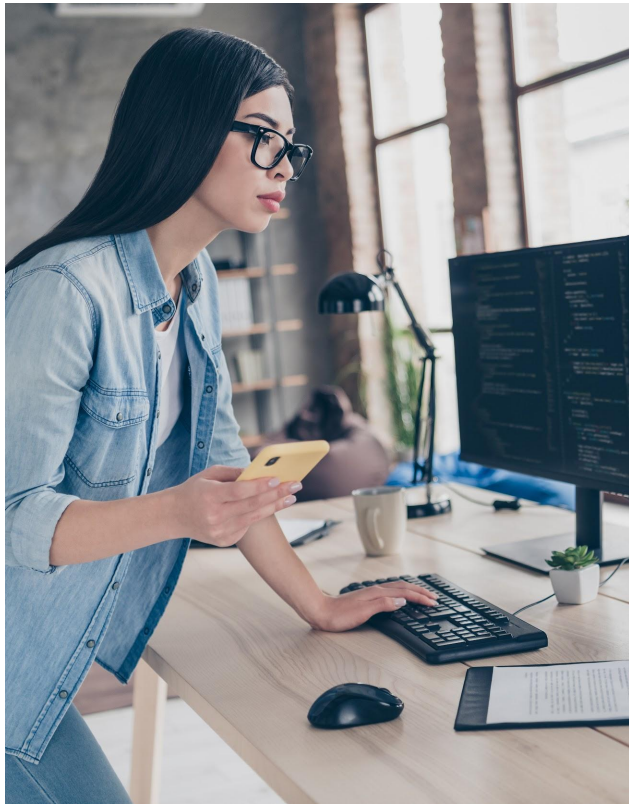
  Though they may be stored well after a user is done browsing the website that set the cookie.

- Used to remember information.

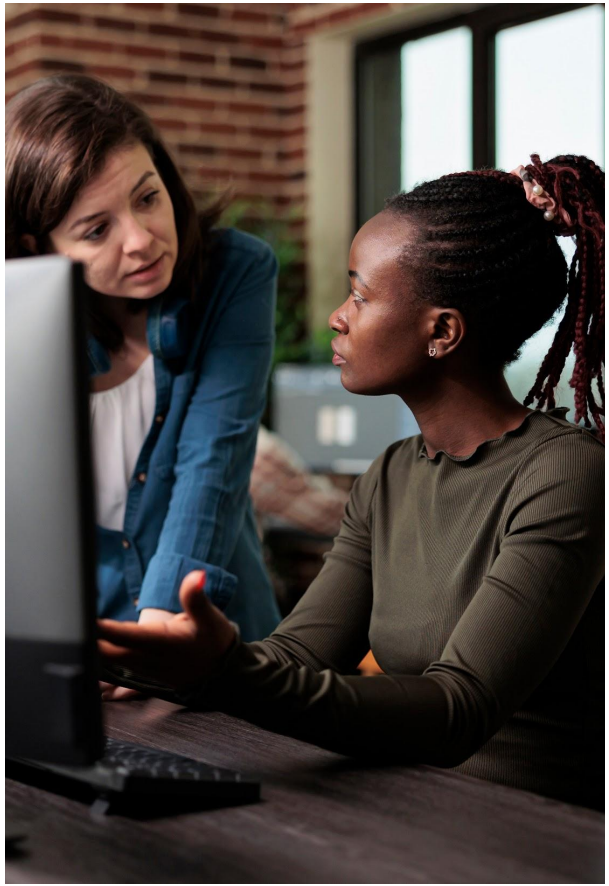
COMPLYAUTO

Other Tracking Technologies

- Tracking Pixels/Web Beacons
  - Small images or lines of code embedded on a website. Users cannot see the tracking pixel and may not know that they exist. Implemented using scripts.
  - 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 web page, items purchased, and information entered into forms on the site.
  - Well-known examples are Meta Pixel and Google Ads.
- Scripts
  - Essential components of modern websites that enable interactivity, functionality, and data collection.
  - 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.



COMPLYAUTO



Other Related Technologies

- Fingerprinting
  Tracking technique that involves collecting a variety of data points 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.
- Chat Modules
  - Interactive feature on websites that allows visitors to communicate in real-time with company or automated chatbots.
  - Chat modules can save and record communications and can collect data about customer interactions, preferences, etc.
- Session Replay
  Allows user's interaction with a website (clicks, page visits, etc.) to be recorded and replayed; used for analytics and marketing.
- Geolocation/Geotargeting
  Scripts and tools that collect and share precise geolocation data to identify a customers location and market to them based on their behavior and/or location history.

Cookie/Script/Pixel Purpose Recap

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

II. Legal Framework and Theories Targeting the Use of these Technologies

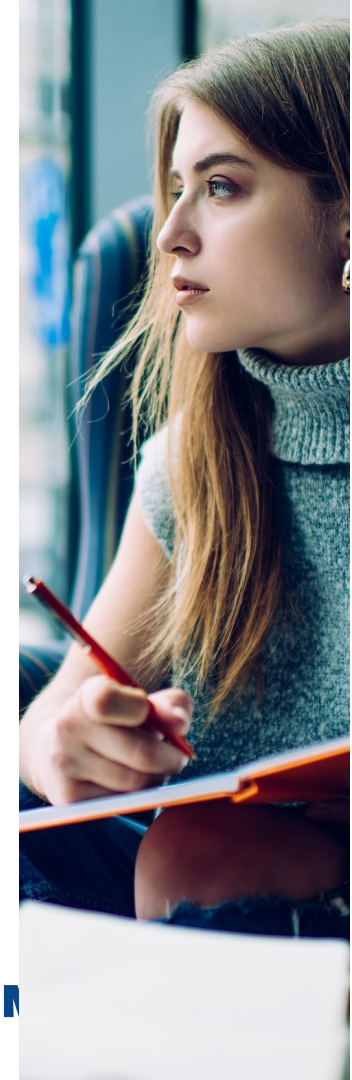
“Wiretapping Claims”

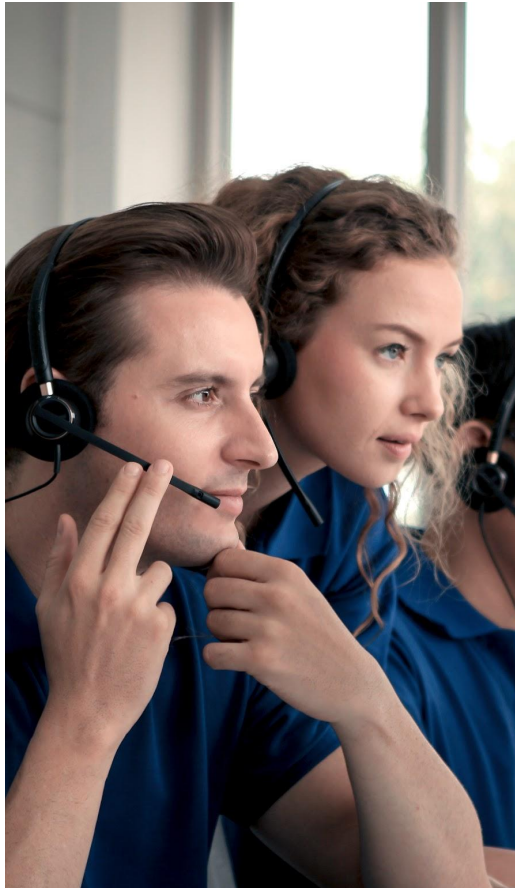
Since 2023, there have been hundreds of lawsuits filed against retailers and other businesses (including third-party service providers). It’s increasing in 2024.

- RODRIGUEZ v. FORD MOTOR CO.
- JESSE CANTU v. DEALER DOT COM, INC.
- SANTORO V. HYUNDAI MOTOR AMERICA
- D’ANGELO v. FCA US, LLC d/b/a DODGE
- SANCHEZ V. CARS.COM INC.
- RODRIGUEZ V. AUTOTRADER.COM
- KIRKHAM v. TAXACT
- MONICA SANCHEZ V. CARGURUS, INC.
- RODRIGUEZ V. AVIS RENT A CAR SYSTEMS
- RODRIGUEZ V. JAGUAR LAND ROVER NORTH AMERICA
- HASSON v. PARTS ID
- HUFF v. INTERNET TRUCKSTOP GROUP

Claims generally focus on the following

- Violation of state wiretapping laws (eavesdropping on website activity & communications without consent).
- Recording of confidential communication without consent.
- Use of illegal “trap and trace”and pen register devices.





California Invasion of Privacy Act (CIPA)

California Penal Code §§630-638

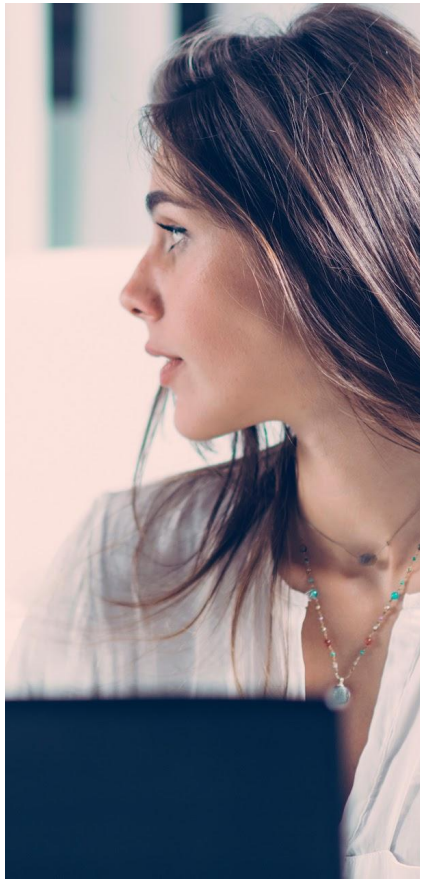
- Prohibits
  - Interception of communications (wiretapping) without consent of all parties,
  - Recording or eavesdropping on confidential communications, *or*
  - Use of a pen register or trap and trace device.
- "Pen register" means a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.

COMPLYAUTO

California Invasion of Privacy Act (CIPA) Continued

- "Trap and trace device" means a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication.
- Pen Register and Trap-and-Trace theories do not require that contents of communications be captured. Mere capturing of common signaling information is enough.
  - Some cases have been brought based on recording of IP address.
  - Kochava Case - suggests pen register applicable to internet, helped set off recent flood of litigation.

    Greenley v. Kochava, Inc., No. 22-CV-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023).
- Wiretapping claims not just based on California law.



Third Circuit Finds Interception in Website Wiretapping Case

Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121 (3d Cir. 2022)

When the plaintiff's browser loaded the retailer's website, the website told the plaintiff's browser to send a separate "GET" request to a marketing company used by retailer. Advertiser's server used a JavaScript code to place a cookie on plaintiff's browser and began sending information to marketing company about plaintiff's activities on the retailer's website.

- 3rd Circuit Court of Appeal held that deploying this type of software and placing cookies to send data about a website visitor's behavior to a third party 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.

COMPLYAUTO

Example:

[redacted]

February 21, 2024

[redacted]

Notice of Dispute and Demand
Protected Communication

Re: [redacted]
www.[redacted]

Please be advised that our client below has claims against your company for violation of California privacy law. This letter is a notice of dispute and demand sent pursuant to the pre-arbitration notice of disputes section of your terms and conditions. A synopsis of our client's claims, detailed information on those claims, the applicable law, a demand, the basis of the demand, as well as further settlement discussion points are below.

Claimant's Information

[redacted]

Governing Law

Under the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630 et seq ("CIPA"), a person whose communications are illegally tapped, read, or contents are learned is entitled to the following damages:

- $5,000 per violation, pursuant to Cal. Pen. Code § 637.2.

Courts have ruled that Cal. Penal Code § 631(a) of CIPA is not limited to phone lines, but also applies to "new technologies" such as computers, the internet, and email. See *Matera v. Google, Inc.*, 2016 WL 8200619 at *21 (N.D. Cal. 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.* 2006 WL 3798134 at *5-6 (N.D. Cal. 2006) (CIPA governs "electronic communications").

Under California common law, claims for intrusion upon seclusion and invasion of privacy involve a similar test, so courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive. *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (2020).

Basis for Demand

[redacted]("Respondent") utilizes tracking software, including a Meta Pixel, that allows Respondent to embed a JavaScript in the HTML code of Respondent's website that intercepts, tracks, stores, and analyzes Claimant's interactions with Respondent's website. By embedding the Meta Pixel within its website, Respondent aided Meta dba Facebook to intercept, store, and analyze Claimant's electronic communications for the purposes of data mining and targeted advertisement.

We downloaded the HTTP Archive Format ("HAR") file from Respondent's website which exposes the vast extent of wiretapping and data mining in which Respondent and its co-conspirator Meta engage. In addition to Meta, Respondent aids other companies in tapping and learning the contents of Claimant's electronic communications with Respondent's website.

Claimant realized this was occurring after finding a detailed list of interactions with Respondent's website in Claimant's personal Facebook account ("off-Facebook activity"). The interactions included Respondent's tracking analysis of Claimant's interactions, each labeled as an "Activity." The information found in Claimant's off-Facebook activity includes (1) Claimant's personalized ID number, (2) the date and time of the activity and (3) the event, or the activity itself (i.e. "Page View" or "Content"). The off-Facebook activity constitutes the tip of the iceberg of the information the Meta Pixel collects. The information in Claimant's Facebook account confirms Respondent embedded a Meta Pixel on Respondent's website which allowed Respondent and Meta to intercept, store, and analyze Claimant's communications for their commercial benefit. The images below depict two data sets which reveal just a snippet of the data obtained by Respondent and Meta by using Meta Pixel on Respondent's website.

Respondent utilizes the Meta Pixel to surreptitiously and covertly gather Claimant's electronic communications and data, which includes, but is not limited to: 1) a full-string, detailed URL for each page on Respondent's website that Claimant views and 2) the website folders and sub-folders on Respondent's web-server, which provides vast quantities of Claimant's data to Facebook. The Meta Pixel script embedded on Respondent's website allows both Respondent and Meta to surreptitiously tap and learn the contents of Claimant's electronic communications. This is the exact factual scenario of which Courts have been concerned; the surreptitious tapping and collection of user data for the purposes of future data mining and benefit.

The information Respondent aided Meta to intercept includes much more than Claimant's IP address and gives rise to serious invasions of privacy and inclusion upon seclusion claims. Respondent's invasion of Claimant's privacy occurred, as the Meta Pixel confirms, within milliseconds – a time where Claimant could not possibly read Respondent's Terms of Use and Privacy Policy, let alone agree to them.

Any alleged consent occurred well after the tapping began. The pixel spyware became active instantaneously upon visiting Respondent's site. Even if Claimant later consented to its use, it would have occurred well after the fact. Such was the case in *Javier v. Assurance IQ, LLC* where

COMPLYAUTO

the Ninth Circuit rejected retroactive consent for tapping website users. *Javier v. Assurance IQ, LLC*, No. 21-16351 (9th Cir. May. 31, 2022).

Such an intrusion is highly offensive even to the most reasonable consumer considering that Respondent willingly chose to embed the script on Respondent's website thereby aiding Meta to tap and collected Claimant's communications in a matter of milliseconds. This is not a case where Respondent can claim that the information collected was just for its own private consumption and therefore can avail itself to any "party exception" which could apply. The Ninth Circuit, along with the First and Seventh Circuits have held that the simultaneous, unknown duplication and communication of "GET requests" like those at issue here do not exempt a defendant from liability under the "party exception." Additionally, the key distinction in this case, separate and apart from other claims that Respondent may face, is that Claimant's data was collected instantaneously by both Respondent and Meta for the sole purpose of having the data aggregated, and then independently used and sold.

The images below depict two data sets which reveal just a fragment of Respondent's and Meta's data collection through use of the Meta Pixel which occurs instantaneously when a consumer visits Respondent's website.

(Image confirms Respondent includes Meta Pixel(s) on Respondent's website)

By way of further explanation, what typically occurs when Claimant visits Respondents website is that Claimant's internet browser sends a GET request to Respondent's website server, which causes the website to send the information requested by Claimant to Claimant. This communication usually only occurs between the user's web browser and the website being viewed. But on Respondent's website, Respondent placed JavaScript code that allowed Respondent and Meta to track visitor activity by directing the user's browser to copy the referrer header from the GET request and send a separate, but identical, GET request and the associated referrer header to Meta's server. This is the conduct Claimant alleges is unlawful.

The screenshot below provides a screenshot of the HAR file downloaded from Respondent's website and exposes the true extent of the data interception, collection, and dissemination in which Respondent engages. The screenshot is not of Claimant's interactions with Respondent's website; however, Claimant alleges the same data collection and dissemination occurred on the day(s) Claimant interacted with the website.

In this sample, Respondent's website received 90 GET requests from the browser with a total of 4.3 megabits of information collected and disseminated within seconds. Of the 90 GET requests, countless went to separate third parties which included, but were not limited to: Facebook, Google, Car Gurus, and Fox Dealer.

Settlement Demand

Claimant's Facebook data shows that Respondent aided and conspired with Meta to tap and learn the contents of Claimant's sensitive and private electronic communications on at least seven separate occasions within the last year. Claimant will testify to that at the arbitration hearing and the back-end data, confirmed by our expert, will support Claimant's testimony. Each such occasion constitutes a separate violation of Cal. Pen. Code § 631(a)with each violation allowing for $5,000 in statutory damages.

Respondent's seven interceptions results in a total of $35,000 in statutory damages under CIPA. Furthermore, GET requests sent to the above-identified third parties results in a total of $25,000 statutory damages under CIPA. Based on this information, the total amount in statutory damages amounts to $60,000. This is Claimant's opening settlement demand.

COMPLYAUTO

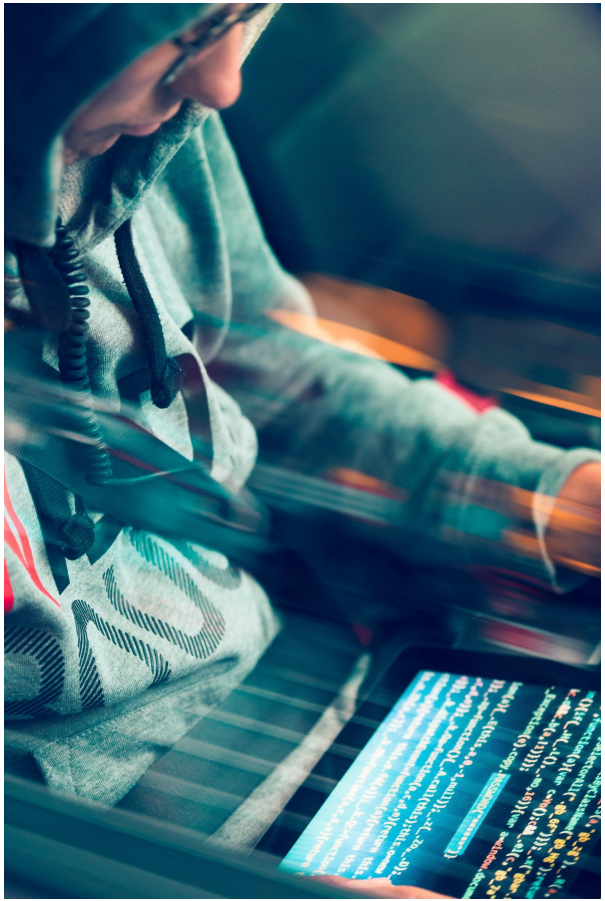
Isn't "Wiretapping" Just an Issue in California?

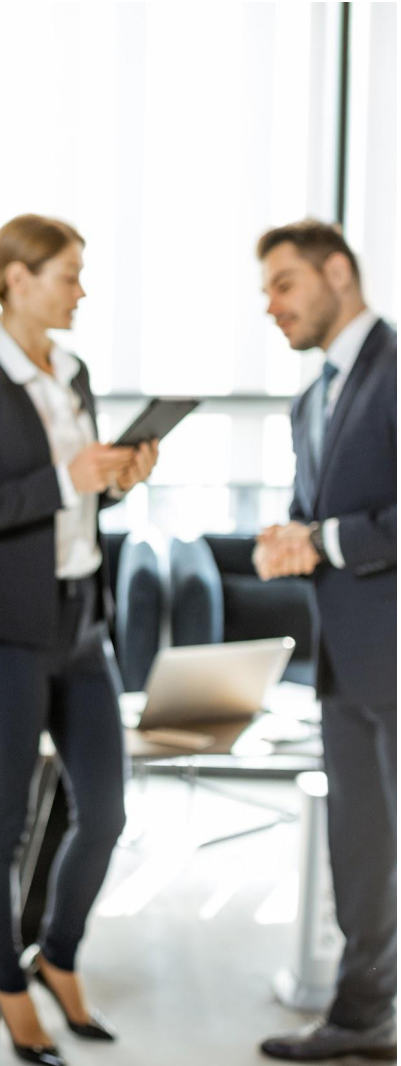
1. Majority of cases are from CA law firms, but many defendants are not from CA.
2. Many important open questions about: (a) Extraterritorial application of state statutes; (b) Personal jurisdiction based on generally available websites
3. But - until resolved, claims likely to continue to spread from state to state
4. "Highest" risk jurisdictions as of today? - CA, MA, PA, IL, FL
    a. Any other "dual consent state"?
    b. Geofencing those states is an option, but no guarantee of a safe harbor and doesn't protect from FTC action

Similar Allegations & Enforcement Actions

Other theories used in these types of lawsuits

1. **Federal Wiretapping -** Violation of federal wiretapping laws by using third-party cookies to track consumer activities and share information without consent.
2. **FTC Act Section 5 (UDAP) -** Violated UDAP by collecting & sharing sensitive information via tracking and advertising cookies/tech. without consumer consent.
3. **State Wiretapping & "Pen Register" Surveillance (hundreds of lawsuits filed recently)** Tracking cookies illegally track consumers online by tracking, collecting and sharing information without consent.
4. **Recording Communications without all parties' consent** Tracking cookies and chat modules are a general violation of privacy for states that require consent of all parties to record "communications."
5. **State Privacy Laws -** Violations of specific state privacy laws.





What Does the FTC Say?

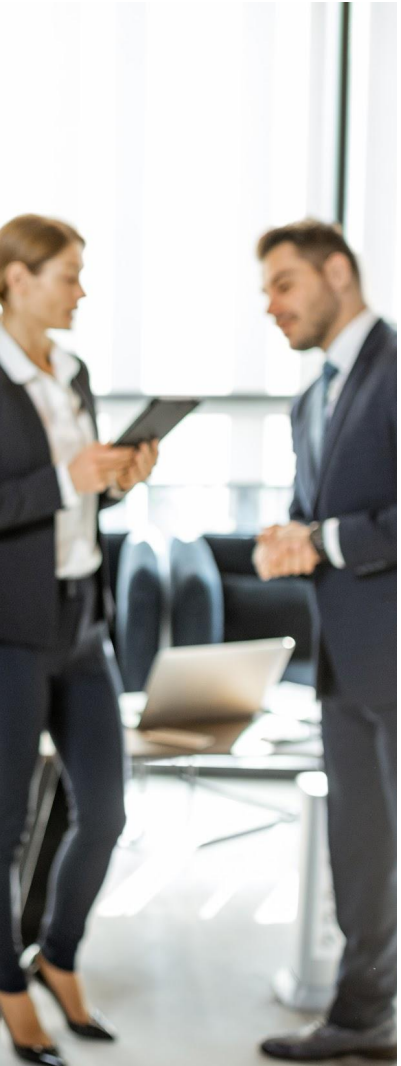
FTC Notice of Penalty Offenses to GLBA-Covered Entities (2023)

In the notices sent to the tax preparation companies, the FTC warned that the following practices may be deceptive or unfair under the FTC Act if companies fail to first obtain affirmative express consent from consumers:

- using information collected in a context where an individual reasonably expects that such information will remain confidential for purposes not explicitly requested by the individual;
- using such information to obtain a financial benefit that is separate from the benefit generated from providing the product or service requested by the individual; and
- using such information to advertise, sell, or promote products or services.

The Commission specifically warned the companies that it considers it an unfair or deceptive practice to use tracking technologies such as pixels, cookies, APIs, or SDKs to amass, analyze, infer, or transfer personal information in the ways outlined above without first obtaining consumers' express consent.

COMPLYAUTO



What Does the FTC Say? (cont.)

FTC Enforcement Actions Re 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.

ANPRM on "Commercial Surveillance" - "the business of collecting, analyzing, and profiting from information about people."

State Privacy Law Implications?

- State personal information laws define "sale" differently
  - Some require exchange of money.
  - Some (incl. OCPA) are broader and say any exchange for value is a "sale."

    If a dealer receives any benefit or advantage by sharing consumer data, even if no money changes hands, it will be considered a "sale" - requires opt out.
- OCPA prohibits Sale or "Targeted Advertising" without opt-out

Do Not Track (DNT) & Global Privacy Control (GPC)

- Mechanisms designed to give users control over their online privacy.

  DNT is older standard, GPC is newer.

- Oregon (and Colorado) (beginning July 2024) requires a business's website to honor GPC signals (also DNT in CA).
  - In CA GPC/DNT treated as option for consumers to express their opt-out preferences for the sale or sharing of their personal information.
  - OCPA requires to treat GPC as opt-out from targeted advertising and sale.
- For dealers that are not physically located in California or Colorado but engage with residents of these states, you will need to consider implementing mechanisms to honor these opt-out signals.

  Effectively requires blocking 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.

Summary

Online tech. will continue to present significant privacy litigation risks in 2024

- ➔ Plaintiffs' attorneys - wiretapping, pen register surveillance, general violation of privacy claims.
- ➔ FTC - UDAP for collecting/sharing personal information without consent via third-party tracking cookies.
- ➔ State AGs - 18+ state privacy laws regulating retargeted advertising and "sales" of information.
- ➔ Applies to third-party tracking cookies, chat modules, session replay tools, and geotargeting tools…(so far).

All dealers are potentially subject to liability

Residents from regulated states (e.g. California) are suing dealers in other states for violating their online privacy rights.

COMPLYAUTO

III. Strategies and Solutions to Avoid Becoming a Target

(Hint: Get Consent)

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.

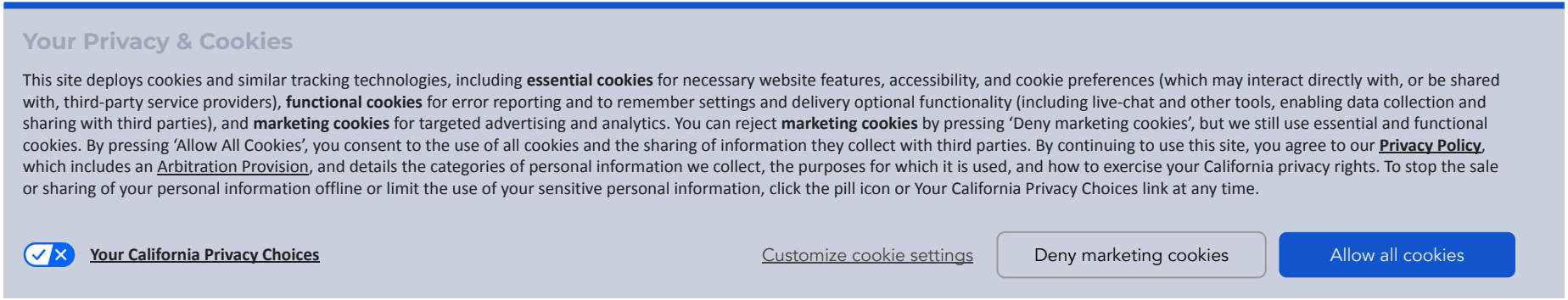
- **Policies** - Draft and update a valid and comprehensive Privacy Policy

- **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
  1. will collect the user data (collected via cookies etc.) solely to fulfill its obligations to the site;
  2. will not share or sell the data to other third parties, or:
  3. exploit the data for its own use, WITHOUT THE USER'S EXPRESS CONSENT

  - This means, chat modules, website providers, OEMs, website tools, schedulers, any third party.

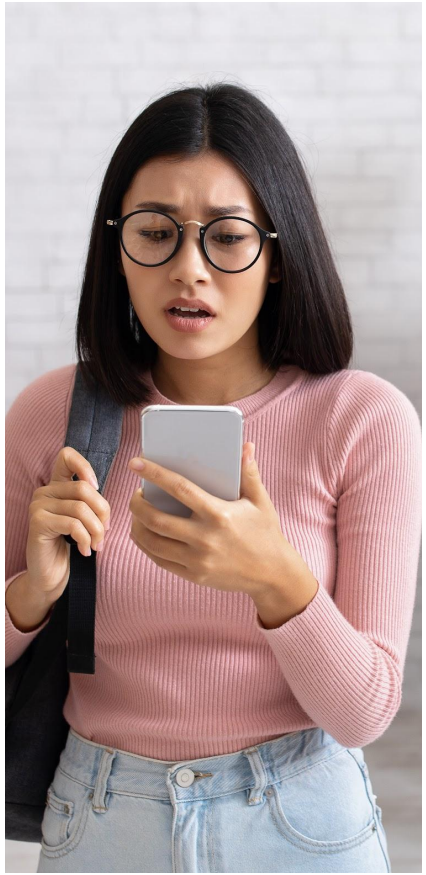
“Low Risk” (Recommended)



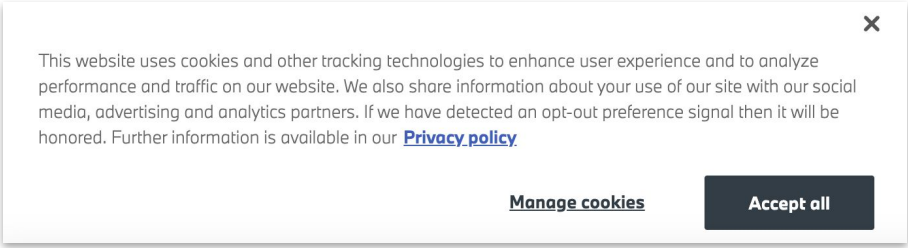
- Auto blocks all marketing cookies until user accepts banner.
- Provides notice of sharing with third parties.
- Has translation options upon deployment.
- User consents to hyperlinked Privacy Policy and receives notice of arbitration provision.
- Allows user ability to customize settings.

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”



Contract Issues

- Dealers should review their sites and have an understanding of the cookies that load, who is getting that information, and why
- They should tighten all contracts with all third party website tools or others that are placing cookies on their sites.
- This includes OEM agreements - but note that often that cannot be detected via the cookies alone
- Beware of reps and warranties in OEM, finance company, and/or advertising partner agreements stating that dealer has obtained consent from consumers for data collection and sharing with third parties.
  - Often paired with an indemnity in favor of the other party.
- Consider enabling Google restricted data processing to have Google act in the context of a "service provider" for state privacy laws. Similar mechanism exists for other providers.

COMPLYAUTO

IV. Practical Considerations: Potential Effects of Limiting Marketing Cookies

Questions?

Schedule a demo

We’re here to help! Questions?

brad.miller@complyauto.com

Schedule a demo

10,000+ active dealers across all 50 states

40+ state dealer association endorsements

NADA AFFINITY PROVIDER

COMPLYAUTO PRIVACY