May 6, 2026

Tracking Technologies & Chatbots:

Managing Evolving Regulatory and Litigation Risks

Privacy+ Security Forum

Speakers

Erin Doyle

Partner
Arnall Golden Gregory LLP

Shaudie Fassih

Director, Legal Counsel
The Coca-Cola Company

Kelley Chandler

Associate
Arnall Golden Gregory LLP

Legal Issues Lurking on Your Website

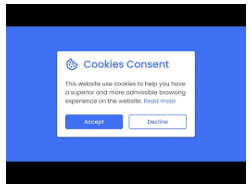
Privacy+ Security Forum

Your website is the **public face** of your company. It is where your customers and business partners can learn about you and your products and services. It is where your branding appears. It is also where **regulators** (and potential **litigants**) can see if you are compliant with privacy laws.

Here are some of the things they can see just by visiting your website:

Whether you use any cookies or tracking technologies...

Whether you have a cookie consent banner and how it works...



Whether you use AI or chatbots to interact with your users...

Whether you have compliant privacy notice(s)...

Whether you provide choices like the right to opt out of sale or sharing or targeted advertising...

Online Tracking Technologies

Examples of Online Tracking Technologies

- **Cookies** are small text files that are placed on a computer or device to remember information about the user's visit, such as login details, preferences, or analytics
  - First party vs. third party
  - Strictly necessary/essential, functional/preference, performance/analytics, marketing/advertising
- **Pixels/Web Beacons** are invisible images embedded on websites to track site visitor activity or other online behaviors like email opens or clicks (email tracking increasingly being treated like website-based tracking technologies)
- **Session Replay Tools** record a user's activities (e.g., mouse movements, clicks, typing) when using a webpage or app
- **Software Development Kits (SDKs)** can be embedded into apps and facilitate the exchange of data between those apps and third parties

Legal Risks of Using Tracking Technologies

Regulatory Risk:

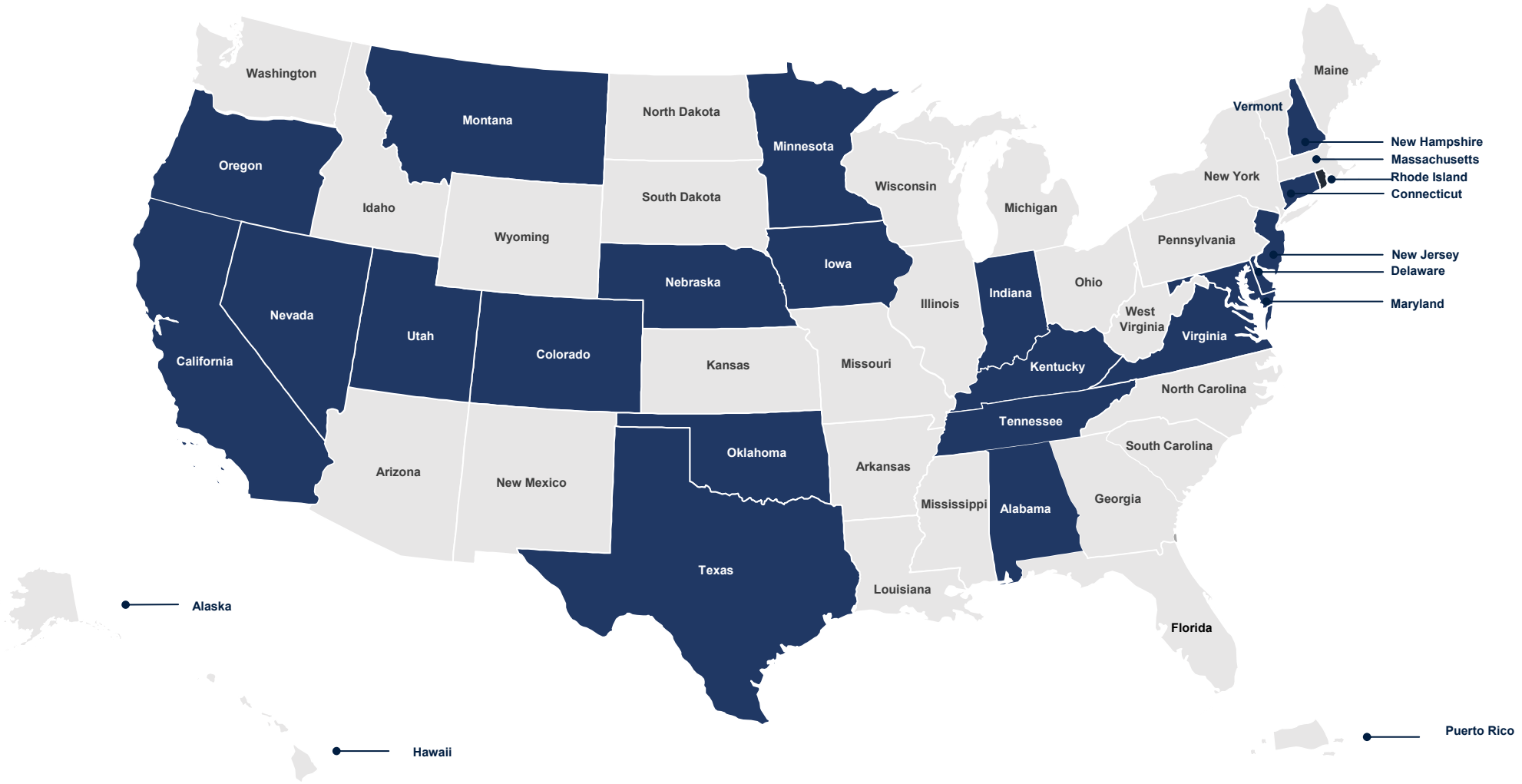
- Regulation of online tracking technologies has increased significantly in the US in recent years, including requirements to provide notice and choice to consumers allowing consumers to opt-out of the "sale" or "sharing" of their data via third party cookies or the use of their data for "targeted advertising"

Litigation Risk:

- Recent litigation under state and federal wiretapping statutes—most notably, the California Invasion of Privacy Act (CIPA)—alleging that the use of online tracking technologies is an illegal wiretap

State Comprehensive Consumer Privacy Laws Map

Privacy+ Security Forum



CCPA (& Other State Comprehensive Privacy Laws)

- **No privacy law in the US explicitly requires cookie consent or cookie banners.**

- The CCPA and the 21 other state comprehensive consumer privacy laws require that companies provide consumers the right to opt-out of the "sale" or "sharing" of their personal information for cross-context behavioral advertising and/or the use of their personal information for "targeted advertising." This is often achieved, at least in part, through an opt-out cookie banner or cookie preference center.

- Under the CCPA, other requirements also apply, including:
  - Displaying a "Do Not Sell or Share My Personal Information" link on the bottom of any webpage that collects personal information that links to a page that allows users to opt-out (even if they have previously accepted cookies)
  - The "Do Not Sell or Share My Personal Information" link can be called "Your Privacy Choices  "

- Note: Consumers will also need to be able to opt-out of offline sales or sharing, too, if you engage in such activities.

GPC Signal

- The **Global Privacy Control (GPC)** is an opt-out preference signal built into a browser-level setting or extension that sends a message to a website that the visitor does not wish to have their data sold or shared or used for targeted advertising
  - At least 12 states (either now or in the near future) require responding to these signals and treating them as an opt-out request
- **GPC Enforcement Sweep**
  - On September 9, 2025, the California Privacy Protection Agency (CPPA), along with the California, Connecticut, and Colorado Attorneys General launched a multi-state privacy enforcement sweep targeting businesses that do not detect and/or honor the GPC signal
  - The Connecticut AG's website includes helpful resources about the GPC signal
- **CA AB 566**
  - On October 8, 2025, California Gov. Gavin Newsom signed AB 566, requiring all web browsers to create an opt out preference signal within their browser
  - It takes effect January 1, 2027

Recent Regulatory Enforcement Example

- In February 2026, Disney settled with the California AG for $2.75 million resolving allegations that Disney failed to apply opt-out requests to its customers' entire accounts, including limiting opt-outs effectuated via the GPC signal to the specific device the consumer was using, even when the consumer was logged into their account.

CIPA

Background:

- Since late 2022, lawsuits and demands for arbitration or settlement under the California Invasion of Privacy Act ("CIPA"), and similar wiretapping laws in other states, have gained significant momentum.
- Statutory damages are available under CIPA of up to $5,000 per violation.
- Both state and federal courts in California have applied legal principles inconsistently, creating uncertainty and a patchwork of rulings.
- Targeting businesses of all sizes and industries (B2C and B2B)

Recent CIPA Developments:

- *Doe v. Eating Recovery Center LLC (N.D. Cal 2025)*—highlighted CIPA ambiguities and the need for legislative clarity
- SB 690—would narrow CIPA's scope with "commercial business purpose" carve out (stalled after passing one chamber)
- The Reform CIPA Coalition—launched in April 2026 to support legislative efforts to reform CIPA
- The Association of Corporate Counsel (ACC)—filed an amicus brief with the California Courts of Appeal

ECPA & VPPA

Background:

- At the federal level, the Electronic Communications Privacy Act ("ECPA") and Video Privacy Protection Act ("VPPA") are privacy laws that also appear in website-tracking and pixel litigation
- ECPA protects wire, oral, and electronic communications (greater of $100/day or $10,000 per violation); federal interception statute most analogous to CIPA
- VPPA is designed to protect privacy in video-viewing records and histories ($2,500 per violation)
- Both statutes have private rights of action
- **Common Theme:** Plaintiffs attempting to reframe website tracking into unlawful interception, monitoring, and disclosure

Recent Developments:

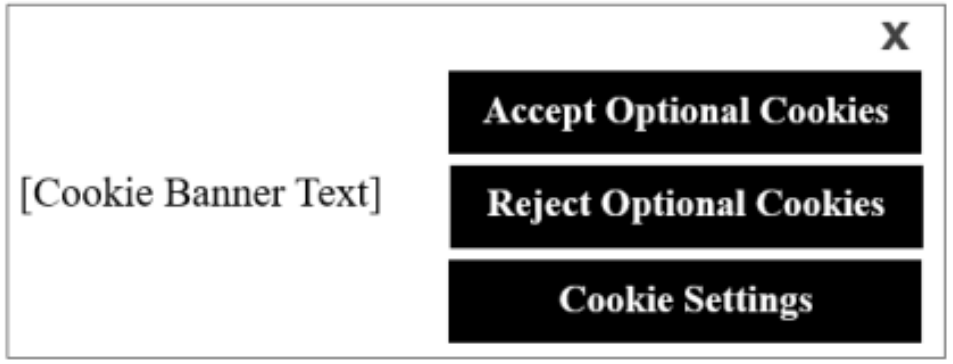
- ECPA claims have been increasingly present alongside CIPA claims
- A VPPA case has been granted certiorari by the U.S. Supreme Court

Cookie Banner Approaches

Common Approaches	Risk Level
Opt-in (Everywhere)	Low (Most Conservative)
Opt-in (California and EU only*)	Low-Moderate
Opt-Out (Everywhere)	Moderate
Notice Only	Moderate-High
No Banner	High

*Other jurisdictions are starting to require this approach such as Québec, Canada and Brazil

Cookie Banner Implementation & Presentation



Cookie Banner Content:

- Should mention whether **third party** tracking technologies are used
- Should explain what action constitutes consent ("By clicking Agree" or "By continuing to use this site", etc.)
- Should include link to Privacy Policy (and Cookie Policy, if separate)
- Ensure that content of cookie banner and Privacy Policy (and Cooke Policy, if separate) all align

Other Considerations:

- Symmetry of choice is increasingly expected by regulators
- No dark patterns
- Remember that liability lies with you, even when using a third party cookie governance tool

Chatbots and Chat Solutions

What are Chatbots & Chat Solutions

- **Types**
  - Rule-based chatbots (only provide certain answers based upon pre-defined rules or decision trees)
  - AI-powered chatbots (e.g., Siri or Alexa, customer service chatbots that use machine learning to answer questions)
  - Chatbot solutions can be implemented by third parties
- **Advantages:** Affordable, easily set up and usable, scalable, advanced integration capabilities
- **Business Uses:** 24/7 customer service, product or transaction support, product recommendations
- **Data Collection in Chatbots**
  - Chatbots can collect information about preferences and behaviors (and can often collect sensitive data if controls are not in place to prevent such data collection)

Legal Risks of Using Chatbots & Chat Solutions

Regulatory Risk:

- As chatbots proliferate, several bills to regulate their use have been introduced and many have been passed at the state level. These include requirements to disclose that a user is interacting with AI (if applicable), as well as enhanced requirements for companion chatbots, for example.

Litigation Risk:

- Recent litigation under state and federal wiretapping statutes—most notably, the California Invasion of Privacy Act (CIPA)—alleges that the use of third party-powered chat solutions is an illegal wiretap or eavesdrop ("extension" vs. "capability" test)

Chatbot Risks & Regulatory Considerations

- **Data Privacy**
  - Notice of collection by company (and third party if applicable)
  - Data minimization principles
  - Purpose limitation principles
  - Consent for collection of sensitive personal data
  - Opportunity to opt-out of engagement in automated decision making
- **Third Party Management**
  - Impose strict privacy and security controls on third party's access to and use of the chatbot prompts and inputs
  - Can be targeted in CIPA-type lawsuits (alleging that third parties are intercepting the inputs)
    - Trend toward including consent language near chatbot input button, which may include display of third party's Privacy Policy
- **Consumer Protection**
  - Statements are treated as representations of the company; UDAP risk
  - AI transparency laws may require disclosure of non-human nature of the chatbot
  - High-risk use cases trigger heightened requirements (e.g., using chatbots to make consequential decisions, chatbots interacting with children, etc.)

Vendor Risk Management

Vendor Risk Management Considerations

Privacy+ Security Forum

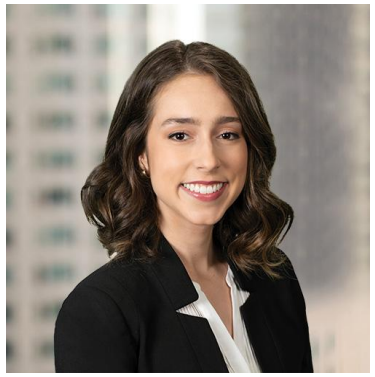
- **Understand the Vendor's Tool**
  Know what vendor tool does, what data it collects, and whether it shares data with any third parties.
- **Limit Data Collection and Use**
  Ensure collection of only the personal information the tool needs to function, and apply added safeguards where sensitive data may be involved.
- **Review User Experience**
  Make sure users receive clear notice, understand they may be interacting with a chatbot (where applicable), and are presented with the right privacy information.
- **Put Guardrails Around Use**
  Establish internal review before launch and before adding new features, integrations, or use cases.
- **Monitor the Vendor Over Time**
  Revisit the tool periodically to confirm it is operating as expected and remains aligned with your privacy, security, and consumer protection expectations.

Vendor Contractual Considerations

- **Use Restrictions**
  Limit vendor use of data to the services provided
- **Privacy and Security**
  Require reasonable safeguards and incident notice
- **Retention and Deletion**
  Address when data is deleted or returned
- **Subcontractors**
  Vendor remains responsible for downstream providers
- **Responsibility and Indemnification**
  Contract should address compliance requirements and remedies for failure
- **Linked Terms and Conditions**
  Confirm any online terms or policies incorporated by reference are clearly identified and reviewed by the appropriate legal team

Questions?

Questions & Contacts



Erin Doyle

Partner
Arnall Golden Gregory LLP

Kelley Chandler

Associate
Arnall Golden Gregory LLP

Shaudie Fassih

Director, Legal Counsel
The Coca-Cola Company