Staying Ahead of the Curve:

Best Practices for Online and AI-Based Advertising in a Changing Legal Landscape

Privacy + Security Fall Forum

Presented by:

Rachel Tarko Hudson
Partner
Sheppard Mullin

Brittany Walter
Associate
Sheppard Mullin

Leigh Freund
President & CEO
NAI

SheppardMullin

Background

Rachel Hudson

rhudson@sheppardmullin.com

415-774-2999

Rachel specializes in advising retail, fashion and beauty companies, food and beverage companies, and other consumer product companies and brands. Her clients also include software and technology providers and wholesale and material suppliers.

Rachel counsels her clients on all things privacy and advertising. She brings her deep subject matter and industry expertise and pragmatic approach to bear on projects ranging from review, clearance, and structuring advertising claims, programs, and campaigns to complying with the complex and ever-changing web of United States and international privacy laws. Drafting and negotiating commercial and IP agreements rounds out her practice.

Background

Brittany Walter

bwalter@sheppardmullin.com

858-876-3525

Brittany's practice focuses on technology transactions and counseling involving intellectual property, commercial and corporate transactions, advertising, and data privacy. Her experience spans multiple industries, including retail, sports, fintech, AI and other technology. She routinely advises clients on legal strategy for these transactions, as well as compliance strategies for advertising and data protection regulations. She has a special focus on disruptive technology, including artificial intelligence and blockchain-based products and services.

Background

Leigh Freund

As President & CEO of NAI, Leigh Freund leads the organization's growth and helps set the agenda and strategic priorities. Leigh joined NAI in 2015 after an eleven-year career at AOL Inc., where she served as vice president & chief counsel for global public policy.

Leigh brings more than a decade of substantive expertise in privacy, advertising, and public policy in the digital sector to her work at NAI. She has first-hand knowledge of the tremendous contributions third parties have made in the digital advertising space and she is a passionate believer in strong self-regulation.

During her time at AOL, Leigh led the company's public policy efforts and was a leading voice on global digital and technology policy. Prior to that role, Leigh headed up the AOL advertising legal team and worked with AOL's privacy team to promote and develop responsible use and collection of data, and ensure compliance with the industry's self-regulatory programs.

Before joining AOL in 2004, Leigh worked at K&L Gates and on Capitol Hill with Rep. Fred Upton from her home state of Michigan.

Leigh holds an undergraduate degree in political science from Kalamazoo College and a J.D. from Georgetown University. She is an active participant in several industry organizations devoted to compliance with key regulatory initiatives and principles, including the Interactive Advertising Bureau (IAB) and Digital Advertising Alliance (DAA).

Agenda

- Online Advertising Regulation
- Web Tracking Litigation
- Generative AI Overview and Potential Legal Issues
- FTC Guidance on AI
- Questions

Some ~~Gibberish~~ Terms

- First Party Cookie
- A cookie that you create and set on your site.

- Third Party Cookie
- A cookie that another company creates and sets on your site.

Some ~~Gibberish~~ Terms

- First Party Data

Data collected about your users on your site (by you or on your behalf).

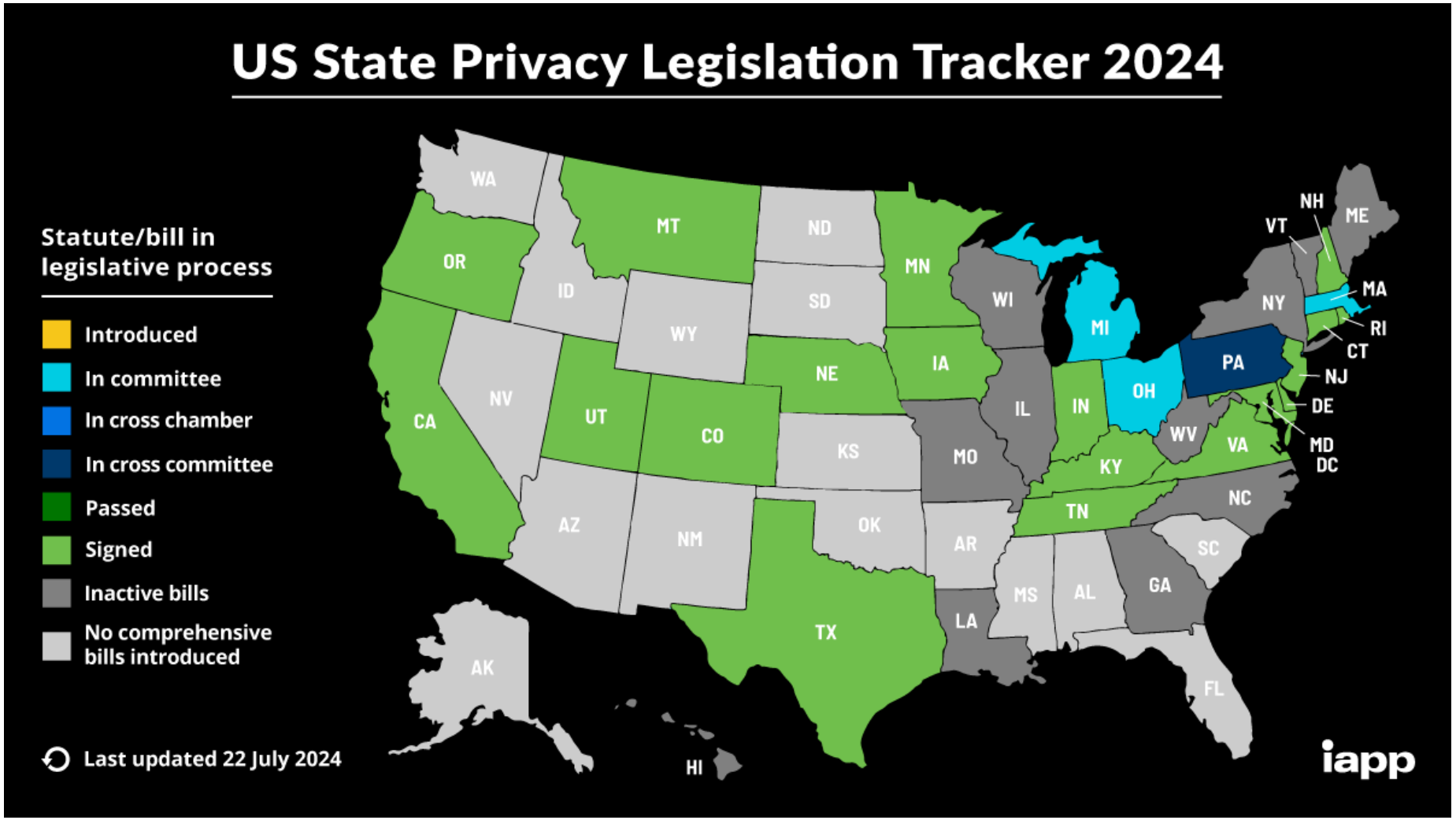
- Third Party Data

Data collected about users on other companies' sites by other companies.

CCPA and Other US Regulations

States	• California Consumer Privacy Act (CCPA) started the landslide • 19 states and counting • Do Not Track
Industry Self-Regulation	• IAB • NAI • DAA • Etc.
FTC Enforcement	• Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology (2009) • Cross-Device Tracking An FTC Staff Report • COPPA

State Privacy Law Deluge



State Do Not Sell/Share and OBA

- Do Not Share for Targeted Advertising
- Targeted/behavioral advertising is expressly included

Right to Opt Out

- Why does this matter?
  - How do you opt a cookie/pixel/browser out from a sale/sharing?
  - AG's Do Not Sell Complaint Tool
- AdChoices and NAI tracking opt out cookies
- IAB Privacy String
- Cookie consent managers
  - But not necessarily the European model
  - OneTrust, Intraedge (Truyo), etc.
  - In house developed

What About Minors?

Consent

CCPA requires opt in consent for sale (not opt out)

- 13-16 years old: from the minor
- Under 13 years old: from a parent/guardian

Knowledge that the consumer is a minor

- But be reasonable

Don't forget about COPPA!

- Notice and verifiable consent are required
- Broad definition of personal information
- Under 13 years old: from a parent/guardian

Industry Self Regulation

- DAA
  - Aggressive enforcement
  - OBA policy disclosure
    - Our Ads
- IAB CCPA Compliance Framework
- Tracking opt out
  - Not all ad networks are members
  - AdChoices
  - NAI

Other Regulatory

- FTC Activity → Notice and choice
  - COPPA and children
  - Online tracking without notice
  - Cross-device tracking without notice
  - Unexpected tracking (smart devices like TVs)
  - GPS data

What Is Web Tracking?

Website tracking (or web tracking) is a method of collecting, storing, and analyzing user activity across one or several web pages

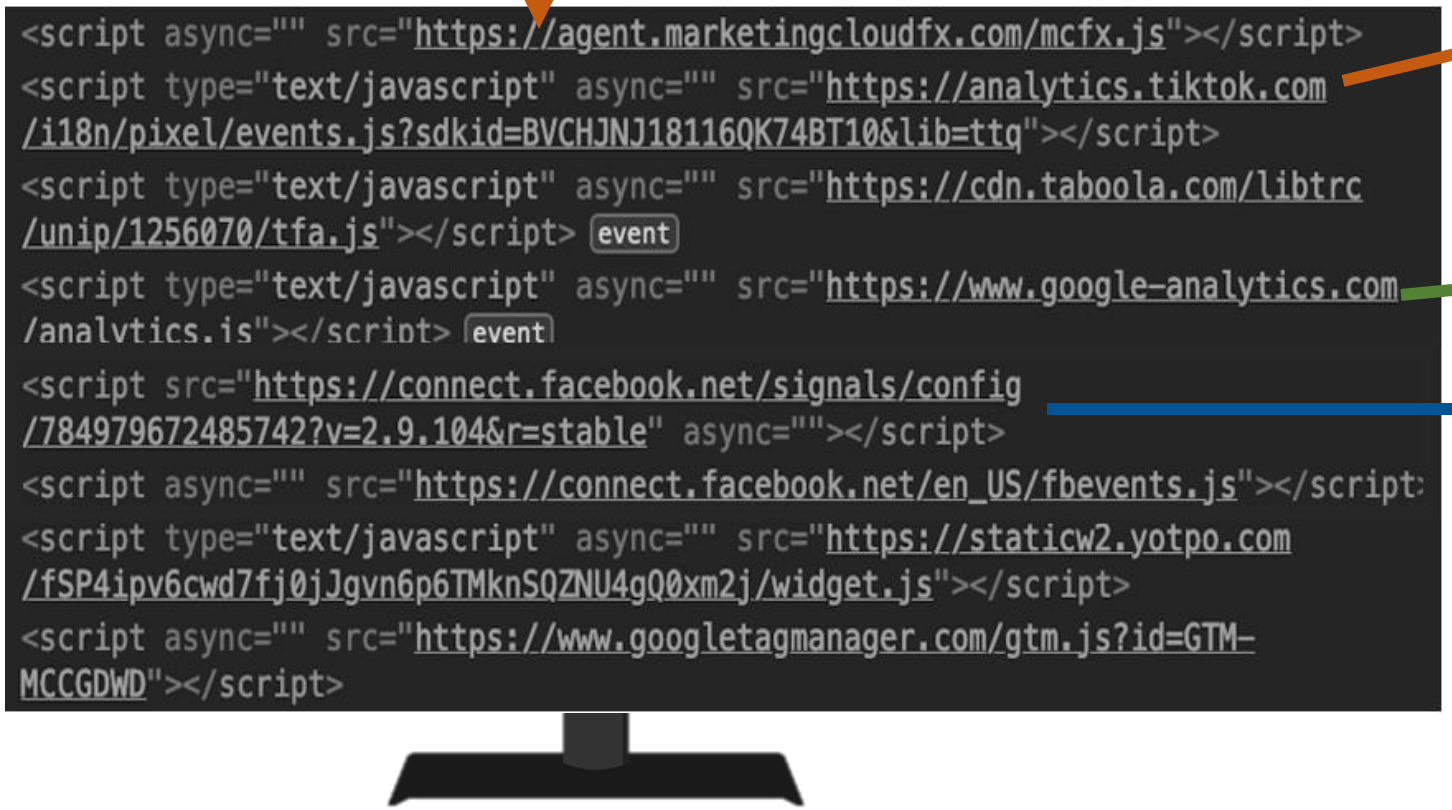
When you visit a website or app, data is collected from your device and web browser

Different kinds of technology is used to collect different types of data

Two kinds of tracking: First-party tracking is data collected directly by the domain you're visiting, while third-party tracking is when data is collected by a different party.

Data Transmission To Third Parties

Your website code



Visitor's Browser

Sends information to TikTok

Sends information to Google

Sends information to Meta/Facebook

Marketing/Advertising Uses

Behavioral Targeting and Ad Personalization: displaying personalized ads to users based on visited websites, search queries and other online habits tracked

Re-Targeting: targeting ads to users who already visited given site and match certain criteria such as position in sales funnel

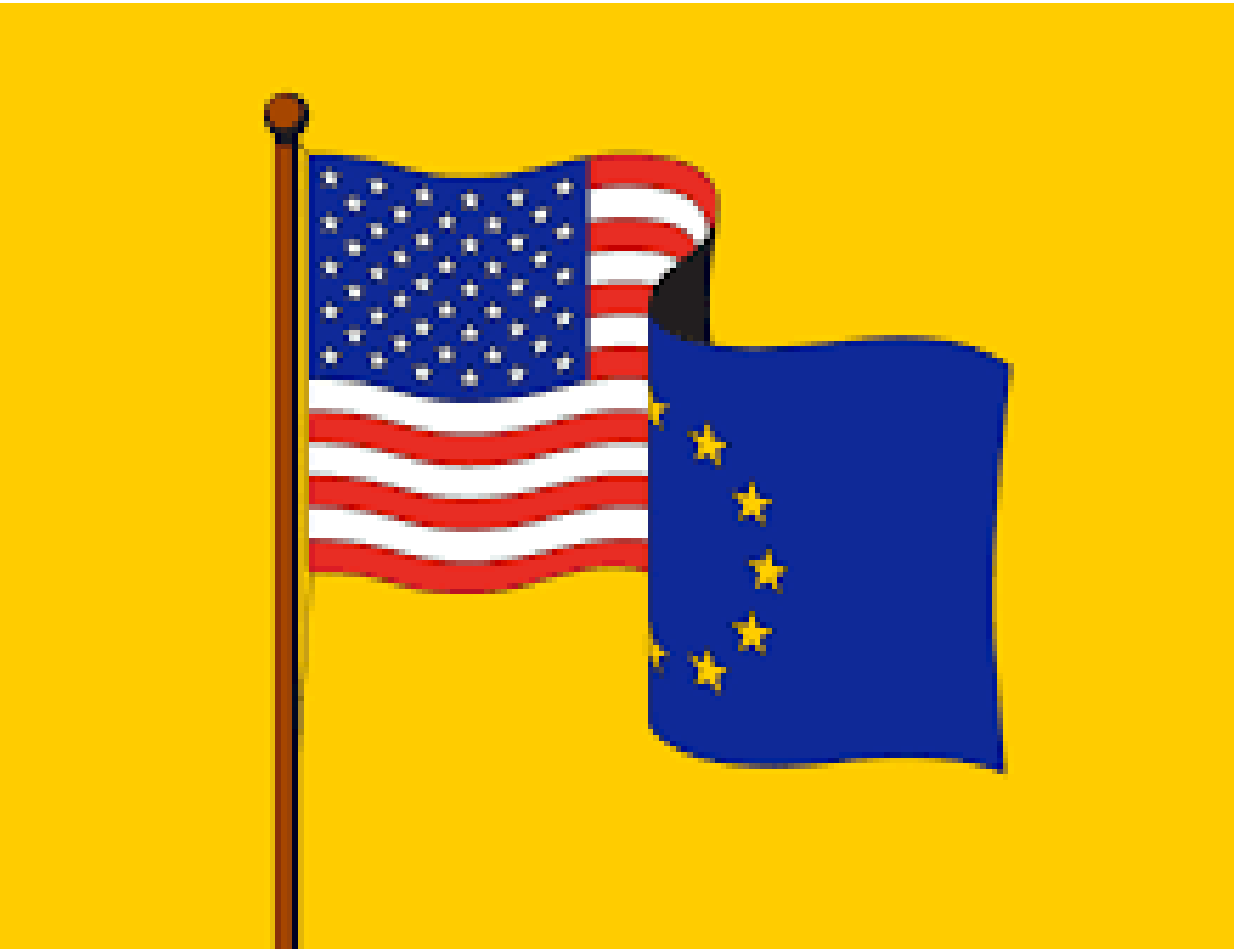
Frequency Capping: limiting number of times showing the same ad to a user through given time, e.g. no more than 3 times per 24 hours

Visitor Profile Building: gathering more information about a user, e.g. by connecting behavioral data with demographics information filled in by user during registration on the website

Matching Visitor Profiles: gathering and combining visitor profiles from different publishers/data sources – it's usually done by DMPs – *Data Management Platforms*

Audience Data Trading: trading visitor profile information, DMPs sell data directly or through ad exchanges to advertisers, so that they can better target their ads

Web Analytics: learning more about users visiting given website



Plaintiffs' Bar Attempting to Do What Governments Could Not – Apply GDPR and Cookie Directives in the U.S.

California Invasion of Privacy Act (CIPA)

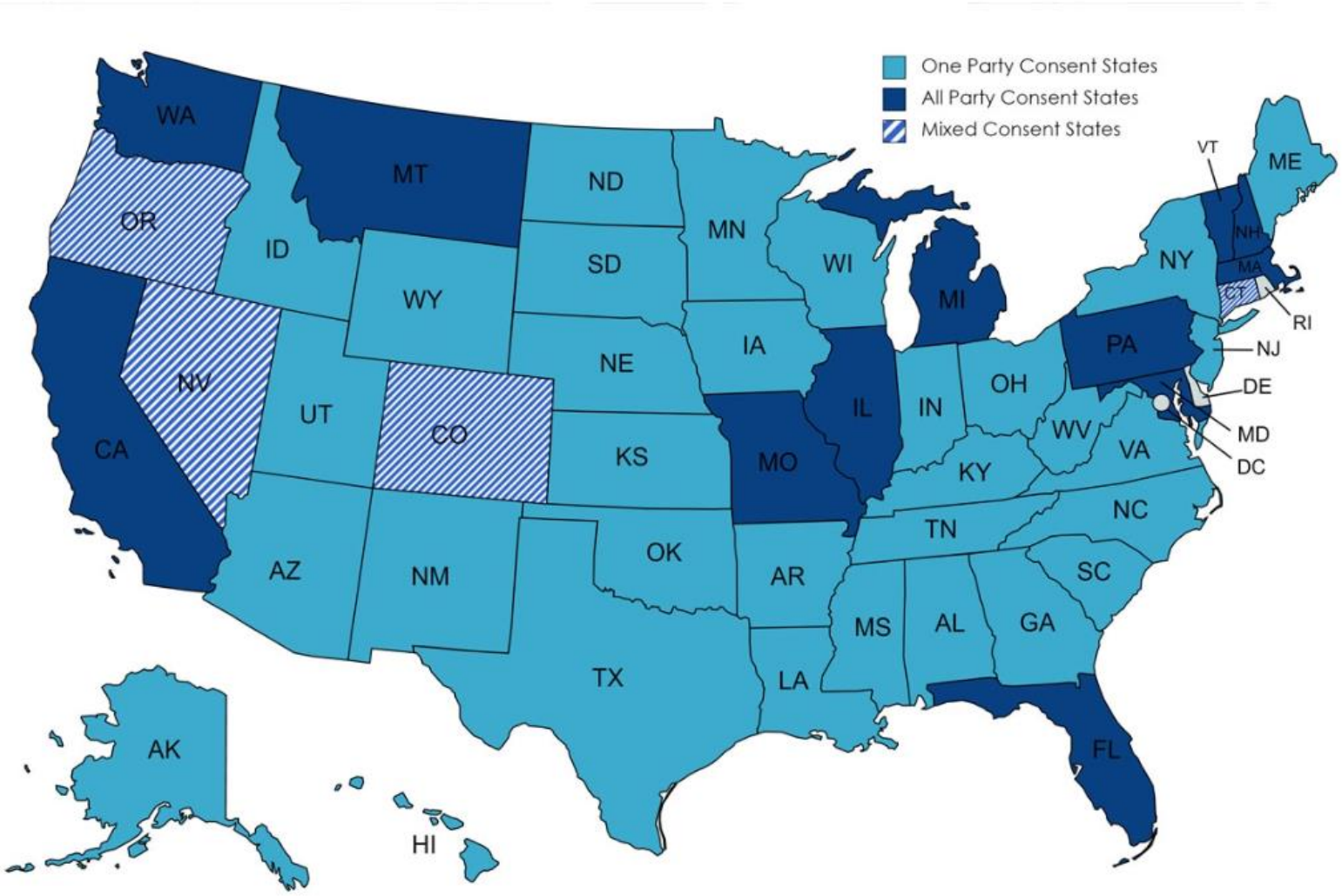
Wiretapping

In a nutshell: 1967 law that prohibits reading, attempting to read, or learning the contents of a communication without the consent of all parties to the communication

Violations: $5,000 or 3x actual damages

Class Action Dream: CIPA allows for a private right of action with statutory damages

California Is Not Alone



Chatbots: What Could go Wrong?

1

False Info - Air Canada AI chatbot created non-existent refund policy; British Columbia Civil Resolution Tribunal found Air Canada liable for misinformation given to a consumer by an AI chatbot

2

BIPA – Use of voiceprints without prior express consent

3

Biased/discriminatory info - Microsoft Tay spewed hate speech; promptly shut down

4

Advice vs. information - DoNotPay legal chatbot to give real-time advice in courtroom to pro se defendants; chatbots that give regulated advice (medical, legal, etc.) vs. information may be illegal

5

Damaging Advice – Tessa (by the National Eating Disorders Association) provided advice about calorie cutting and weight loss deemed to exacerbate eating disorders

6

Wiretapping and Other Privacy Complaints – over 400 lawsuits filed since 2022 regarding web tracking and chatbot usage

Proactive Steps

- Educate your teams
  - Get teams on board with thinking about privacy issues and looping you in early and often
- Know your website and apps
  - Review your deployments of all third-party integrations / trackers / SDKs etc.
  - What are you sharing? With Whom?
- Update Privacy Policies and Terms
  - Mass arbitration terms
  - New JAMS mass arbitration procedures
- Limit data to what you actually need
- Get consents where you can
- Have a contract that spells out what vendors can/will do and what they will not do

Overview of AI

Artificial Intelligence (AI)

Machines with human-inspired capabilities including:

Communication

Perception

Planning

reasoning

knowledge representation

move and manipulate objects

learning

Machine Learning (ML)

Machines use data to generate output that is:

Descriptive – explain what happened

Predictive – predict what will happen

Prescriptive – make suggestions about what action to take

Generative AI (GAI)

AI used to generate new:

Text

Images

Code

Video

Audio

Other content

Robotics

Can automate repetitive tasks

Can do certain tasks more cost effectively

Can do jobs humans cannot – dangerous environments

Overview of Potential Legal Issues

Training data – need rights to *access* and *use data*

Training AI Models – Just Because It's Your Data Doesn't Mean You Can Use It

Input – Copyright, PI, PHI (HIPAA), Biometric Info (BIPA), confidentiality, disclose and get license if using for any other purpose

Output – accuracy, no medical advice, disclose and get license if using for any other purpose

Advertising – don't overstate AI capabilities; need to be able to substantiate claims

You Don't Need a Machine to Predict What the FTC Might Do About Unsupported AI Claims

Disclosure requirements – CA, UT laws

Colorado – AI consumer protection law

Colorado Introduces an AI Consumer Protection Bill

Training AI Models

You need the right to use the data on which you are training and for that purpose!

- Copyright issues
- License concerns (open source, attribution)
- Illicitly collected data – verify the source
- Responsible use: Biased data, incorrect data
- Ability to comply with state privacy laws (Right to access, deletion, correction, opt outs from sale, targeted advertising, and automated decision-making, and opt in to use of sensitive personal information)

Sample Lawsuits

- **Copyright Lawsuits:**
  - **Getty Images**
  - **Book Publishers**
  - **Code Generators**
- **Privacy Issues**
- **Biometric Information**
- **Defamation**

Why Does This Matter?

Liability Issues – Output of GenAI Tools

- Liability may arise if the output:
  - Breaches the license
  - Infringes IP
  - Contains PII, NIL
  - Is defamatory
  - Is false or inaccurate
  - Others?
- Different tools provide different legal protections (or lack thereof)

Ownership / Protection of GenAI Output

- Terms of Use for different tools treat ownership differently
  - Some grant ownership, some don't
  - Some recognize another user's prompt may generate the same output and they own it too
  - Some require that **you grant a license** to the tool provider
  - Some require you to indemnify the tool provider
- Copyright protection for the output of GenAI is limited – not human authorship
  - Consider prohibiting the use of GenAI to create works for which the company typically needs copyright protection

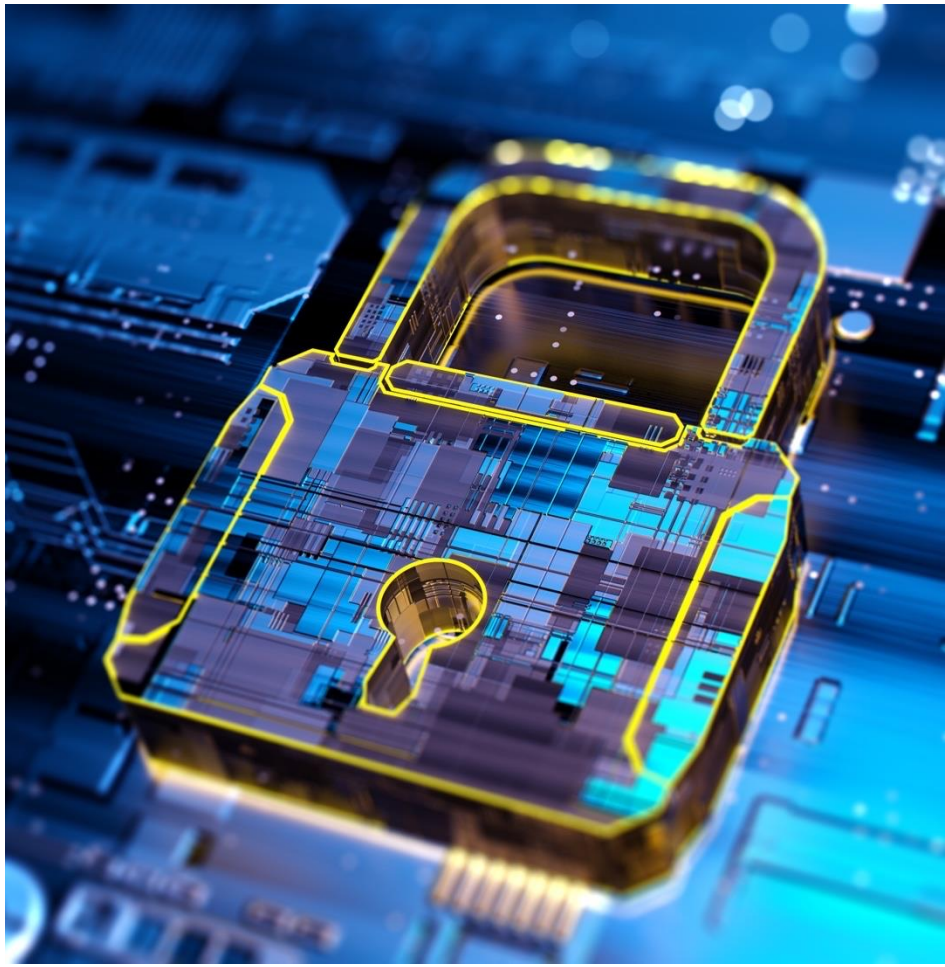
Third Party Contractors' Use of GenAI

- Third parties – prohibit the use of GenAI to generate content without prior written approval
- Require disclosure if they have used GenAI in the past for deliverables (copyright protection issues)
- Data Protection Agreement – ensure that it addresses the limitations of what the vendor can do with personal information and complies with the various applicable privacy laws (i.e., CCPA, GDPR, etc.)
- Carefully review AI vendor contracts

FTC and AI

The FTC has been actively involved in regulating AI and its applications

- Key Topics
  - Privacy, geolocation and biometric data privacy and security
  - Accuracy
  - Fairness and non-discrimination
  - Transparency and explainability
  - Safety and reliability
  - Advertising
- Enforcement Actions – Algorithmic Disgorgement



Keeping your AI Claims in Check

The FTC Division of Advertising Practices updated guidance on the use of AI to caution on:

- **False or Exaggerated Claims**: Advertisers must substantiate claims about the efficacy of AI products. Exaggerating capabilities or making claims beyond the current scope of AI technology can be deceptive.
- **Comparative Claims and Proof**: Assertions that AI products outperform non-AI alternatives require adequate evidence. Unsupported claims should be avoided, especially if they contribute to price inflation or influence labor decisions.
- **Understanding Risks**: Companies must comprehend the foreseeable risks associated with AI products before bringing them to market. Blaming third-party developers or citing AI as a "black box" excuse is not acceptable.
- **Verification of AI Usage**: Merely labeling a product as AI-powered without substantiation is insufficient. The FTC can investigate claims and analyze underlying technology to ensure compliance.
- **The Importance of Truthful Claims**: Regardless of its capabilities, AI merits truthful and transparent advertising. Unsupported claims may lead to FTC enforcement actions.

Operation AI Comply

- FTC's recent enforcement sweep targets multiple companies that the FTC believes have "relied on artificial intelligence as a way to supercharge deceptive or unfair conduct that harms consumers."
  - DoNotPay
  - Ascend Ecomm
  - Ecommerce Empire Builders
  - Rytr
  - FBA Machine

FTC Guidance:

Engineering Consumer Trust

- Increased use of generative AI tools to influence beliefs, emotions, and behavior.
- Chatbots are being deployed for various purposes, including providing information, advice, support, and companionship, often designed to persuade with confident, even fictional, answers.
- Trust in AI output is influenced by "automation bias" and anthropomorphism, where people may trust machines that appear neutral or use personal pronouns and emojis.
- Commercial actors exploit the unearned trust in generative AI tools for various purposes, including financial gain.
- FTC concerns focus on the potential deceptive or unfair steering of individuals into harmful decisions in areas such as finances, health, education, housing, and employment.
- Manipulative design elements in generative AI, such as those found in ads customized to individuals or groups, raise FTC scrutiny.
- Clear labeling of ads within generative AI output is essential to avoid deception or unfairness.

SheppardMullin

AI Companies: Uphold Your Privacy and Confidentiality Commitments

- **Legal Enforcement and FTC Actions:**
  - Violations of privacy commitments in advertising practices can lead to legal liability under FTC regulations.
    - Amazon settles with FTC for $25M
  - Algorithmic Disgorgement: FTC mandated deletion of products developed with unlawfully obtained data, particularly in the context of advertising and consumer targeting.
    - Penalty for improperly using data to build algorithmic systems– destruction of ill-gotten data and the models/algorithms derived from it
    - *Everalbum*
- **Transparency and Consent in Advertising:**
  - The FTC actively pursues actions against companies that omit material facts affecting consumer decisions, particularly regarding data usage for advertising purposes.

FTC Investigation of OpenAI

Determining whether OpenAI "engaged in unfair or deceptive privacy or data security practices or engaged in unfair or deceptive practices relating to risks of harm to consumers"

- FTC is investigating OpenAI over possible consumer harm through its data collection and the publication of false information.
- FTC sent a 20-page letter that requests documents related to developing and training its large language models, and data security issues.
- FTC wants detailed information on how OpenAI vets information used in training its AI models and how it allegedly prevents false claims from being shown to ChatGPT users. It also wants to learn more about how APIs connect to its systems and how data is protected when accessed by third parties.

FTC Investigation of OpenAI

Examples of Types of Information Being Sought by FTC About AI Products:

How Marketed	Process to Correct “Hallucinations”
How You Ensure Ads/Reps are clear	Process for Retraining/Refining Models
Research Tests re: accuracy of Products	Process of Reinforcement Learning Through Human Feedback
How You Use Info Retained or Collected	Policies and Procedures to Assess Risk
Data Used to Train and How Collected	Policies to Protect PII
How you Review Data Used to Train	Policies to Delete PII if Requested
How do you manage bias	Policies re: Accuracy of Statements About Individuals

Questions?