Title Staying Ahead of the Curve:

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

ACC Association of Corporate Counsel SAN DIEGO

SheppardMullin

Our Panelists

Wynter Deagle
Partner
858-720-8947
Wdeagle@sheppardmullin.com

Gazal Pour-Moezzi
Partner
714-424-8219
Gpour-moezzi@sheppardmullin.com

Brittany Walter
Associate
858-876-3525
Bwalter@sheppardmullin.com

Agenda

1. Mitigating Privacy Risks from Using Web Tracking for Marketing and Advertising

2. Protection of IP

3. AI-Generated Content

PRIVACY

What Is Web Tracking?

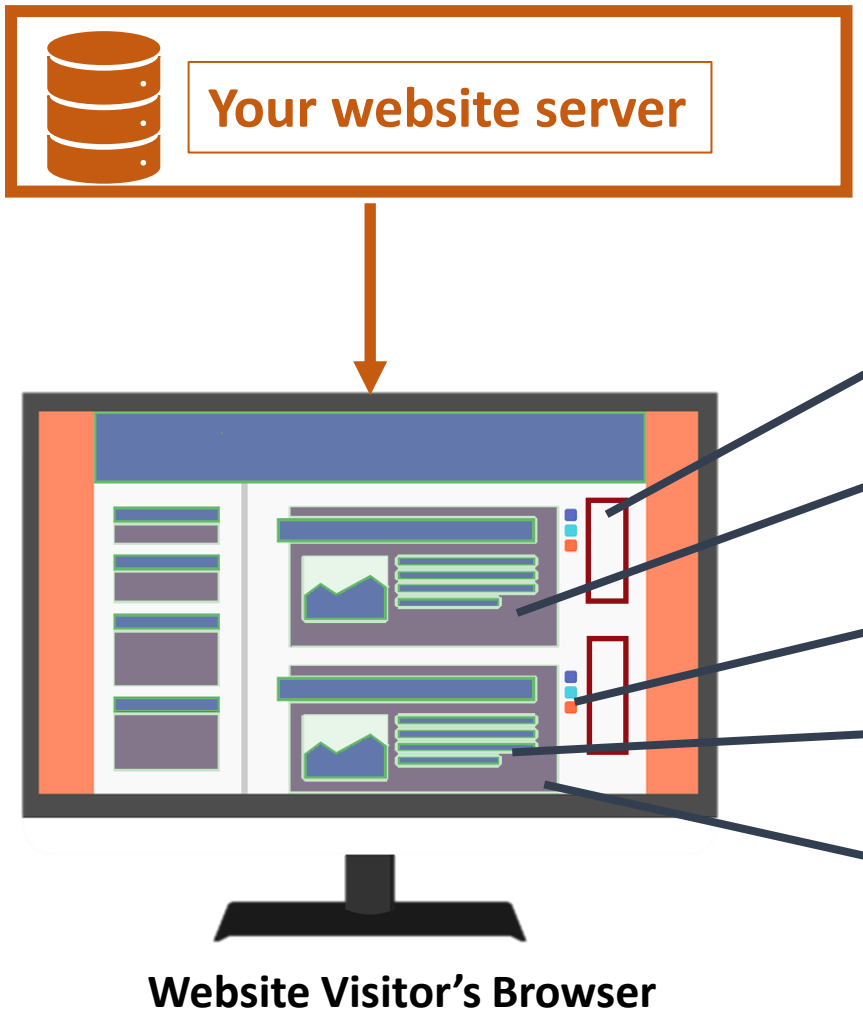
Website tracking (or web tracking) is a method of collecting, storing, and analyzing user activity across one or several web pages

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.

Types of Web Tech



Advertising / Tracking Pixels & JavaScript
(Facebook, Google, TikTok, etc.)

Media Players
(YouTube, Vimeo, Twitter, etc.)

Ad Servers

Session Replay &
Other Analytics

Customer Chat Window
(chatbot)

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

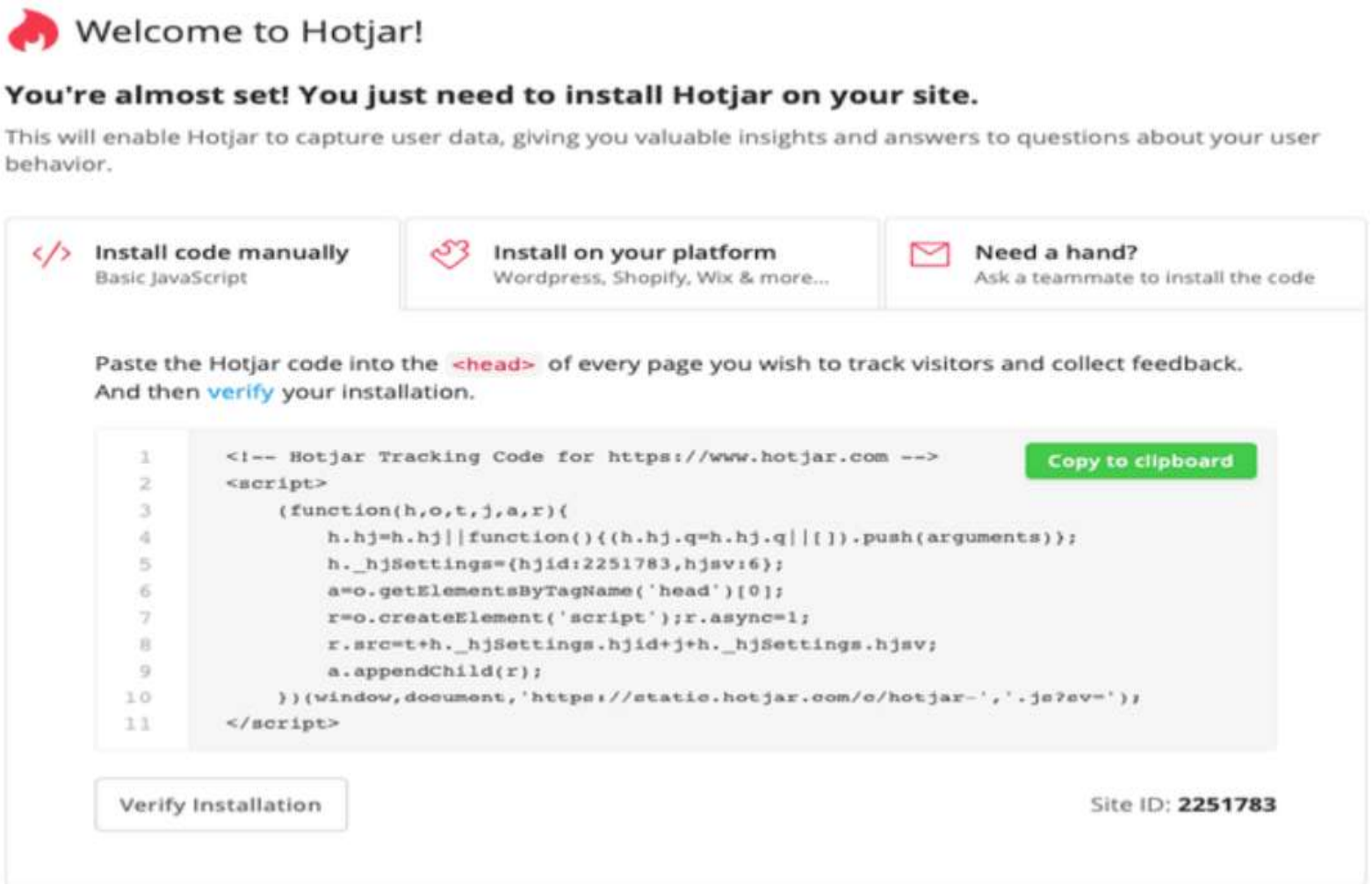
Visitor Profile Building: gathering more information about a user, e.g. by connecting behavioral data with demographics information filled in by user during registration on the website

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

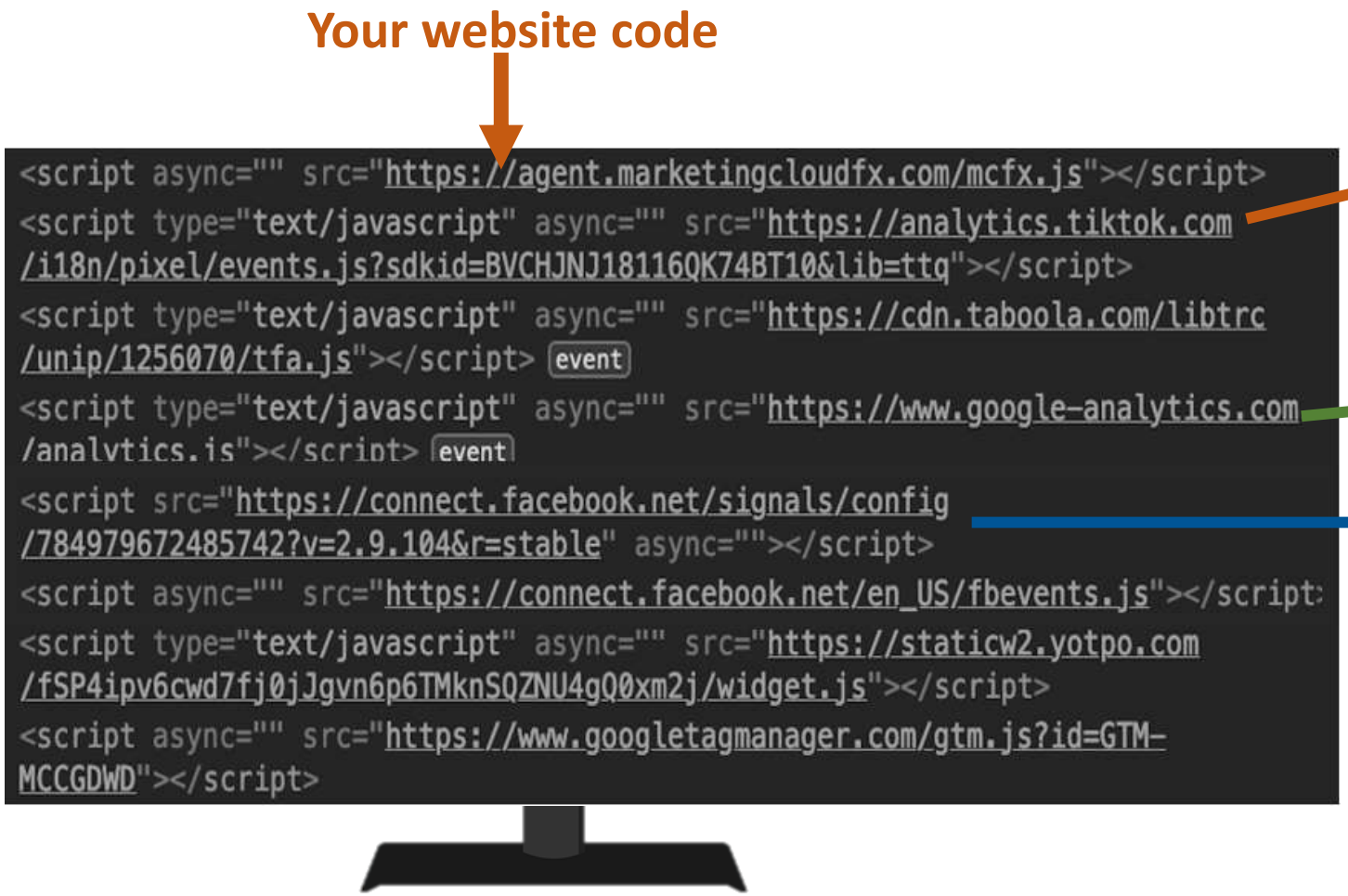
Audience Data Trading: trading visitor profile information, DMPs sell data directly or through ad exchanges to advertisers, so that they can better target their ads

Web Analytics: learning more about users visiting given website

How Web Tracking Technology Works



Data Transmission To Third Parties



Sends information to TikTok

Sends information to Google

Sends information to Meta/Facebook

What Data Is Transmitted?

What Third-Party Vendors May Receive:

Header Information

- Webpage URL (sometimes detailed*)
- IP Address

"Events" data*

- Video views and/or URL of video content
- Items placed in shopping cart
- Items purchased
- Information entered on forms
- Searches performed
- Data/information retrieved

Additional Data*

- Name, Email or "hashed" email
- Account or customer ID
- Cookie Identifiers (and can set cookies)

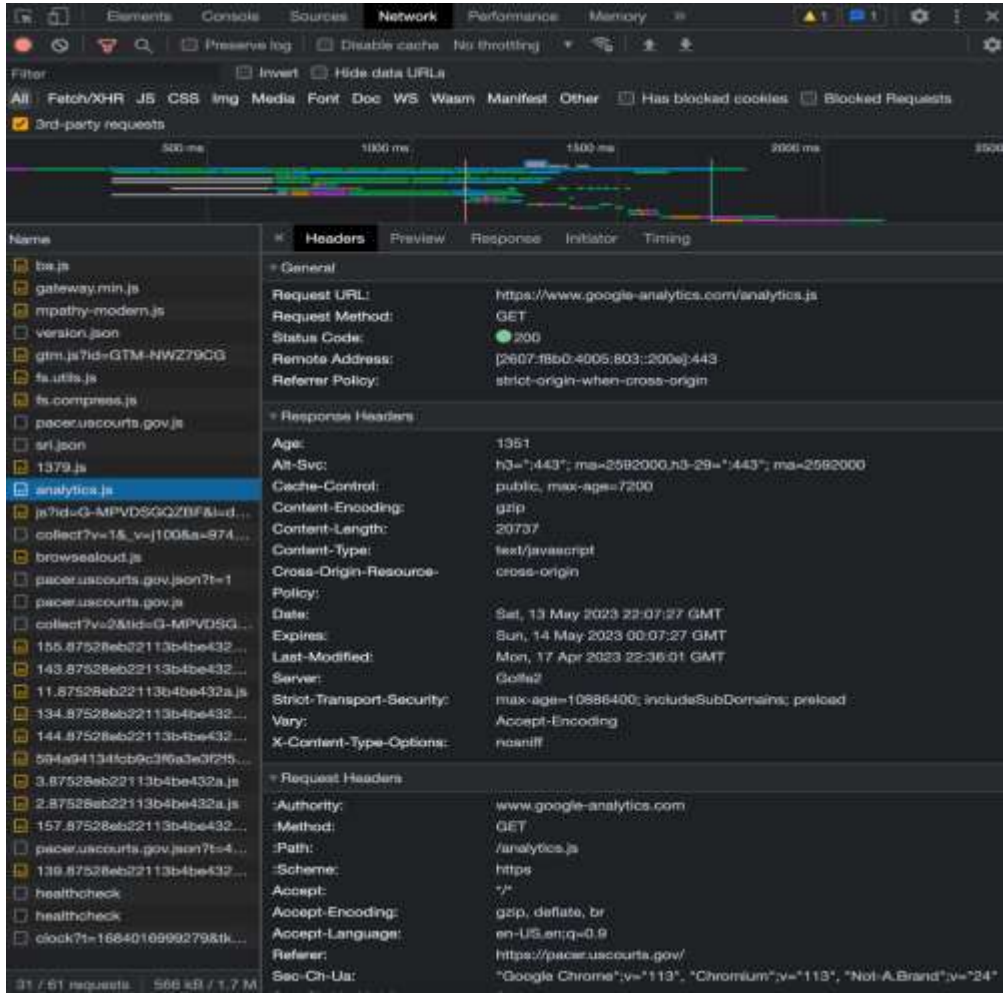
Bob's Fish Shop

- GET https://www.facebook.com/tr/?id=1236227986843860&ev=PageView&dl=https%3A%2F%2Fbobsfishshop-ca.org%shop%2Fsearch2Ffishing tools%rods%&rl=&if=false&ts=1688407008517&sw=1440&sh=900&v=2.9.110&r=stable&ec=0&o=30&fbp=fb.1.1688407008516.821700889&cs_est=true&it=1688407008460&coo=false&rqm=GET HTTP/1.1
- Host: www.facebook.com
- Connection: keep-alive
- sec-ch-ua: "Not.A/Brand";v="8", "Chromium";v="114", "Google Chrome";v="114"
- sec-ch-ua-mobile: ?0
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
- sec-ch-ua-platform: "Windows"
- Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
- Sec-Fetch-Site: cross-site
- Sec-Fetch-Mode: no-cors
- Sec-Fetch-Dest: image
- Referer: www.bobsfishship-ca.com
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.9
- Cookie: sb=nQujZGPtCbYMD_4yWAMq-cfg; datr=nQujZLm0gj4YIbPYME0TDUJo; locale=en_US; c_user=1000895621911297; xs=18%3Ag8wXJiG5BuhNnA%3A2%3A1688406974%3A-1%3A11520; fr=06eyUSCbpHxBjqKRF.AWWzZ4LPMjVlHHWrUyiiIQ-VLRo.Bkowud.Un.AAA.0.0.Bkowu_.AWXlBaAuA3k

Stalking Pixels

Anyone Can See It: Tools to view website transmissions are widely available

The Result: Plaintiffs' counsel have transformed into web technology detectives



Class Action Deluge Begins

California Invasion of Privacy Act (CIPA)

- **In a nutshell:** 1967 law that prohibits (1) reading, attempting to read, or learning the contents of a communication without the consent of all parties to the communication and (2) installing a pen register or trap and trace device without a court order subject to certain exceptions
- **Violations**: $5,000 or 3x actual damages
- **No Need to Prove Harm:** CIPA allows for a private right of action with statutory damages.

CIPA Dials Up Trouble For Businesses

- Javier v. Assurance IQ, LLC – CIPA "applies to Internet communications."
- Initially focused on wiretapping/eavesdropping – Sections 631 and 632
- Theories:
  - (1) chatbots managed by third-party vendors illegally intercepted and recorded the contents of communications
  - (2) web technology was an illicit and unannounced eavesdropper
  - (3) web technology constituted "doxing" because it revealed the identity of anonymous consumers.
- Healthcare industry claims bolstered by HHS guidance concerning use of web tracking technology
- Over 400 suits filed

The Pen Is Mightier Than The Sword

- Section 638.51 added in 2015
- Allow law enforcement to obtain a court order for trap and trace or pen register
- November 2023 - *Greenley v. Kochava* pits CIPA section 638.51 against web technologies.
- *Greeley* did not address whether a business that operates a website, as opposed to third-party technology providers, could be liable under for violations of CIPA's pen register and trap and trace device provisions for implementing website technology such as pixels on their own website.
- Another surge of demand letters and lawsuits

Strategies For Risk Mitigation

Inventory and Classify Technology

Risk v. Reward Analysis

Robust Disclosures

Express Consent

Indemnification and Limitation of Liability

IP PROTECTION

Use of Trademarks as Search Engine Keywords

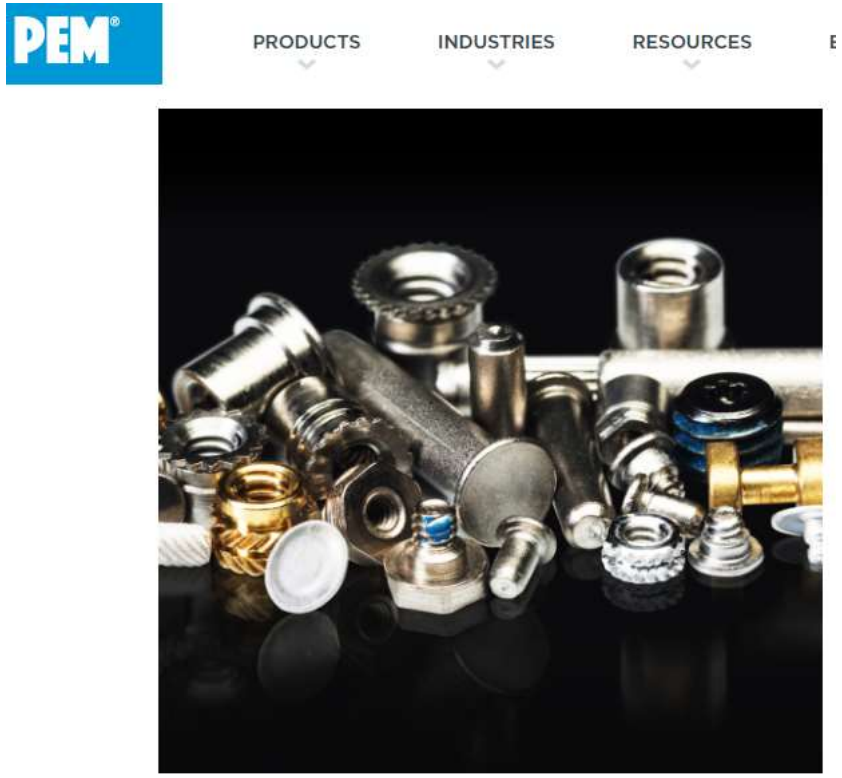
- Sponsored Links
  - Search engines generate income by selling advertising space on the search results page – "sponsored links" that are placed above/alongside organic search results
  - Search engines sell "keywords" to advertisers that trigger sponsored links when consumers search for identical/related search terms

- Keywords
  - Not necessarily trademarks
  - Keywords can also be generic terms
    - Ex: Ford, Toyota, KIA purchase keywords such as "cars" "autos" "sedans" through Google so that their sponsored links appear when consumers search for those words
  - What happens when a company buys/bids on a third party's trademark?

Use of Trademarks as Search Engine Keywords

Penn Eng'g & Mfg. Corp. v. Peninsula Components, Inc. (E.D. Penn.)

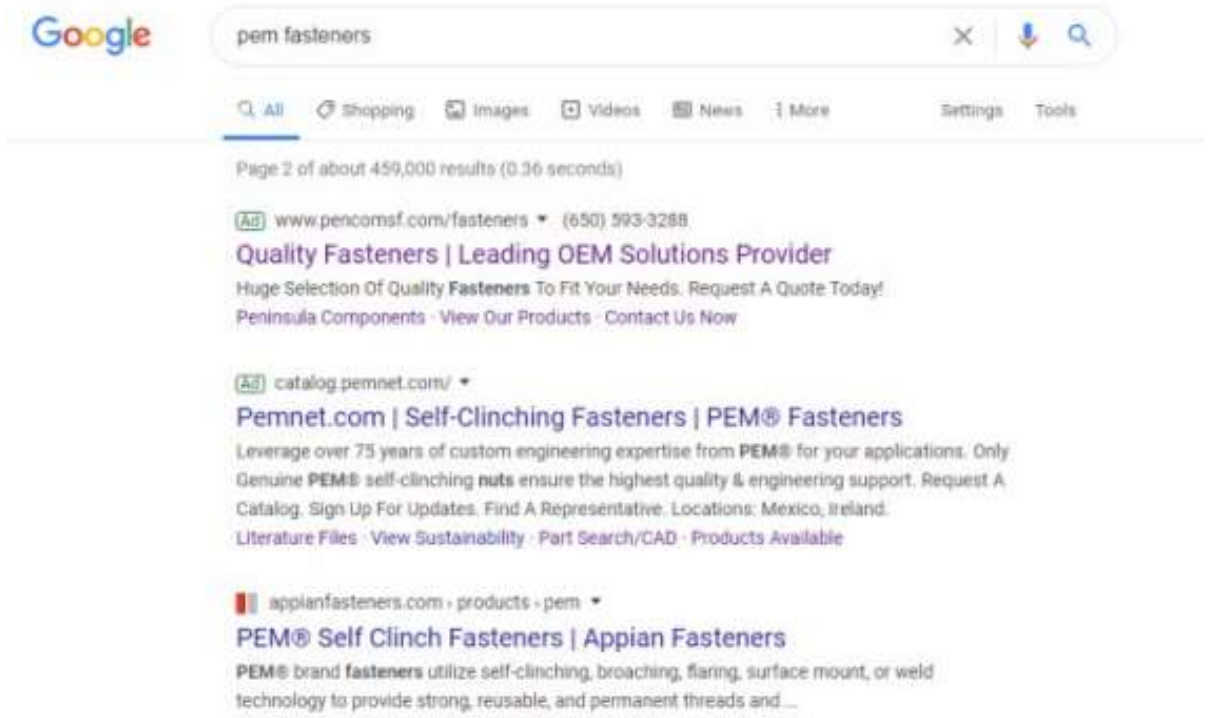
- PennEngineering and Peninsula are competitors in the market for industrial fasteners.



Use of Trademarks as Keywords

Penn Eng'g & Mfg. Corp. v. Peninsula Components, Inc. (E.D. Penn.)

PennEngineering argued that Peninsula's use of its trademarks as keywords triggered advertisements in search results (through Google Ads) causing initial interest confusion.



Use of Trademarks as Keywords

Penn Eng'g & Mfg. Corp. v. Peninsula Components, Inc. (E.D. Penn.)

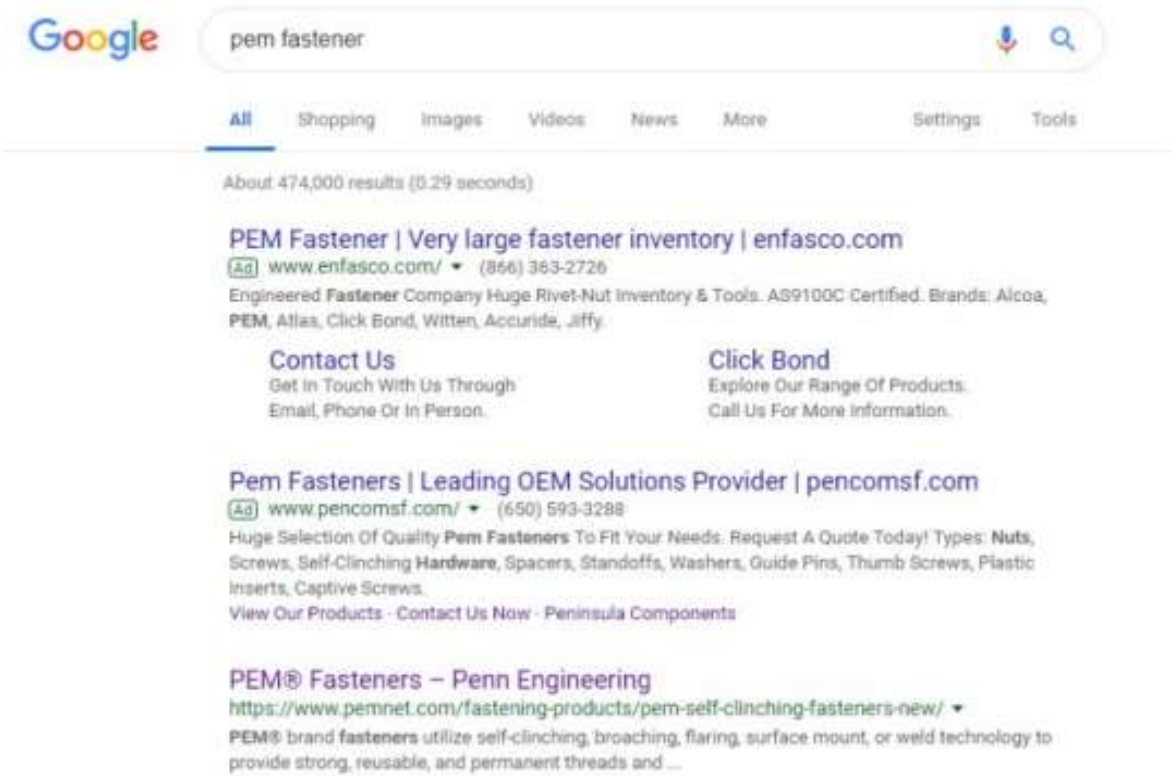
- **Hidden Use of "PEM" as Keyword**
  - Courts grants SJ in favor of Peninsula (as to hidden use only)
  - No likelihood of confusion as keywords were not visible and Peninsula's linked ads were clearly labeled as belonging to Peninsula

- ***What did Peninsula do right here?***
  - Peninsula's website appeared as one of several clearly labeled search results
  - Peninsula's website was clearly identified as belonging to Peninsula
  - Peninsula's use of "PEM" was "entirely invisible" to consumers

Use of Trademarks as Keywords

Penn Eng'g & Mfg. Corp. v. Peninsula Components, Inc. (E.D. Penn.)

- **Visible Uses of "PEM" as Keyword**
  - SJ denied as to visible use; triable issue regarding initial interest confusion from visible use of PEM mark

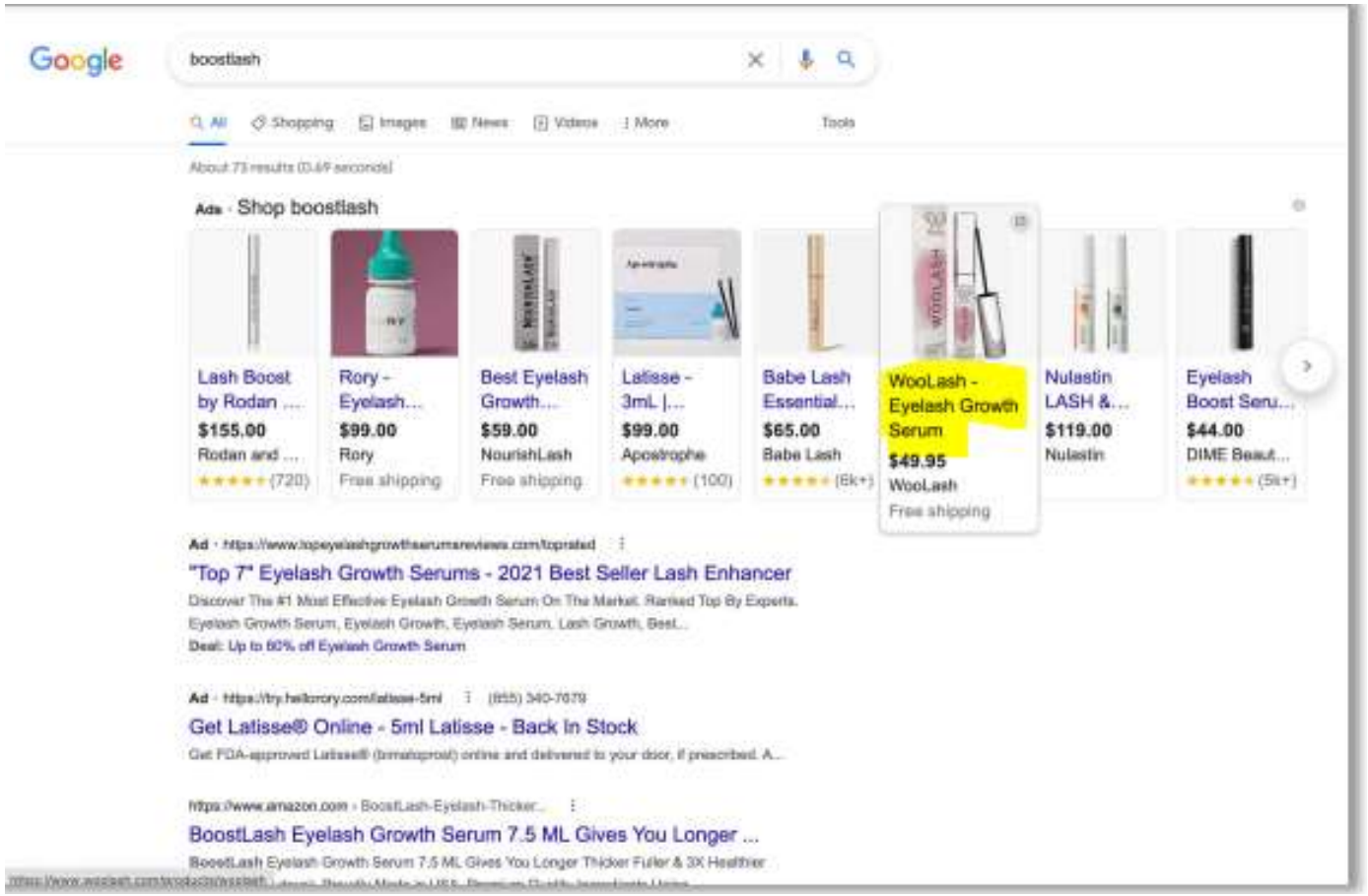


Use of Trademarks as Keywords
Boost Beauty, LLC v. Woo Signatures, LLC (C.D. Cal.)

- Boost Beauty and Woo Signatures sell competing eyelash growth serums under their respective BoostLash and WooLash marks.

Use of Trademarks as Keywords
Boost Beauty, LLC v. Woo Signatures, LLC (C.D. Cal.)

- Woo Signatures purchased BoostLash as a keyword on Google.



Use of Trademarks as Keywords
Boost Beauty, LLC v. Woo Signatures, LLC (C.D. Cal.)

Court granted summary judgment in favor of Woo Signatures

- No likelihood of confusion as a matter of law
  - WooLash product clearly labeled with no reference to Boost's product
- "In evaluating claims of trademark infringement in cases involving Internet search engines, an important additional factor is the **labeling and appearance of the advertisements and the surrounding context on the screen displaying the results page**." *Multi Time Mach., Inc. v. Amazon.com, Inc.,* 804 F.3d 930, 930 (9th Cir. 2015).
- "[I]n the keyword advertising context, the **likelihood of confusion will ultimately turn on what the consumer saw on the screen and reasonably believed, given the context**." *Id*. at 937.

Use of Trademarks as Keywords - Takeaways

Can I use third party trademarks as Keywords?

Safest to avoid using a third party's trademark as a Keyword

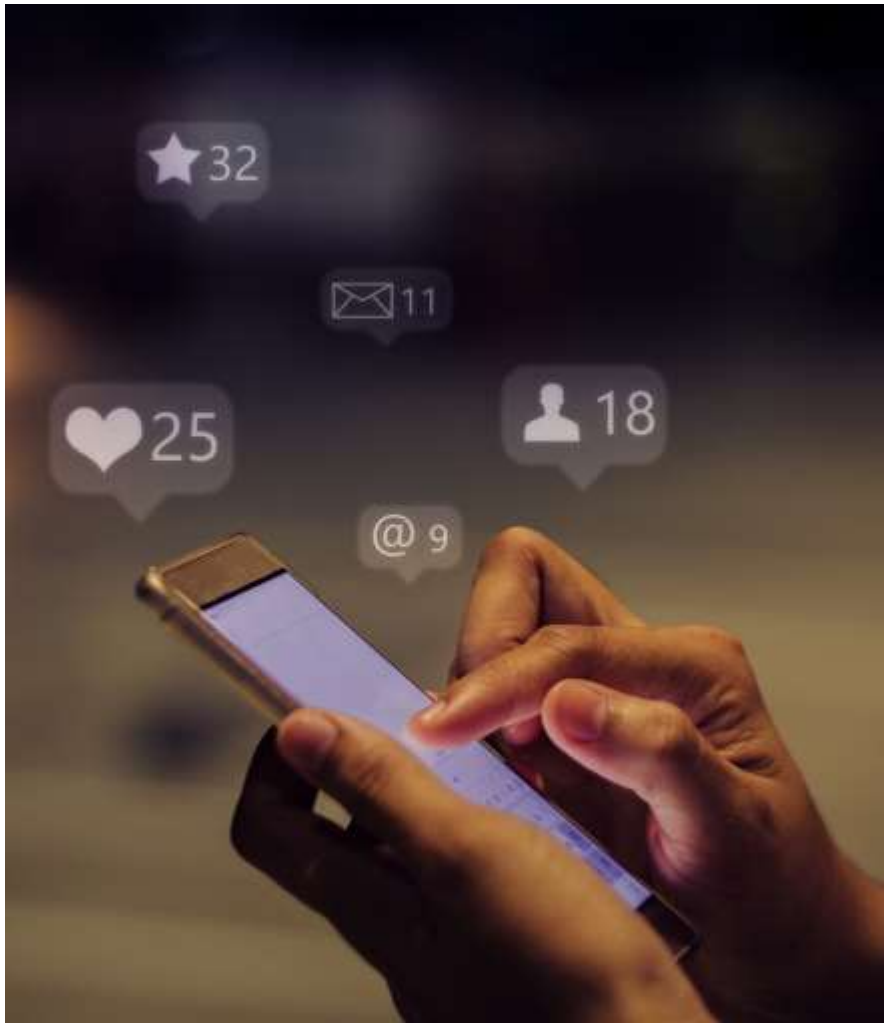
If you opt to use, you should:

- use in a hidden capacity only, and
- clearly label ads to avoid confusion

Use of Copyrighted Content on Social Media

When the Copyright Act was amended in 1976, the words "tweet," "viral," and "embed" invoked thoughts of a bird, a disease, and a reporter. Decades later, these same terms have taken on new meanings as the centerpieces of an interconnected world wide web in which images are shared with dizzying speed over the course of any given news day. That technology and terminology change means that, from time to time, questions of copyright law will not be altogether clear. In answering questions with previously uncontemplated technologies, however, the Court must not be distracted by new terms or new forms of content, but turn instead to familiar guiding principles of copyright.

Goldman v. Breitbart News Network, LLC, 302 F. Supp. 3d 585, 586 (S.D.N.Y. 2018)



Social Media: Fertile Ground for Copyright Litigation

- *Barbera v. Cyrus* (C.D. Cal. Sept. 2022)

Use of Copyrighted Content on Social Media

- To use copyrighted content online, one must either:
  - Own the copyrighted content
  - Have permission to use the content (e.g., a license)
  - Have a bona fide claim of fair use (remains a highly subjective test, even after *Warhol*)
    - **inherently risky to rely on a fair use defense**

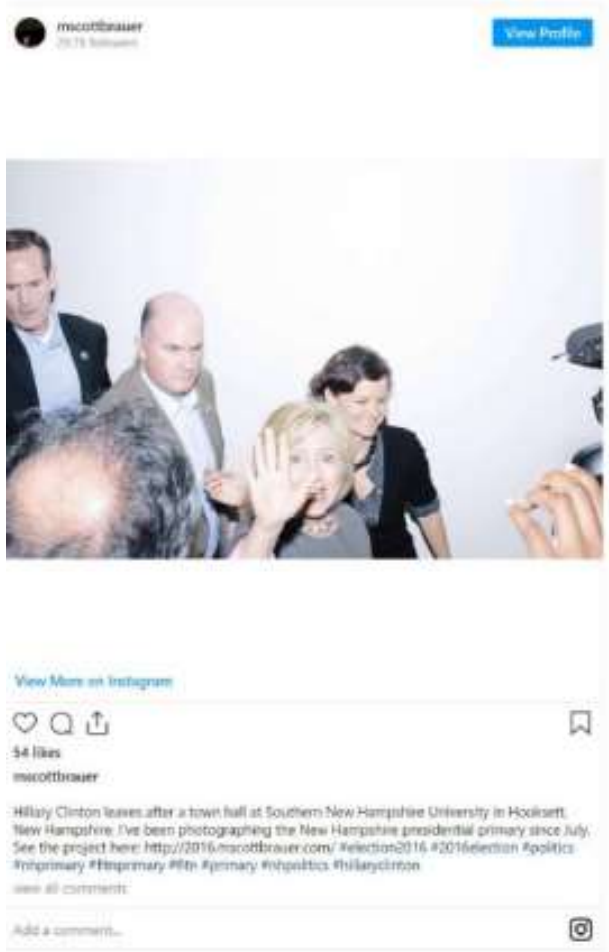
Does Embedding = Infringement?

- **Copyright ownership = exclusive right to copy / publicly display the work**

- **Embedding**
  - Embedding allows a third-party site (the embedding website) to incorporate content directly from the website where it originally appeared (the host website)
  - HTML instructions that direct a user's web browser to retrieve an image from a specific location on a server
  - Importantly, embedding does *not* create a copy on the embedding website or its server; remains stored on host website's server

- **Does embedding a copyrighted post constitute copying and public display?**
  - Ninth Circuit: No
  - Second Circuit: Yes

Hunley v. Instagram, LLC (9th Cir. 2023)



Plaintiffs sued Instagram, claiming that Instagram's embedding tool violated plaintiffs' exclusive display right by enabling third party websites such as *Buzzfeed* and *Time* to display copyrighted photos posted on Instagram

Hunley v. Instagram, LLC (9th Cir. 2023)

- District court granted Instagram's motion to dismiss for lack of direct infringement under the Ninth Circuit's "Server Test"

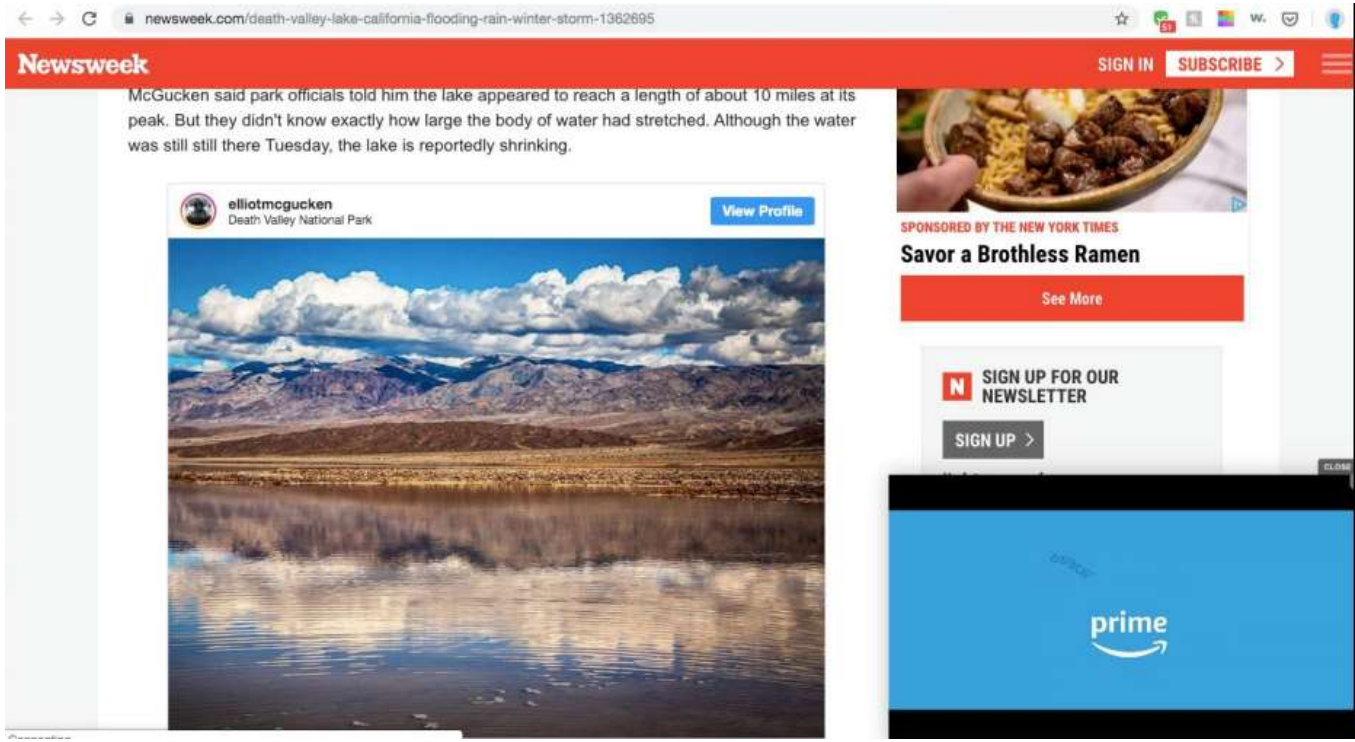
- Embedding does not constitute *copying or displaying*.
  - "Because [*Buzzfeed* and *Time*] do not store the images and videos, they do not 'fix' the copyrighted work in any 'tangible medium of expression.' See 17 U.S.C. § 101 . Therefore, when they embed the images and videos, they do not display 'copies' of the copyrighted work."

- Without direct infringement by *Buzzfeed*/*Time*, Instagram could not be held secondarily liable

- Ninth Circuit affirmed; Server Test remains applicable

McGucken v. Newsweek LLC (SDNY 2022) – Rejecting Server Test

- Plaintiff's photo embedded in *Newsweek* article
- Parties filed cross MSJs. *Newsweek* moved for SJ on, *inter alia*, the Server Test.
- District Court expressly renounced the Ninth Circuit's "Server Test."
- Copyright Act defines "display" as "to show a copy of" a work, and by embedding the photograph in its article, *Newsweek* did display plaintiff's work



Embedding On The Basis Of A Fair Use Defense?

Fair Use Factors:

1. The purpose and character of the use
    1. Whether the use is for a commercial versus educational/nonprofit purpose
    2. Whether the use is “transformative,” i.e., a different character/purpose than the original work
2. The nature of the copyrighted work.
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole.
4. The effect of the use upon the potential market for, or value of, the copyrighted work.

Does *Warhol* Decision Impact Fair Use Analysis?

- Supreme Court held that Warhol's use of a photograph of Prince without photographer Goldsmith's permission did not constitute fair use under the first factor, i.e., not transformative

- Decision relies largely on the fact that Warhol's use was commercial and was for a similar purpose as the original (i.e., licensed to a magazine)

- Important to ask: Does the use divert revenue away from the original copyright holder?

- Decision does not materially change fair use analysis (remains subjective), but does emphasize the commercial nature of defendant's use

Best Practices For Using Copyrighted Content on Social Media

- Given the Circuit split, best to avoid embedding images
- Create your own social media content
- Find royalty free content for your social media posts (ensuring license extends to commercial/editorial uses)
  - Creative Commons / Flickr
- If using third party content on your social media, always ask permission from the content's original creator
  - Written license is best
  - Ensure license extends to social media use
- Relying on a fair use defense remains inherently risky, particularly where use is commercial in nature and may be viewed as diverting revenue from plaintiff

ARTIFICIAL INTELLIGENCE

FTC and AI

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

- Has issued warnings, guidance, policy statements, and engaged in enforcement actions related to AI and potential harms to consumers and competition
- Key Topics
  - Privacy, biometric privacy and security
  - Accuracy
  - Fairness and non-discrimination
  - Transparency and Explainability
  - Safety and reliability
  - Advertising

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.

Digital Content

Claims about digital ownership and creation in the age of generative AI

- Purchase vs. License
- Unilaterally changing terms
- Undermining reasonable ownership expectations (e.g., AI vs. human-created content)
- Clear terms regarding rights and access
- Clear disclosures regarding AI tool training data (e.g., copyrighted or otherwise protected material)

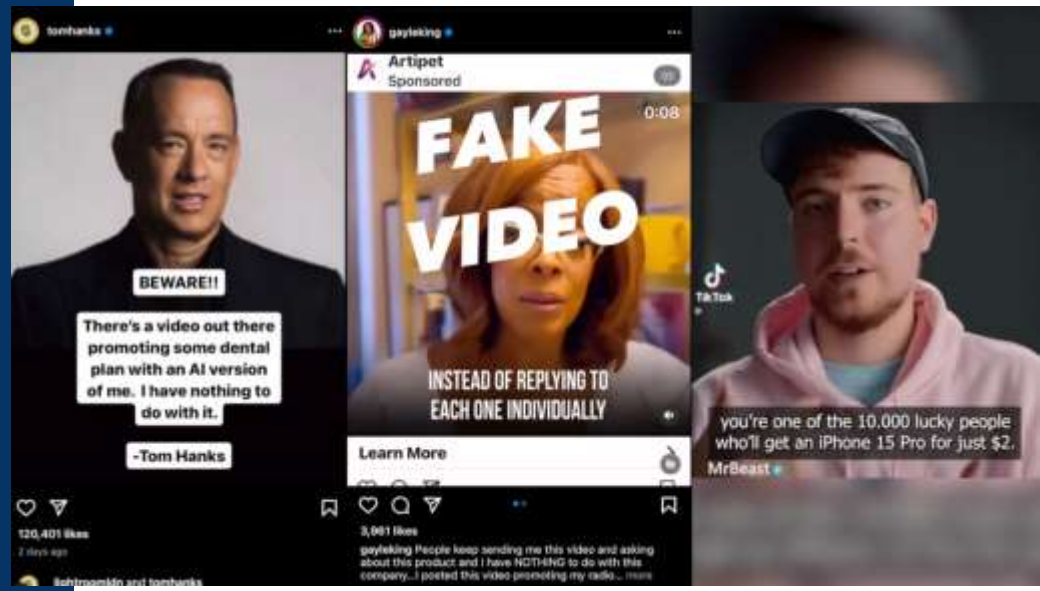
FTC Guidance:

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.

Chatbots, deepfakes, and voice clones: AI deception for sale

- Increased use of AI to create deceptive content, including deepfake videos, voice clones, chatbots, and other forms of synthetic media.
- Cautioning against the spread of fraudulent content like fake consumer reviews, phishing emails, and impostor scams facilitated by AI technology.
- Emphasis on the responsibility of companies to mitigate risks associated with AI tools and prevent consumer harm.
- FTC proposes new protections to combat AI impersonation of individuals



Other Regulatory Guidance and Enforcement Examples

April 2023 – FTC guidance on enforcement efforts against AI systems that result in illegal discrimination, such as in credit, employment, housing, or health care

May 2023 – FTC policy statement on biometric information; FTC will challenge the misuse of biometric information (facial recognition, fingerprints, iris scans, or voiceprints) by AI

March 2024 – SEC cracks down on over-hyped AI claims

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

Developing AI Policies

- Do data mapping/audit for data used to train AI; ensure the right to use the data for the intended purpose
- Ensure compliance with any applicable restrictions/obligations in any licenses
- Responsible AI – fair, transparent, explainable (test for bias, discrimination)
- Employee Use Policy
- Truthful advertising

Questions?

Thank you!

Keep Up To Date

See articles on
Artificial Intelligence

Subscribe
to blog for updates

ACC Association of Corporate Counsel SAN DIEGO

SheppardMullin