White & Case LLP CLE Materials: ANA 2024 Law Conference

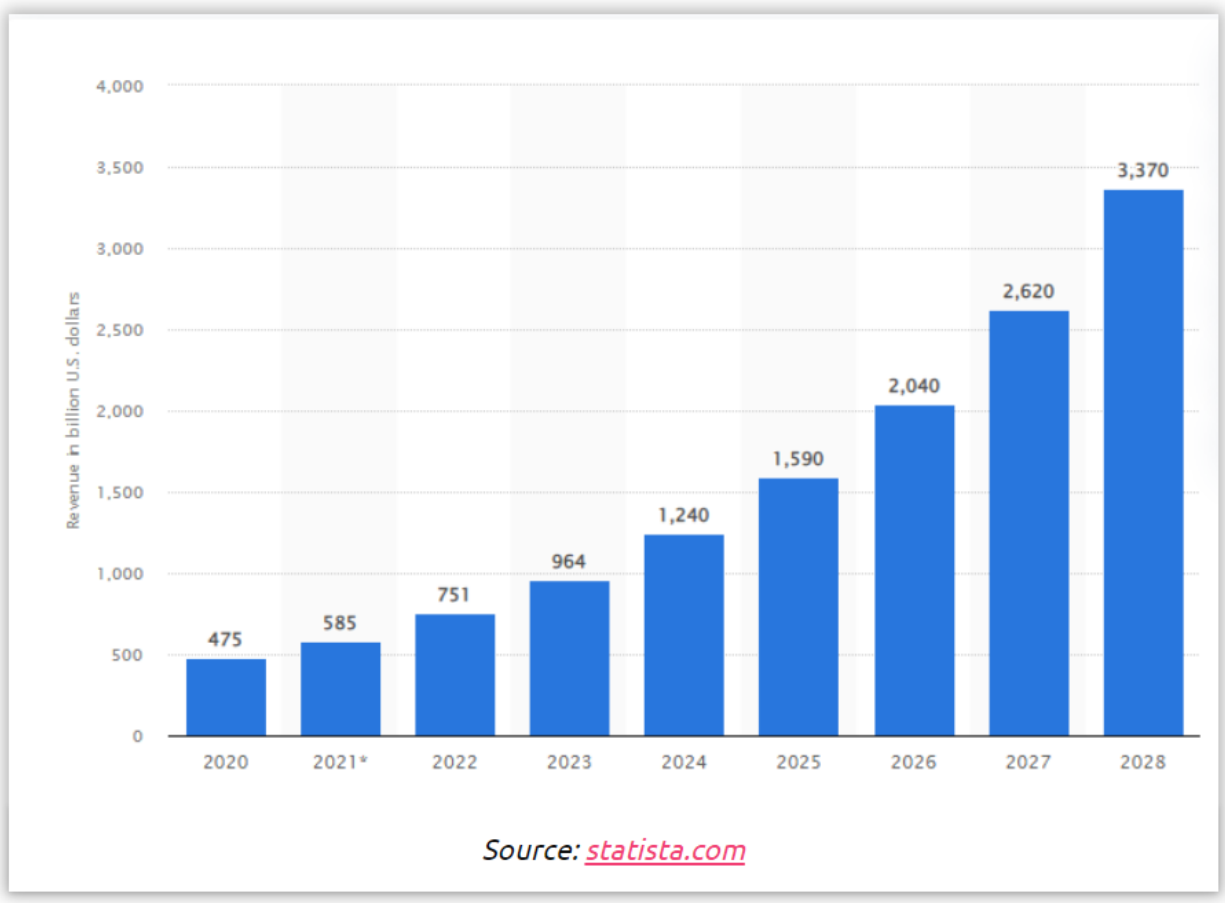
Topic: When Shopping, Social Media Content, and AI Collide: Spotlight on eCommerce and Platform Litigation Trends

Speakers: Anna Naydonov; TBD

Trending Social Commerce:

- Social media platforms are more and more becoming destinations to shop.

- **Data and survey results for reference to demonstrate the trend**:
  - 98% of customers plan to utilize social purchasing to make at least one purchase this year; up from 68% last year. *Source*: influencermarketinghub.com
  - Social commerce generated $475 billion in sales in 2020 and is expected to generate $3.37 trillion by 2028. *Source*: Statista.



  - According to a 2023 study, Facebook ranks as the top social network for shopping in the United States, with 20.6 percent of digital buyers using it as a shopping destination.
    - Instagram follows closely, with 11.8 percent of U.S. shoppers;
    - YouTube comes in third with 10.7 percent.
      - *Source*: Statista.

- Statista forecasts suggest that by 2029, the number of U.S. social media users will exceed 340 million.

- Retailers and brands rely on social media to engage consumers, with games, entertainment, and other forms of creative content.

AI Challenges on E-Commerce and Social Media:

- Using AI-Generated, Deep Fake, and Other Celebrity "Endorsements":
  - In fear of her image created by generative AI to falsely endorse Donald Trump, Taylor Swift posted on Instagram that she would support Harris.
    - Swift was a victim of deepfake nude photos spread on "X", formerly known as Twitter, sparking outrage and controversy over deepfake AI.

- FTC's New Rule on Fake and AI-Generated Reviews and Social Media Bots:
  - August 14, 2024, the FTC announced a final rule that prohibits fake and artificial intelligence-generated consumer reviews, consumer testimonials, and celebrity testimonials, along with other types of unfair or deceptive practices involving reviews and testimonials.
  - The rule will go into effect in October 2024.

- FTC's Operation AI Comply:
  - Through Operation AI Comply, the FTC is taking action against several companies that have relied on AI to engage in deceptive or unfair conduct.
    - "Claims around artificial intelligence have become more prevalent in the marketplace, including frequent promises about the ways it could potentially enhance people's lives through automation and problem solving. The cases included in this sweep show that firms have seized on the hype surrounding AI and are using it to lure consumers into bogus schemes, and are also providing AI powered tools that can turbocharge deception."

  - <u>Cases</u>:
    - *FEDERAL TRADE COMMISSION v. EMPIRE HOLDINGS GROUP LLC et al.*, 2:24-cv-04949 (E.D. Pa.)
      - The FTC brought an enforcement action against a business opportunity scheme falsely claiming to help consumers build an "AI-powered Ecommerce Empire" by "participating in its training programs that can cost almost $2,000" or by buying a "done for you" online storefront for tens of thousands of dollars. Empire Builders (EEB) claimed consumers have the potential to make millions of dollars. The FTC's complaint alleged that those profits fail to materialize.
      - The complaint alleged that EEB's CEO used consumers' money to enrich himself while failing to deliver on the scheme's promises of big income by selling goods online. Through marketing, EEB encourages consumers to "Skip the guesswork and start a million-dollar business today" by harnessing the "power of artificial intelligence" and the scheme's supposed strategies.
      - In social media ads, EEB claimed its clients can make $10,000 monthly, but the FTC's complaint alleged that the company has no evidence to support this claim. In reality, multiple consumers complained that stores

they purchased from EEB made little or no money, and that the company resisted providing refunds to consumers.
        - The district court issued an order temporarily stopping the scheme. The case is ongoing.

    - *FEDERAL TRADE COMMISSION v. THEFBAMACHINE INC. et al.*, 2:24-cv-06635 (D.N.J.)
        - FTC brought an enforcement action against a business opportunity scheme that allegedly falsely promised consumers that they would make guaranteed income through online storefronts that utilized AI-powered software. According to the FTC, the scheme cost consumers more than $15.9 million based on deceptive earnings claims that rarely, if ever, materialized.
        - The complaint alleged that Bratislav Rozenfeld launched the scheme in 2021 as Passive Scaling. When Passive Scaling was discovered to be a scam and consumers sought refunds and brought lawsuits, Rozenfeld rebranded it as FBA Machine in 2023. FBA Machine's marketing materials claim that it uses "AI-powered" tools, such as those for pricing products and maximizing profits.
        - The scheme promised consumers that they could operate a "7-figure business" and cited supposed testimonials from clients who "generate over $100,000 per month in profit." FBA Machine employees told consumers that the business was "risk-free" and falsely guaranteed refunds to consumers who did not make back their initial investments, which ranged from tens of thousands to hundreds of thousands of dollars.
        - The district court issued an order temporarily stopping the scheme. The case is ongoing.

Communication Decency Act Section 230's Safe Harbor Rules:

- What Is the Section 230 Safe Harbor?
    - "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."
    - Limited liability provision that gives companies broad immunity from legal complaints related to content on their platforms.
    - Immunity for companies when they take action against content deemed as "obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable."

- Whether a Platform's Recommendation Algorithm Is Protected by Section 230:
    - So far, social media companies have not been held liable for the consequences of their recommendation algorithms.
    - The Supreme Court sidestepped the question in the following two cases.
    - Cases:

        - *Twitter, Inc. v. Taamneh*, 143 S. Ct. 1206 (2023).
            - Plaintiffs sought to hold Twitter liable for aiding and abetting a terrorist attack, thereby violating the Antiterrorism Act, under which U.S. nationals who are injured in an act of terrorism can sue anyone who "aids and abets" international terrorism "by knowingly providing substantial assistance."

        - Plaintiffs alleged that Twitter had provided substantial assistance to the 2017 terrorist attack by knowingly allowing ISIS and its supporters to use Twitter's recommendation algorithms as tools for recruiting and fundraising.
    - SCOTUS rejected the argument on the grounds that the link between Twitter and the 2017 ISIS attack was too attenuated to justify holding Twitter liable.
        - Mere knowledge of a terrorist group's use of Twitter to promote terroristic activities generally was deemed insufficient to qualify as aiding and abetting.
    - "The fact that these algorithms matched some ISIS content with some users thus does not convert defendants' passive assistance into active abetting."

- *Gonzalez v. Google LLC,* 143 S. Ct. 1191 (2023).
    - Plaintiffs—parents of a 2015 ISIS terrorist attack victim in Paris—alleged that online platforms like YouTube should be held liable for recommending third-party content to users through its algorithms.
    - The Ninth Circuit held that the claim was barred by Section 230.
    - SCOTUS declined to address the issue. Instead, the Court remanded the case back to the Ninth Circuit in light of the *Taamneh* decision.

- Whether Section 230 Immunizes a Platform from Liabilities From AI-Generated Content:
    - <u>Cases</u>:
        - *Anderson v. TikTok, Inc.*, No. 22-3061, 2024 WL 3948248 (3d Cir. Aug. 27, 2024)
            - Mother of social media user, who died as result of participation in "challenge" in which users recorded themselves engaging in acts of self-asphyxiation, brought action against social media platform.
            - The Third Circuit reversed lower court's dismissal of the case and found that TikTok could be held liable for the plaintiff's daughter's death, finding that such claim is not immune under Section 230 of the CDA. The court found that Tik Tok is liable for continuing to host "blackout challenge" videos, despite knowing they were causing the deaths of children, and the plaintiff's claims seeking to hold it liable for its targeted recommendations of videos it knew were harmful should proceed.

- Proposed New Legislation Reform:
    - Proposed legislation to strip Section 230 immunity when civil and criminal lawsuits relate to AI-generated content.
    - The "SAFE TECH Act" proposed to address cyber-stalking, discrimination and online harassment while removing Section 230 protections for ads and paid content.

- Company Action:
    - Meta announcement in April 2024 that it will begin adding "AI info" labels to a wider range of video, audio and image content when it detects industry standard AI image indicators or when people disclose that they're uploading AI-generated content.

The DMCA Notice and Takedown System for Social Media Platforms:

- The DMCA Notice and Takedown System (17 U.S.C. § 512)

- When Is a Takedown Not Enough?
  - Cases:
    - *Sony Music Ent. v. Cox Commc'ns, Inc*., 93 F.4th 222 (4th Cir. 2024)
      - In 2018, Sony Corp. and other music industry groups sued Cox claiming that Cox should be held responsible – or secondarily liable – for its customers' alleged copyright infringement.
      - In 2019, a jury found Cox liable under two theories -- vicarious infringement and contributory infringement. Cox then appealed.
      - In February 2024, the Fourth Circuit Court of Appeals reversed the verdict holding that Cox was not vicariously liable for the actions of its consumers. But it ruled that Cox was liable for contributory infringement.
      - Cox has appealed to SCOTUS contesting that aspect of the Appellate Court decision.
        - Cox argues that the ruling, should it stand, would force ISPs to terminate internet service to households or businesses based on unproven allegations of infringing activity, and put them in a position of having to police their networks—contrary to customer expectations. This would result in a fundamental change to how ISPs must manage their networks as many may feel that the only way to avoid liability is to monitor the activity of their subscribers to ensure no one is engaging in potentially unlawful conduct.

- Rise in Lawsuits Regarding Fraudulent Takedown Notices:
  - Cases:
    - *Amazon.com Inc et al v. Morton et al*, 2:24-cv-01471 (W.D. Wash.); *Amazon.com Inc v. Singh*, 2:24-cv-01464 (W.D. Wash.)
      - Amazon's Counterfeit Crimes Unit (CCU) brought suit against multiple bad actors who submitted false infringement notices in an effort to have the accused listings removed.
        - Amazon alleged the false takedown notices "harmed Amazon selling partners and customers by attempting to reduce product selection, thereby damaging the integrity of Amazon's store."

    - *Benson Mills Inc. v. Fortenberry*, 2024 U.S. Dist. LEXIS 115844 (W.D. Was. Jul. 1, 2024)
      - Plaintiff accused defendant of sending false takedown notices to Amazon when plaintiff owned copyrights.
      - Defendant did not appear in action and Plaintiff showed it was entitled to default judgment under its DMCA and unfair competition claims.
        - Plaintiff entitled to entry of injunctive relief prohibiting defendant from submitting fraudulent takedown notices.
      - Court went through Ninth Circuit's *Eitel* factors to conclude Plaintiff entitled to default judgment.
        - Plaintiff identified specific DMCA takedown notices submitted, the targeted products and the copyright registrations.

- Court found Plaintiff demonstrated entitlement to permanent injunction prohibiting any further sending of false DMCA notices.
    - Plaintiff suffered irreparable injury through removal of its products and photos from Amazon, one of its largest selling channels (court cited *Beyond Blond* here)
    - Plaintiff alleged notices occurred over course of five months and would likely continue.
    - Burden on defendant was not a hardship because the narrow language of the injunction merely requires him to follow the law.
    - Court edited injunction language to ensure injunction only applied to Defendant and his agents.

- *Google LLC v. Van Duc*, 2024 U.S. Dist. LEXIS 144187 (N.D. Cal. Jul. 23, 2024)
    - Plaintiff brought claims including for misrepresentation under 512(f) of the DMCA.
        - Plaintiff alleged defendants submitted fraudulent takedown notices to Google's copyright agent unlawfully seeking removal of more than 117,000 third-party URLs and product listings, and they were subsequently delisted.
        - Plaintiff alleged economic harm from lost advertising revenue and business relations as well as expending resources to investigate and remedy the fraudulent notices.
    - Plaintiff was authorized to serve defendants via Gmail accounts and phone numbers fraudulent notices originated from.
    - Defendants did not answer or respond to complaint and clerk entered notice of default.
        - Court found Ninth Circuit *Eitel* factors favored default judgment.
    - Court found Plaintiff correctly alleged required elements under 512(f) of Defendant's knowing misrepresentations, that Plaintiff relied on them and was subsequently injured.
    - Magistrate judge recommended granting motion for default judgment and granting injunctive relief.
    - Proposed injunctive relief recommended included enjoining:
        - Submitting any notifications of copyright infringement or takedown requests to Plaintiff based on false assertions of right of copyright ownership.
    - District court adopted the recommendation and enjoined the defendant.