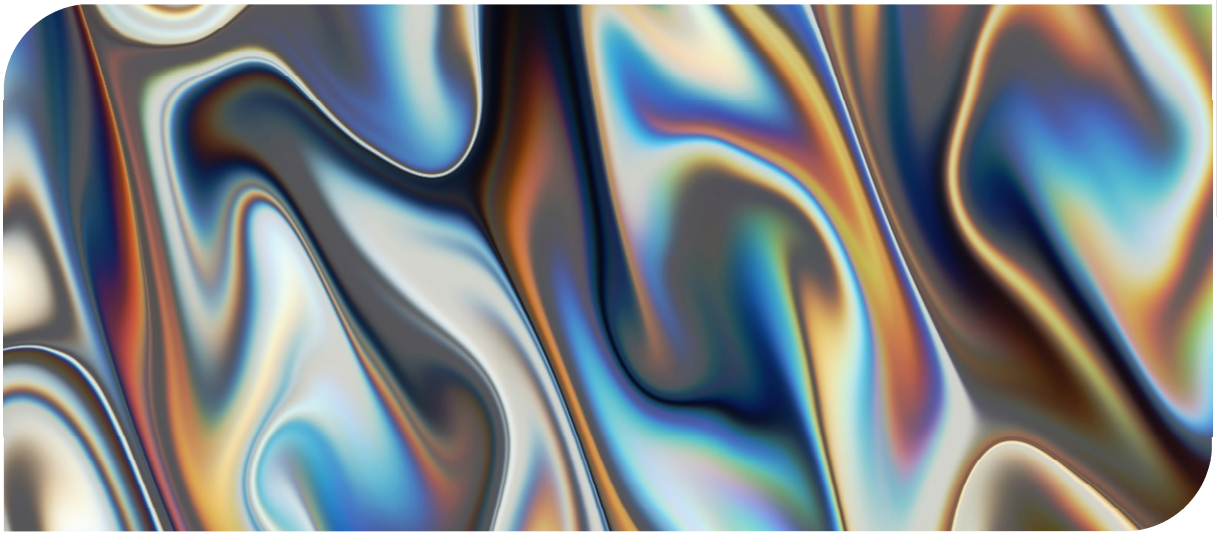
DAVIS + GILBERT



Consumergeddon – Can You Survive The Deceptors?

2024 ANA Masters of Advertising Law Conference

November 12, 2024

Ronald Urbach

Partner/Co-Chair, Advertising + Marketing
Davis+Gilbert LLP
rurbach@dglaw.com

DAVIS GILBERT

Table of Contents

Advertising Law and Regulatory Framework

DAVIS + GILBERT

Advertising Law and Regulatory Framework

A. Overview

Federal Law

a. Federal Trade Commission Section 5 of FTC Act (15 U.S.C. § 45)

   i. Deception: Misrepresentations or omissions likely to mislead consumers acting reasonably under the circumstances

   ii. Unfairness: Acts or practices that cause or are likely to cause substantial consumer injury, not reasonably avoided by the consumer, and not outweighed by countervailing benefits to consumers or competition

b. Lanham Act, §43(a)

   i. "Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any…false or misleading description of fact, or false or misleading representation of fact, which…in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable to a civil action by any person who believes that he or she is likely to be damaged by such act."

State Laws

a. State Unfair Competition Laws – differ by state and enacted by most jurisdictions:

   i. "Baby FTC Acts" are modeled after FTC Act

      1. One critical difference between the FTC Act and most Baby FTC Acts is that the latter allows for private enforcement.

   ii. The Uniform Deceptive Trade Practices Act

      1. Some state consumer protection laws are based on the UDTPA the primary feature being an itemized list of twelve specific practices deemed to be deceptive, which include, among other things, misleading trade identification (e.g., passing off and trademark infringement), false advertising, deceptive advertising, and a catchall ban on "any other conduct which similarly creates a likelihood of confusion or misunderstanding."

Enforcement of the Law

a. Government agencies, like the Federal Trade Commission, Federal Communications Commission, Food and Drug Administration, state Attorney Generals.

   i. In its holding in *Loper Bright Enterprises v. Raimondo,* 603 U.S. ___ (2024), 144 S. Ct. 2244, the Supreme Court overturned decades of precedent of deference to federal agency rulemaking and enforcement under *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.,* 467 U.S. 837 (1984). Under *Loper Bright*, courts can no longer defer to an agency interpretation of the law simply because a statute is ambiguous. This will increase scrutiny on federal agency rulemaking and may limit the ability of federal agencies to enforce unclear statutes.

b. Self-Regulatory Bodies (e.g., National Advertising Division ("NAD"), Digital Advertising Alliance, Children's Advertising Review Unit, Advertising Self-Regulation Council, Direct Marketing Association etc.).

c. Competitors. Companies monitor and contest the "errors" of their competitors.

d. Consumers. Individuals can sue advertisers, but most consumer lawsuits are in the form of class action lawsuits.

e. Rights owners (e.g., copyright and trademark owners, personality rights holders).

B. Reasonable Person

General Principles

a. The reasonable person standard is used in advertising law to determine whether:

   i. Consumers may be misled by an advertisement;

   ii. consumers interpret certain claims as fact or opinion (e.g., in a puffery analysis);

   iii. a claim is material to the purchasing decision.

Standard for the Reasonable Consumer

a. The advertising practice at issue must be examined "from the perspective of a consumer acting reasonably in the circumstances." F.T.C. Policy Statement on Deception, 103 F.T.C 110, 174 (1984) (http://www.ftc.gov/bcp/policystmt/ad-decept.htm).

b. "To be considered reasonable, the interpretation does not have to be the only one. When a seller's representation conveys more than one meaning to reasonable consumers, one of which is false, the seller is liable for the misleading interpretation. An interpretation will be presumed reasonable if it is the one the respondent intended to convey." F.T.C. Policy Statement on Deception, 103 F.T.C 110, 174 (1984) (http://www.ftc.gov/bcp/policystmt/ad-decept.htm).

c. If the representation or practice affects or is directed primarily to a particular group, the FTC examines reasonableness from the perspective of that group (e.g., children, the elderly or educated professionals).

d. To be deceptive, an advertisement must be likely to mislead this reasonable consumer, and the consumer's interpretation must be reasonable in light of the claims made.

e. The act or practice in question must be likely to mislead a consumer acting reasonably under the circumstances in a material respect.

Definition of the Reasonable Consumer

a. The FTC has defined the reasonable consumer as a typical person who:

   i. Makes decisions based on a "net impression" of the advertisement or representation.

      1. *See Telebrands Corp*., 140 F.T.C. at 290 (2005), *aff'd,* 457 F.3d 354 (4th Cir. 2006), in which the Commission found that a reasonable consumer would take into account the "net impression" of an advertisement for an abdominals-firming device. "Net impression" was defined as the "interaction between and among the constituent elements of the ad." This included express and implied claims as well as omission. The FTC found that to be found misleading, the advertisement must be likely to mislead this reasonable consumer, either by direct statement or indirect suggestion.

      2. *See also JTH Tax, Inc. v. H & R Block E. Tax Servs., Inc.,* 28 Fed. Appx. 207, 214 (4th Cir 2002), in which the judgment concluded that a tax preparation service provider engaged in false and deceptive advertising when representing a new loan product as a 'refund amount' in its advertising campaign, since this overall representation would affect a reasonable consumer's purchasing decision.

   ii. Does not interpret the advertisement in a rare or unusual manner that is not shared by a "significant minority" of similarly targeted persons.

1. As noted in the FTC Policy Statement, the Commission has evaluated advertising claims in light of the sophistication and understanding of the targeted persons. The "reasonable person" standard applies to a reasonable member of the category of persons to whom the advertising was directed.

2. The reasonable person need not share his interpretation of the advertisement with a majority of the interpreting audience as long as a "significant minority" would share his view. Although the FTC does not quantify what constitutes a "significant" minority of an audience, in *Telebrands*, a significant minority was judged to be 10% (or even lower), though in most FTC cases the deception threshold for the reasonable consumer is about 20-25%.

C. Reasonable Basis

General Principles

a. Advertisers must substantiate both the express and implied claims that make objective assertions about the item or service advertised when these representations of substantiation are material to consumers.

   i. FTC has stated that consumers would be less likely to rely on the claims made about a product or service if they knew that the advertiser did not have a reasonable basis for believing them to be true, and for that reason the consumer's purchasing decision could be affected.

b. An advertiser's failure to possess and rely upon a reasonable basis for objective advertising claims constitutes an unfair and deceptive act or practice in violation of Section 5 of the Federal Trade Commission Act.

Prior Substantiation Doctrine

a. Advertisers must have a reasonable basis for advertising claims before they are disseminated. This requirement applies to both express and implied claims.

b. If an ad implies more substantiation than it expressly claims or implies to consumers that the product/service has a certain level of support, the advertiser must possess the amount and type of substantiation the ad actually communicates to consumers.

c. Absent an express or implied reference to a certain level of support, and absent other evidence indicating what consumer expectations would be, the FTC requires that advertisers and their agencies have a "reasonable basis for advertising claims before they are disseminated." *See* FTC Policy Statement Regarding Advertising Substantiation, 49 F.R. 30999 (1984).

Reasonable Basis

a. Generally, means competent and reliable scientific evidence.

b. What constitutes competent and reliable evidence depends upon a variety of factors, including:

   i. The type of claim;
   ii. the media in which the claim appears;
   iii. the product;
   iv. the consequences of a false claim;
   v. the benefits of a truthful claim;
   vi. the cost of developing substantiation for the claim; and
   vii. the amount of substantiation experts in the field believe is reasonable.

c. Evidence of a reasonable basis generally includes tests, analyses, research, studies, or other evidence based on the expertise of professionals in the relevant area that:

   i. Has been conducted and evaluated in an objective manner;
   ii. by persons qualified to do so; and
   iii. using procedures generally accepted in the profession to yield accurate and reliable results.

d. Where tests and surveys are used to support a claim, the sample size must be large enough so that the results can be projected to the audiences to whom the claim is directed. Moreover, claims must be statistically significant at the 95% confidence level.

e. Not only must an advertiser have a reasonable basis for its advertising claims prior to dissemination it must also ensure that it has such substantiation as its advertising continues to run.

f. In April 2023, the FTC issued nearly 700 Notices of Penalty Offenses to various companies for failing to adequately substantiate product claims. The FTC cited unlawful practices including making an objective product claim without having a reasonable basis of competent and reliable evidence at the time the claim is made and misrepresenting the type or level of substantiation for a claim. While receiving a Notice of Penalty Offense does not indicate fault on the part of a company, it does give the recipient actual knowledge of the FTC regulations around claim support, and entitles the FTC to seek enhanced civil penalties in the event of a subsequent violation after the recipient has been put on notice.

Nature of the Claim

a. A key consideration for the advertiser in determining the adequacy of its level substantiation should be the type of claim that it is making and the media in which the claim appears.

b. Claim Stating Substantiation

   i. When the type/degree of substantiation is explicitly stated (e.g., "tests prove" and "studies show") in the advertisement, the advertiser must possess at least the advertised level of substantiation.

c. Claim Implying Substantiation

   i. When a certain type/degree of support is implied by the advertisement, the advertiser must possess the amount and type of substantiation the advertisement actually communicates to consumers.

d. Puffery

   i. Substantiation is not required if the claim is generalized, non-specific and not expressly or implicitly grounded in facts (e.g., "the world's greatest coffee").

      1. Recently, the NAD has paid special attention to when claims cross the line from puffery to an objectively provable claim (and requires support). In cases involving "ultimate" claims, such as "ultimate immune system support" and "ultimate energy bar," the NAD determined that a claim is non-puffery when presented in a context with objectively measurable attributes. In cases involving "best" claims, like "best tasting," "world's best glass cleaner" and "world's best fruit and vegetable juice," the NAD conducts the same analysis – but seemingly has found that "world's best" claims are more likely to constitute puffery that simply "best" claims.

e. National Claims or National Media

   i. When a claim is geographically unqualified and/or appears in national media, the advertiser must possess substantiation demonstrating that the claim is true in each of the markets in which the advertising appears. If applicable, the advertiser can avoid the burden of substantiating the claim in each local market by disclosing the fact that the claim is based on certain national data and is not necessarily true in each market in which the advertisement appears.

f. Local Claims or Local Media

i. When a claim is geographically qualified or appears in local media, the advertiser must possess substantiation demonstrating that the claim is true as to that particular market.

g. Disease Treatment or Prevention Claims

i. Such claims should be substantiated by two well-designed, well-conducted, double-blind, randomized controlled clinical trials (RCTs). *See In the Matter of POM Wonderful LLC,* FTC File No. 082-3122, Docket No. 9344 (2012).

Comparative Advertising

a. Advertising in which an advertiser compares its product or service with that of a competitor, either directly or indirectly. While the "reasonable basis" standard still applies to comparative claims, an advertiser should pay particular attention to its substantiation, as comparative claims are considerably more likely to be challenged than general claims.

b. Claims Regarding Specific Competitors

i. Where a claim regarding a specific competitor is made in an advertisement, the advertiser must possess substantiation demonstrating that the claim is true as to that competitor.

ii. Tests or studies may be used to support a comparative claim. If the advertised product wins at the 95% confidence level on key attributes and is at parity on others, an overall superiority claim may be permitted. If the advertised product does not demonstrate wins for all key attributes, the claims must be limited to the winning attributes.

c. Claims Regarding Competitors Generally

i. The general rule is that where a product or service is being compared to an entire market, it must be tested against the top 85% of that market, based on current sales data.

D. Clear and Conspicuous Disclosure

General Principles

a. Advertisements can contain claims that require a disclosure to modify the claim. All disclosures need to be clear and conspicuous. *See, e.g., Thompson Medical Co.*, 104 F.T.C. 648, 842-43 (1984), *aff'd*, 791 F.2d 189 (D.C. Cir. 1986), *cert. denied*, 479 U.S. 1086 (1987). Fine print cannot be used to contradict statements or to correct misrepresentations. *See* FTC Policy Statement on Deception, *appended to Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984).

b. Material information must be disclosed in a clear and conspicuous manner so that the consumer will receive the message and all material information relevant to the advertising.

c. As consumers may only glance at a headline, accurate information in the text may not remedy a false headline. Disclosures should not contradict or be inconsistent with the headline.

d. The Federal Trade Commission regularly enforces this requirement and has sent warning letters to many advertisers for allegedly failing to make adequate disclosures in their advertising.

Factors for Disclosure

a. Audience: Does the disclosure take into account the target audience?

   i. If the advertisement is targeting a specific group, the advertisement must account for the ordinary needs of that specific group (e.g., vision, hearing and cognitive abilities of older adults or children).

   ii. If an advertisement is in a language other than English the disclosure should be in that language as well.

b. Prominence: Is the disclosure large enough for consumers to notice and read/hear it?

   i. Type size should be large enough to read easily.
   ii. Sharp contrast between disclosure and background.
   iii. Clear typeface.
   iv. Visual disclosures should be displayed long enough to be read.
   v. Audible disclosures should be delivered in a volume, speed, and cadence to be easily heard and understood.

c. Presentation: Is the wording and format easy to understand?

   i. Wording should be easy to understand.
   ii. Format should not inhibit careful reading.
   iii. Free of distractions that compete for consumer attention.
   iv. Consumers more likely to grasp disclosures made in same mode (visual and/or audio) as the claim it qualifies. A disclosure presented simultaneously in both visual and audible portions of a communication are more likely to be clear and conspicuous.

d. Placement: Is the disclosure located in a place or made in a format that consumers will see/hear? Specifically, is the disclosure located in a place or made in a format where the target audience will not miss it?

e. Proximity: Is the disclosure near the claim it qualifies?

f. *See, e.g.,* Dot Com Disclosures: Information about Online Advertising available at: https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf.

Print Disclosures

a. Fine-print footnotes and dense blocks of text are often inadequate to modify claims found in the print ad. *See, e.g., Am. Home Prods. Corp. v. Johnson & Johnson,* 654 F. Supp. 568, 590 (S.D.N.Y. 1987); *Stouffer Food Corp.*, 118 F.T.C. 746 (1994).

b. Adequacy of disclosure depends on location of disclosure in relation to the claim it is modifying. The more material a claim is, the closer the disclosure must be to the claim.

c. *In re Petition of Cricket Wireless, LLC*, 2023 Md. App. LEXIS 590

i. After the merger of Cricket and AT&T, Inc., the successor company planned on decommissioning Cricket's wireless network whereby Cricket consumers phones would no longer be operable. The company disclosed this fact in small print statements on stickers 2x3/4 inches in height, outlined in a black border, printed on a lighter backdrop located in the bottom left-hand corner of the phone box with additional small print disclosures at the bottom of the store's price cards displayed near the boxes. In a 2020 action, the Maryland Attorney General's office found that the foregoing disclosures failed to adequately disclose to Maryland consumers that their phones would no longer work. On appeal, the court found in favor of the state AG, concluding that the disclosures had the capacity, tendency, or effect of deceiving, misleading or damaging consumers.

Television Disclosures

a. Generally, all of the laws, rules and regulations that govern advertising apply to radio, television, and infomercial advertising. Networks maintain their own advertising standards, enforced through pre-submission of proposed advertising.

b. Advertisers often opt to alert consumers to existence of limitations and restrictions while highlighting material information.

c. Video superscripts that are hard to understand, superimposed over distracting backgrounds, compete with audio elements, or placed in non-memorable portions of the ad have been found ineffective. *See, e.g., United States v. Mazda Motor of America, Inc.,* (C.D. Cal. Sept. 30, 1999); *Chrysler Corp.,* C-3847 (Jan. 13, 1999).

Enforcement Actions:

d. *Mint Mobile, LLC*, NAD Case No. 7250 (September 2023)

   i. AT&T Services, Inc. ("AT&T") challenged the prominence and sufficiency of disclosures in connection with Mint Mobile's claim that its Unlimited plan is "now just $15/mo." In a television commercial promoting this plan the disclaimer the "Promotional rate for first three months" appears in small font at the bottom of the screen while actor, Ryan Reynolds, talks about the offer. AT&T argued that the disclosure should be part of the claim itself or equally prominent and in close proximity to the claim.

   ii. The NAD found that the advertising does not adequately disclose that the promotional offer was only for three months. In addition, specifically in the television commercial, NAD found that the prepaid nature of the services was not communicated. NAD recommended that Mint Mobile either discontinue the claim or clearly disclose that the offer is promotional for a three-month period as part of the main claim or in similar size text and font in close proximity to the main claim. Mint Mobile disagreed with the NAD's findings and indicated that it would appeal the decision.

Internet Disclosures

a. Generally, all the laws, rules and regulations that govern advertising apply to internet advertising.

b. If it is not possible to make a disclosure in an ad due to space constraints, in some circumstances it is acceptable to include the disclosure clearly and conspicuously on the page to which the ad links. In such cases, the link must:

   i. Be obvious.
   ii. Be labeled appropriately to convey the importance, nature and relevance of the disclosed information.
   iii. Use hyperlink styles consistently to alert consumers to the link.
   iv. Link directly to the disclosure on the click-through page.

c. Disclosures should not be relegated to "terms of use" or other contractual agreements.

d. Disclosures should be included in a size, color and graphic treatment that is noticeable to consumers. On social media platforms such as Snapchat and Instagram Stories, disclosures can be superimposed as text over images.

e. *See, e.g.*, Dot Com Disclosures: Information about Online Advertising available at: https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf; *FTC v. EDebitPay, LLC*, 2011 U.S. Dist. LEXIS 15750, (C.D. Cal Feb. 3, 2011).

Enforcement Actions:

f. *Diamond Foundry, Inc.*, NAD Case No. 6843 (March 2021)

   i. The FTC's Jewelry Guides provide that, in connection with the sale of manufactured diamonds, advertisers must clearly disclose the man-made nature of their product. The sufficiency of Diamond Factory's disclosures in connection with advertising for its laboratory-grown diamonds was challenged by Natural Diamond Council USA, Inc. ("NDC"), an association of the world's leading diamond companies. NDC noted that certain social media advertisements either simply described Diamond Foundry's man-made diamonds as "diamonds", and failed to disclose the man-made nature of the product, or, to the extent there was a disclosure, such disclosure was not easily visible, and required consumers (especially those on mobile devices) to scroll down the page.

   ii. The NAD agreed with NDC and recommended that Diamond Foundry update its adverting to ensure that necessary man-made disclosures are placed immediately preceding, and with equal conspicuousness, to the word "diamond". Further, the NAD advised that Diamond Foundry must take the mobile user experience into account when placing disclosures, to ensure that disclosures remain clearly visible to consumers, without requiring the consumer to scroll down the page or click additional buttons (like "more" or "view all comments" on Instagram) to see the disclosure.

g. *Agape Diamonds, LLC*, NAD Case No. 7191 (August 2023)

   i. The FTC's Jewelry Guides provide that, in connection with the sale of manufactured diamonds, advertisers must clearly disclose the man-made nature of their product. The sufficiency of Agape Diamonds' disclosures in connection with advertising for its laboratory-grown diamonds and simulated diamonds was challenged by NDC. NDC noted that certain advertisements either simply described Agape Diamonds' lab-grown and simulated diamonds as "diamonds" or "stones" and failed to disclose the man-made nature of the product, or, to the extent there was a disclosure, such disclosure was not easily visible, and required consumers to scroll down the page or click on a "click to see more" link.

ii. Agape Diamond maintained that its advertising was compliant with the FTC's Jewelry Guides, but nevertheless made adjustments to its advertising and NAD found that much of the modified advertisements were compliant with the FTC's Jewelry Guides. The NAD agreed with NDC and, to the extent not already reflected in Agape Diamond's updated advertising, recommended that Agape Diamonds update its adverting to ensure that necessary man-made disclosures are placed immediately preceding, and with equal conspicuousness, to the word "diamond" or "stone".

Native Advertising Disclosures

a. The terms "native advertising," "sponsored content," "branded content," and "advertorial" are all used to describe the practice of blending advertisements with news, entertainment, and other editorial content in digital or other media.

b. Before consumers choose to watch, read, view, or click on native advertising content, the FTC wants consumers to understand the content is advertising which has been created or paid for by an advertiser. In order to avoid consumer confusion if it is not apparent to consumers that the content is advertising, the FTC has indicated that additional disclosures may be necessary.

c. In December 2015, the FTC released an Enforcement Policy Statement on Deceptively Formatted Advertisements, supplemented by a Native Advertising Guide for Businesses (Native Advertising Guidelines) outlining why, when and how disclosures should be made when disseminating native advertising.

d. According to the FTC, if a consumer could be confused about whether native advertising was paid for or created by an advertiser, clear and prominent disclosures should be included to avoid misleading the consumer. In evaluating whether an advertisement's format is misleading, the FTC will examine the "net impression" of the ad, reviewing factors such as the similarity of the native ad's written, spoken or visual style to non-advertising content offered on a publisher's site, and the degree to which the appearance of the native ad is distinguishable from other content, for example, by using different fonts, colors, and shades.

e. The Native Advertising Guidelines set general parameters for businesses to determine what those disclosures should say, and how they should appear.

   i. As for what the disclosures should say, the Native Advertising Guidelines state that consumers are likely to understand terms such as "advertisement" or "sponsored advertising content," as opposed to "at best ambiguous" terms such as "promoted," which could lead consumers to believe that content is endorsed by a publisher site, or simply underwritten by the advertiser.

ii. As for how the disclosures should appear, disclosures should utilize font size, color, boldness, and placement on the page to ensure that they are clear and prominent to the consumer. Disclosures should appear in close proximity (in front of or above) the native advertising headline, accompanied by visual cues such as shading or borders, and not be buried in an end link. In addition, the FTC has stated that disclosures must follow the native advertising content wherever it is posted, including when it is republished via social media, email, search results, or other media.

Enforcement Actions:

f. *Lord & Taylor, LLC*, FTC File No. 152 3181 (May 23, 2016)

i. In May of 2016, the Federal Trade Commission approved a final consent order with national retailer Lord & Taylor, prohibiting it from, among other things, failing to properly disclose paid native advertising for its products by paying the online fashion magazine Nylon to run an article and Instagram post featuring a dress sold by Lord & Taylor. Neither the article nor the post disclosed that they were paid for by Lord & Taylor, which, according to the FTC, was deceptive to consumers.

ii. As part of the settlement, Lord & Taylor was prohibited from misrepresenting that its paid advertisements are the statements or opinions of independent, editorial publishers or sources.

g. *My Talking Tom,* CARU Case No. 6255 (February 2019)

i. In 2019, the Children's Advertising Review Unit (CARU) challenged, among other things, the adequacy of Outfit 7's disclosure practices in connection with its "My Talking Tom" video game app; a game which markets itself as being for both kids and adults.

ii. Within the app players were served advertisements in a variety of ways, including in the form of game play. Players were given the option to unlock a virtual prize by clicking on various icons, which could be characterized as native advertising. Once clicked, players were directed to complete the task of watching an advertisement in order to redeem a virtual prize.

iii. CARU found that, although there was some form of ad disclosure that appeared alongside the "watch video" to win a virtual prize directive, several of the disclosures were too small, and/or the language that accompanied the disclosure was contradictory or confusing. CARU stated that the disclosures were "presented in a manner that blurred the distinction between the advertising and the content in a manner that would be misleading to children", and recommended Outfit 7 take steps to

more clearly and conspicuously disclose that the content served as a result of clicking is advertising, and not part of the game.

h. *Amerisleep LLC*, NAD Case No. 6369 (May 2020)

   i. Casper Sleep, Inc. challenged the sufficiency of native advertising disclosures appearing on two mattress ratings and review websites, SleepJunike.org and Savvysleeper.org, which were both owned by Amerisleep, a competitor mattress manufacturer.

   ii. Disclosures were included on both websites, but were in small font, at the top of the page, in a position where large font drop down menu options easily obscured the disclosures or sandwiched between the website title and a large font headline. Further, the language of the disclosures did not clearly state the ownership relationship between Amerisleep and the sites.

   iii. NAD determined that not only were Amerisleep's disclosures insufficient, but that the content and format of the sites inherently conveyed a message that the sites were independent and not advertising – a message that could not be cured by disclosure. Any disclosure would directly contradict the inherent independent nature of the site. The NAD recommended that Amerisleep discontinue the sites or modify them in a way that makes it clear that the sites are advertising for Amerisleep.

i. *Roblox Corporation,* CARU Case No. 6446 (May 2023)

   i. Roblox came to CARU's attention through its routine monitoring activities, whereby CARU noticed that in certain shops within Roblox "experiences", including a Ralph Lauren store, there were no disclosures notifying users that the store was advertising. Given that most of Roblox's audience are children under 18, CARU flagged that when engaging in virtual spaces it is difficult for children to distinguish between advertising and non-advertising content.

   ii. CARU recommended that Roblox ensure that such advertisements are clearly and conspicuously identified as ads in language and/or audio that children can see, hear and easily understand as advertising. While CARU acknowledged that Roblox was not the advertiser when brands worked with developers to include these advertising messages, CARU believes that Roblox has an important role to play in assisting brands and developers with compliance. Despite the new Roblox standards which Roblox had published prior to the CARU violation, CARU will continue to monitor Roblox to ensure compliance with the CARU Advertising Guidelines. CARU also recommended that Roblox establish and implement a monitoring process to enforce its new Advertising Standards.

j. *Datarails, Inc.*, NAD Case No. 7359 (August 2024)

i. Cube Planning, Inc. (a Datarails competitor) challenged content on the Finance Weekly website recommending and ranking Datarails products, including a ranking listing Datarails' products as the number one financial planning and analysis software solution.

ii. Datarails advertises on the Finance Weekly website (and appears to be the only advertiser on the website). The NAD determined that this advertising relationship constitutes a material connection requiring disclosure when Datarails is included in Finance Weekly rankings, endorsements, and reviews. In addition to including disclosure of this material connection, the NAD recommended that Datarails discontinue expert endorsements that do not come from experts who review and rate products using their expertise.

k. *See*, *e.g.*, Native Advertising: A Guide for Business available at: https://www.ftc.gov/business-guidance/resources/native-advertising-guide-businesses.

Enforcement Actions Involving Different Types of Claims

a. Deceptive and influencer endorsements and consumer review practices:

i. In October 2024, the FTC's new rule banning rake reviews and testimonials took effect (16 C.F.R § 465). This new rule aims to protect consumers from fake reviews that unfairly inhibit honest competition and trick consumers into wasting time and money. Under the rule, the following is prohibited: (i) the creation, sale, purchase, and/or distribution of fake or false consumer reviews, consumer testimonials, and celebrity testimonials (including AI generated fake reviews); (ii) the provision of compensation or other incentives conditioned on the writing of reviews expressing a particular sentiment – positive or negative (e.g. paying consumers to write a positive review), (iii) company insider reviews and testimonials that do not clearly and conspicuously disclose the insider's material connection to the company (i.e. as an officer, manager, employee, or agent of the company, or immediate relative of such parties), (iv) misrepresentation by a company that a company-controlled review website or entity is providing independent reviews or opinions about a category of products/services that includes the company's own products and services; (v) the suppression of reviews, including by threat or the screening of negative reviews; and (vi) knowingly (knew or should have known) buying or selling fake indicators of social media influence (e.g. followers or views generated by bots).

ii. In November 2023, the FTC's first high-profile enforcement efforts of the new Endorsement Guides were warning letters targeted at the American Beverage Association and the Canadian Sugar Institute, and several influencers they had engaged who did not clearly disclose their connection to these organizations.

iii. In July 2023, the FTC published highly anticipated updates to the Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255 (July 26, 2023) ("Endorsement Guides"). The Endorsement Guides' scope has been further expanded to cover endorsements made by virtual or fabricated endorsers (such as bots), the writers of fake reviews, and non-existent entities that purport to give endorsements. The current Endorsement Guides stipulate that it would be a deceptive practice for a social media account to use fake indicators to misrepresent his or her influence to the public for a commercial purpose by, for example, purchasing fake online followers. An effective disclosure in the revised Endorsement Guides would be one that is "understood or expected by all but an insignificant portion of the audience."

iv. In October 2021, the FTC issued Notices of Penalty Offenses to 700 companies for misleading endorsements. The FTC cited unlawful practices including failure to identify that an endorser is sponsored by the brand, continuing to use an endorsement without good reason to believe that the endorser still subscribes to the opinions presented, and misrepresenting the experience of the endorser as that of an average consumer. While receiving a Notice of Penalty Offense does not indicate fault on the part of a company, it does put the recipient on notice of actual knowledge of the FTC regulations governing endorsements and testimonials and entitles the FTC to seek civil penalties in the event of a subsequent violation.

v. *Fashion Nova*, FTC File No. 192 3138 (January 25, 2022) — In its first action involving suppressed consumer reviews, the FTC entered a $4.2 million settlement against the online clothing retailer Fashion Nova based on claims that Fashion Nova used a third-party online product review management interface to automatically post all four- and five-star reviews to Fashion Nova's website, while putting all reviews with less than four stars on hold, pending Fashion Nova's approval, which never materialized. As part of the settlement, Fashion Nova is obligated to post on its website all consumer reviews of products that are currently being sold and are relevant, verified and do not contain offensive content.

vi. *Smile Direct Club LLC* (January 2022) — In early 2022, the NAD published its findings following investigation of Best Company, a platform that

aggregated, analyzed and verified consumer reviews of aligner vendors, including Smile Direct Club LLC (Smile Direct). The NAD found that while Smile Direct could claim, generally, that its Best Company-collected reviews were "moderated through a tech-enabled, proprietary, seven-point moderation process to ensure they are real and authentic," Best Company could only claim that a review was 100% verified if the review was submitted by a *bona fide* customer of the aligner company.

vii. *Roomster Corp.*, 654 F. Supp. 3d 244 (S.D.N.Y. 2023) — The FTC joined six states in a lawsuit against Roomster, a rental listing platform alleged to have fabricated reviews and listings, and its owners John Schriber and Roman Zaks. The plaintiffs simultaneously entered a proposed order requiring Jonathan Martinez, who allegedly sold Roomster the fake reviews, to pay an $100,000 fine and to cooperate in the FTC's case against Roomster.

viii. *Travelers United v. Cassandra De Pecol and Expedition 196, LLC*, No. 2022-CA-003089-B (D.C. Super Ct. Jan. 16, 2024) — Citing FTC inaction, the non-profit Travelers United sued Cassandra De Pecol under DC's Consumer Protection Procedure Act, alleging that the influencer commercially leveraged the false claim that she was the first woman to travel the world. The Complaint further alleged that Ms. De Pecol invented sponsors and failed to disclose paid promotional posts on her social media platform, charging as much as $4,500 per post. As part of its suit, Travelers United demanded Ms. De Pecol correct 325 Instagram posts and seven TikToks it believed are in violation of the FTC's guidance on social media influencing and that Ms. De Pecol remove any reference of her being the first woman to travel to every country on all her social media channels.

ix. *Google LLC and iHeart Media, Inc.,* FTC File No. 2023092 (November 2022) – The FTC along with state attorneys general brought lawsuits against Google and iHeart Media for airing nearly 29,000 endorsements whereby radio personalities promoted their use of and experience with Google's Pixel 4 phone in 2019 and 2020 when these individuals had never been provided with or used the product before recording and airing a majority of the advertisements. The final orders prohibit Google and iHeart from making similar misrepresentations with separate state judgments requiring them to pay a total of $9.4 million in penalties.

x. Lindsay Lohan, Jake Paul, Austin Mahone and other celebrities (March 2023) –

    1. Pursuant to violations of the Endorsement Guides and Section 17(b) of the Securities Act, the SEC charged eight celebrities, including Lindsay

Lohan, Jake Paul and Austin Mahone, with failing to disclose their commercial relationships with Justin Sun's crypto companies: Tron Foundation Limited, BitTorrent Foundation Ltd. and Rainberry, Inc. In an effort to combat rumors that Sun engaged celebrities to post about the tokens, Sun posted, "There have been rumors lately of third-party celebrities being paid to promote #TRON. #TRON Foundation is not involved in these activities. Nor is the foundation aware of the actors behind this." and "[I]f any celebrities are paid to promote TRON, we require them to disclose." when in fact an employee was tasked with ensuring that no celebrity made disclosures.

2. The settlements, reached with most of the celebrities charged, include disgorgement of the fees they were paid, as well as prejudgment interest and civil penalties totaling more than $400,000, including $40,670 from Lohan and $101,587 from Paul. In addition, the celebrities must forgo receiving or agreeing to receive any form of compensation or consideration from any issuer, underwriter or dealer for publishing, giving publicity to, circulating any notice, circular advertisement, newspaper, article, letter, investment service, or communication, which though not purporting to offer a crypto asset security for sale, describes such crypto security asset, for three years from the date of their respective orders.

xi. *The Bountiful Company*, FTC File No. 2223019 (April 2023) – In a first of its kind action for "review hijacking", the FTC alleged that The Bountiful Company used an Amazon tool to create "variation" relationships between products sold on Amazon.com that are substantially similar to the brand's products. Products with a variation relationship are featured on the same product detail page and display the total number of ratings and reviews and the average star rating of all the products in the variation relationship, as well as any "#1 Best Seller" or "Amazon's Choice" badges. According to the FTC, "variating new products with 'top sellers' allowed new products to essentially 'borrow' the best-selling flags, ratings, reviews and first page placement." As such, this allowed the company to manipulate Amazon.com product pages to misrepresent the reviews, the number of Amazon reviews and the average star ratings of some products, as well as to make it falsely appear that some were number-one best sellers or had earned an Amazon Choice badge. The Bountiful Company was ordered to pay $600,000 in fines.

b. Natural claims:

i. There has been continued focus on challenges to "natural", "naturally derived" and "natural origin" claims in the food, beverage, household products, and cosmetics industries.

1. Certain challenges have alleged that unqualified "natural" claims – including in brand names – imply that the product does not contain any synthetic or highly processed ingredients.

a. *Whiteside v. Kimberly-Clark Corp*., 108 F.4th 771 (9th Cir. 2024) concerned wipes advertised as "natural care" and "plant-based wipes," along with nature-themed imagery. The Ninth Circuit determined that a reasonable consumer could interpret these claims as representing that the products do not contain synthetic ingredients.

b. *Orrico v. Nordic Naturals, Inc*., No. 1:22-CV-03195 (E.D.N.Y. Sept. 28, 2023) concerns class action allegations that Nordic Naturals falsely marketed its range of health food and supplement products as "natural," despite the fact that such products contained non-natural, synthetic ingredients. The court denied motion to dismiss this case, finding that a prominent representation of "Naturals" on the label could plausibly deceive consumers.

c. *Luib v. Henkel Consumer Goods Inc.*, No. 1:17-CV-03021 (E.D.N.Y. 2019) settled for $1,500,000 and concerned allegations that Purex laundry products labeled "Natural Elements" misled consumers to expect that the products were all natural when in fact they contained synthetic ingredients.

d. *Langan v. Johnson & Johnson Consumer Companies, Inc.,* No. 13-CV-01471 (D. Conn. Feb. 4, 2019) settled or $2,400,000 (Complaint alleged false labeling of Aveeno Baby Wash and Shampoo and Baby Calming Comfort Bath, claiming that "Natural Oat Formula" was false and misleading given the inclusion of synthetic ingredients in the products.).

e. *Klar et al. v. Sendayco, LLC d/b/a Pure Body Naturals*, 23-CV-823 (E.D.N.Y. Feb. 3, 2023) concerns allegations that Pure Body Naturals products, including shampoos, body washes, and serums are falsely advertised since its marketing and advertising campaign claims that the products are "Pure", "100% Natural" or

"100% Pure" but the products contain various synthetic ingredients including citric acid and xanthan gum.

c. Health & Dietary Supplements

i. The FTC and Food and Drug Administration ("FDA") – independently and jointly - issue warning letters alleging that advertising for health-related products may violate the FTC Act and/or the FDA Act.

1. In August 2022, the FDA sent a warning letter to Amazon for distributing unapproved new drug products of third parties ("Deisana Skin Tag Remover, Mole Remover and Repair Gel Set" and "Skincell Mole Skin Tag Corrector Serum"). This means that the FDA may take action against a brand for selling an unapproved new drug, and against a retailer for distributing such. This also indicates that FDA is more likely to take action when it has safety concerns about drugs marketed over-the-counter directly to consumers for advertised uses—FDA cited such concerns in its warning letter regarding mole or skin tag removal (as these may be cancerous or precancerous, and FDA has issued a consumer warning noting that products marketed for removing moles and other skin lesions can cause injuries and scarring).

2. In June 2023, the FTC and FDA sent out joint warning letters to Delta Munchies LLC, Exclusive Hemp Farms, Etienne-Dubois, LLC/Oshipt, North Carolina Hemp Exchange, LLC (d/b/a NC Hemp Shoppe), Dr. Smoke, LLC (a/k/a Dr.S, LLC), Nikte's Wholesale, LLC, and The Haunted Vapor Room for selling edible products containing Delta-8 THC in packaging that was nearly identical to snacks and candies that children eat, including, Doritos, Cheetos and Nerds. According to the letters, after reviewing the online marketing for the Delta-8 THC products sold by these companies, the FTC found that the advertising may violate Section 5 of the FTC Act by utilizing unfair or deceptive acts, including practices that present unwarranted health or safety risks. One of the FTC's priorities is preventing risk to children and the FTC expressed that imitating non-THC containing food products that children consumer is misleading. In July 2023 cease and desist letters were issued to the foregoing companies.

3. In November 2023, the FTC sent warning letters to two trade associations and 12 registered dieticians and other online health influencers warning them about the lack of adequate disclosures in their Instagram and TikTok posts promoting the safety of the artificial

sweetener aspartame or the consumption of sugar-containing products.

4. In July 2024, the FTC and FDA sent out joint warning letters to several companies currently marketing edibles containing Delta-8 tetrahydrocannabinol (THC) in packaging deceptively similar to many foods children eat such as Froot Loops and Chips Ahoy! chocolate chip cookies.

ii. Beyond warning letters, the FTC has taken action against companies falsely or deceptively advertising health-related products, or for making unsubstantiated health-related claims.

1. *doTERRA International, LLC*, No. 2:23-CV-00063 (2023) — The FTC brought suits against three current and former high-level distributors (a/k/a "Wellness Advocates") of doTERRA International, LLC pursuant to the COVID-19 Consumer Protection Act for making claims that the company's essential oils and dietary supplements could treat, prevent or cure COVID-19. In court orders agreed upon by the defendants, they will cease making unfounded COVID-19 claims, have reliable human clinical testing to supports claim, require scientific proof for any health claims they make, prohibit misrepresentation that a product's benefits are scientifically or clinically prevent and pay a $15,000 civil penalty.

2. *Dalal A. Akoury d/b/a AWAREmed, et al., U.S.*, FTC File No. 2123039 (2023) — In March 2023, the FTC took action against Dr. Dalal A. Akoury and companies under her control operated as the medical clinic, AWAREmed Health & Wellness Resource Center, for making false and unsupported claims for additional services, cancer treatment services, and treatment of other conditions, under the Opioid Additional Recovery Fraud Prevention Act. The proposed order bars the doctor and the clinic from making unsupported claims and required payment of a $100,000 civil penalty.

d. Education

i. *Grand Canyon Education, Inc.; Grand Canyon University; and Brian E. Mueller*, No. CV-23-02711-PHX-JZB (D. Ariz. Dec. 27, 2023) -- In December 2023, the FTC alleged that Grand Canyon Education, Inc. ("GCE"), Grand Canyon University ("GCU"), and Brian E. Mueller as President of GCU and CEO, Chairman of the Board, and a director of GCE, deceptively advertised GCU as a nonprofit to prospective students as well as an "accelerated" doctoral program that in actuality required thousands of dollars' worth of

"continuation courses". The FTC's complaint also alleges that the defendants, sent millions of abusive marketing calls to consumers to individuals who specifically requested not to be solicited as well as individuals on the National Do Not Call Registry.

ii. *Sollers Educations, LLC*, FTC File No. 2123142 (2023) – The FTC alleged that the defendants used false or unsubstantiated representations, including representations touting the school's relationship with prominent employers, to convince consumers to enroll at Sollers College. The defendant's encouraged students to pay for schooling using income share agreements which are unlawful due to their failure to include legally mandated disclosures. Sollers College and its parent company were ordered to cancel $3.4 million in student debt.

iii. *Intercontinental Solutions LLC, et. Al*, No. 8:23-CV-01495- SB-JDEx (D.D.C. Aug. 14, 2023) — According to the FTC's complaint, Express Enrollment LLC (also doing business as SLFD Processing) and Intercontinental Solutions LLC (also doing business as Apex Doc Processing LLC) targeted students seeking debt relief and collected $8.8 million in advance fees in exchange for non-existent student loan debt relief services. The companies promised to lower or eliminate the students' loan payments, pretended to be affiliated with the U.S Department of Education and convinced students to stop corresponding with their loan providers. Further in violation of the Telemarketing Sales Rule, the complaint alleges that the defendants used misrepresentation to obtain bank account, debit card, and credit card information. In 2024, settlements were reached where parties were permanently banned from the debt relief industry and required to turn over certain assets to the FTC.

iv. For Profit Schools (October 2021) — The FTC issued Notices of Penalty Offenses to 70 different for-profit higher education institutions for false claims regarding employment and earning potential of graduates. The Notices target claims made by institutions (i) about the career outcomes of their graduates, including whether a particular career field is in demand, (ii) the percentage of graduates who get jobs in their chosen field, (iii) whether the institution can help a graduate get a job, (iv) the amount of money a graduate can expect to earn after graduating. As a result of the FTC's actions, the U.S. Department of Education will forgive $71.7 million dollars in student loans held by students of DeVry University who may have been deceived by the University's allegedly inaccurate false employment statistics.

v. *American Financial Support Services, Inc., et. al.*, No. 8:19-CV-02109-JWH-ADSx (September 2020) — The FTC settled a case in September 2020 against the operators of a student loan debt relief scheme, who owe at least $835,000 in order to settle allegations that they charged illegal upfront fees and made false promises to consumers struggling with student loan debt. The FTC alleged that the defendants pretended to be affiliated with the Department of Education and deceptively promised loan forgiveness, consolidation, and repayment programs to reduce or eliminate monthly payments and principal balances. The order bans the settling defendants from providing student loan debt relief services, prohibits them from violating the Telemarketing Sales Rule, and includes a monetary judgment of $43.3 million, which is partially suspended due to an inability to pay. The defendants will be required to surrender at least $835,000 and additional assets, which will be used for consumer redress. The order also requires the defendants' full cooperation in this ongoing case and any related investigation.

vi. *Age of Learning,* FTC File No. 172 3186 (September 2020) — The FTC settled charges against online children's education company Age of Learning, Inc., which operates a childhood learning program called ABCmouse. Age of Learning will pay $10 million and change its negative option marketing and billing practices to settle Federal Trade Commission charges that it made misrepresentations about cancellations and failed to disclose important information to consumers, leading tens of thousands of people to be renewed and charged for memberships without proper consent.

e. Environmental/"Clean" Claims

i. The FTC is in the process of reviewing and potentially revising the Green Guides based on increasing consumer focus on buying environmentally friendly products. In a request for public comments, the FTC indicated that it may focus on issues including carbon offsets and climate change and the terms "recyclable" and "recycled content." In May 2023, the FTC hosted a public workshop to examine "recyclable" environmental marketing claims.

ii. In May 2022, the FTC reached a combined $5.5 million settlement with Kohl's and Walmart for allegedly making misleading representations that textile products were made of bamboo fabric and provided environmental benefits because those products were derived from bamboo. The FTC asserted that the products were, in fact, made of rayon (derived from bamboo), using a chemical process that is harmful to the environment.

iii. *Duchimaza v. Niagara Bottling, LLC*, No. 21 Civ. 6434 (EAM) (S.D.N.Y. 2022) — a New York court dismissed a class action alleging that Niagara's claim that its Kirkland water bottles are 100% recyclable is false and misleading under New York's General Business Law because the caps and labels on the bottle are not recyclable, and because New York's low recycling capacity effectively renders the other components unrecyclable as well. The Court cited the FTC's Green Guides in dismissing the case, finding that the caps and labels were "minor incidental components" and that plaintiff had failed to plead that recycling was actually unavailable to her community (even if its capacity was limited).

iv. *American Beverage Association*, NAD Case No. 7011 (November 2022) — As part of its Every Bottle Back Initiative, American Beverage Association made claims about their recycling practices and their commitment to the environment. NAD found that the claim, "They're collected and separated from other plastics so they can be turned back into material that we use to make new bottles" expressly refers to the fact the bottles are recycled when in actuality they are not. In addition, with respect to the claim, "That completes the circle and reduces plastic waste," NAD determined that the reference to completing the circle refers to the recycling process in part refers to the use of recycled material that "reduces plastic waste." but the supporting evidence is not clear about a meaningful reduction in plastic waste. In each case NAD recommended that the claims be modified.

v. *JBS USA Holdings, Inc.*, NAD Case No. 7135 (June 2023) — The Institute for Agriculture and Trade Policy challenged JBS' claims that it would achieve "net zero" emissions by 2040 including "JBS is committing to be net zero by 2040" and "bacon, chicken wings, and steak with net zero emissions. It's possible". NAD determined that the "net zero" claims create consumer expectations of a measurable outcome. Although JBS provided evidence of significant preliminary investment towards their 2040 goal, the record did not convey that they were implementing a plan at present to achieve their future goals. As a result, the NAD recommended that they discontinue each of the challenged "net zero" claims. Aspirational environmental benefit claims create reasonable expectations for consumers and therefore require substantiation. This case was appealed to NARB, and the decision was upheld.

    1. In February 2024, the New York Attorney General filed a lawsuit against JBS for these same claims. Specifically, the case alleges that JBS has misleadingly claimed that it will achieve net zero greenhouse gas emissions by 2040, despite documented plans to increase production and therefore increase its carbon footprint.

f. Auto-Financing Offers & Vehicle-Related Claims

i. In December 2023, the FTC announced 2023 the Combating Auto Retail Scams Rule (CARS Rule). The rule, which applies to "Covered Motor Vehicle Dealers" focuses on increased clarity for add-on terms (such as costs, limitations and benefits), prohibited misrepresentations and recordkeeping. While the CARS Rule was supposed to go into effect on July 30, 2024, the FTC issued an order postponing the effective date after the National Automobile Dealers Association and the Texas Automobile Dealers Association filed a petition for review challenging the rule as "arbitrary, capricious, an abuse of discretion, without observance of procedure required by law, or otherwise not in accordance with law."

ii. *Asbury Automotive Group, Inc., et al,* FTC File. No 222 3135 (2024) – In an administrative complaint, the FTC alleged that three Texas dealerships engaged in a variety of deceptive practices, including "payment packing", to charge consumers for unwanted add-ons. The complaint also alleged that the dealerships discriminate against Black and Latino consumers by targeting them with unwanted and higher-priced add-ons.

iii. *Napleton*, No. 1:22-CV-01690 (Mar. 21, 2022) — In 2022, the FTC and the State of Illinois took action against Napleton, a multistate auto dealer group based in Illinois, for sneaking illegal junk fees and "add-ons" to customer's bills and discriminating Black consumer by charging them a higher price for financing. The FTC settled the lawsuit for $10 million in a record-setting monetary judgment for an FTC auto lending case.

iv. *Passport Automotive Group Inc,* FTC File No. 2023199 (2022) — The FTC sent more than $3.3 million to customers of Passport Auto after charging the dealer with adding hundreds, if not thousands, of dollars in illegal junk fees to car prices and discriminating against Black and Latino consumers by charging them higher fees and financing costs.

v. *Romoff v. Gen. Motors LLC*, 574 F. Supp. 3d 782 (S.D. Cal. 2021) — In a class action complaint, plaintiffs alleged that General Motors violated California and New Jersey law by including a "destination charge" in the listed sticker price of its vehicles that did not reflect the actual cost incurred by General Motors of delivering vehicles to dealerships and did not disclose that General Motors received a profit. The court granted General Motors motion to dismiss, which was affirmed in 2023, based on the premise that a reasonable or average consumer would not expect the destination charge to exclude profit. General Motor's omission of additional information regarding the destination charge was not deemed material.

vi. *Tate's Auto Center of Winslow, Inc.*, FTC File No. 162 3207 (2021) — A group of auto dealerships in Arizona and New Mexico must cease business operations as part of an August 2020 court-approved settlement resolving FTC charges that the dealerships deceived consumers and falsified information on vehicle financing applications. In a case filed in 2018, the FTC alleged that Tate's Auto Center of Winslow, Inc.; Tate's Automotive, Inc.; Tate Ford-Lincoln-Mercury, Inc. (doing business as Tate's Auto Center); Tate's Auto Center of Gallup, Inc.; and Richard Berry, an officer of the dealerships, falsified consumers' income and down payment information on vehicle financing applications and misrepresented important financial terms in vehicle advertisements. Berry's settlement resulted in a $450,000 payment to the FTC as well as a stipulated dismissal of relief for relief defendant Linda Tate. The settlement against the remaining defendants included a monetary judgment of $7,203,227 against the defendants.

vii. *Uber Technologies*, FTC File No. 152 3082 (2018) — Uber settled charges brought by the FTC that its advertising on its website intended to attract new Uber drivers was deceptive. Uber advertised a "Vehicle Solutions Program" that would provide financing for new Uber drivers to purchase or lease a car. According to the FTC, Uber exaggerated how much income drivers could make, for instance stating that the median annual income in New York City was more than $90,000, when in fact it was $61,000. Uber settled the lawsuit for $20 million.

g. Made in the USA / Production Claims

i. In 2021 the FTC formalized its prior guidance on Made in the USA claims. The FTC's Rule prohibits unqualified Made in the USA claims unless: 1) final assembly or processing of the product occurs in the United States; 2) all significant processing that goes into the product occurs in the United States; and 3) all or virtually all ingredients or components of the product are made and sourced in the United States. The rule also makes civil penalties available to the FTC.

ii. Since 2022, the FTC brought several enforcement actions against companies for allegedly making false, misleading, or unsupported Made in the USA claims, in violation of the Made in USA Labeling Rule, including:

1. *ElectroWarmth Products, LLC*, FTC File No. 222 3096 (Aug. 30, 2022) — FTC action against electric blanket company and its founder alleging that its bunk warmer product that ElectroWarmth marketed as "Made in the USA" was actually wholly imported from China. The company

was required to pay $815,809 and send letters to consumers correcting the false claim.

2. *Lions Not Sheep*, FTC File No. 222 3023 (July 28, 2022) — The company allegedly added false Made in USA labels to clothing and accessories imported from China and other countries. The company was required to stop making these claims and was required to pay a judgment of $211,335.

3. *US v. Lithionics Battery, LLC*, FTC File No. 2123141 (May 2, 2022) — The company allegedly falsely labeled its battery products with an American flag image surrounded by the words "Made in U.S.A.," often accompanied by the statement "Proudly Designed and Built in USA," when these products are primarily made overseas. The company had to stop making these claims and pay civil penalties of over $100,000 (equal to three times Lithionics' profits attributable to the illegal activity).

4. *Instant Brands, LLC*, FTC File No. 2223140 (Jan 18, 2023) – The FTC brought an action against Instant Brands, the manufacturer of Pyrex-brand kitchen and home products, for falsely claiming that its measuring cups were made in the United States during a period of time when they were imported from China. The FTC sent more than $88,000 in refunds to consumers.

5. *Chaucer/Bates Accessories*, FTC File No. 222 3163 (Aug. 29, 2023) – In August 2023, the FTC took action against Massachusetts and New Hampshire based clothing companies and their owner for falsely claiming that certain products were manufactured in the United States. The respondents are required to pay $191,481 and are prohibited from making misrepresentations, misleading or unsubstantiated representations regarding U.S origin claims.

iii. *Nectar Brand LLC*, FTC File No. 182 3038 (2021) — The FTC reached a $753,000 settlement with Resident Home LLC, the parent company of Nectar Brand LLC d/b/a Nectar Sleep, and owner Ran Reske. The settlement covers both 2018 false claims by Nectar Sleep alleging that the DreamCloud mattress was manufactured in the USA and 2020 false claims that the same mattress is made of 100% USA-made materials. The FTC's order prohibits Reske and his companies from making unqualified US-origin claims unless the relevant item is substantially transformed in the US and principally and substantially assembled in the US. Qualified US-origin claims will require a clear disclosure stating the extent to which the item contains foreign parts, ingredients, components, or processing.

iv. *US v. Williams Sonoma*, No. 3:24-CV-2396 (March 30, 2020) — The FTC reached a $1,000,000 settlement with Williams Sonoma, over false "Made in the USA" claims. After a similar case was resolved in 2018 when Williams Sonoma described it as an "isolated incident," the FTC encountered several Williams Sonoma products that were labeled as "Made in the USA," even though the products were either manufactured outside of the USA or were comprised of significant foreign materials. In addition to the monetary settlement, Williams Sonoma is prohibited from making any unqualified "Made in the USA" claims with respect to the products at issue, and is required to prominently disclose the extent to which its products contain foreign parts or inputs when making qualified "Made in the USA" claims. As a result of violating the 2020 FTC order, Williams Sonoma is required to pay a record civil penalty of $3.175 million.

v. California Senate Bill 633 (2020) — CA law had previously required 100% American production, for products making the claim, but that was a rarity among state laws. This legislation brings CA into line with the rest of the country as well as with federal regulations more relaxed standards for products carrying the "Made in America" or "Made in USA" labels. This also aligns the state with the Federal Trade Commission standard that "all, or virtually all" of a product must be made in the country for a "Made in" label to be lawfully used.

h. Pricing and "Free"

i. *Jacobo v. Ross Stores, Inc.* (C.D. Cal 2016) — In 2019, Ross Stores settled a class action complaint for $4.8 million over deceptive reference pricing allegations. In 2015, a class complaint was filed against Ross Stores, alleging that Ross Stores' advertised "compare at" prices constituted "former prices," but because they did not represent the prevailing market prices for those goods within the three months immediately preceding the publication of the advertisement, they violated Cal. Bus. Prof Code section 17501 (in addition to the California Consumer Legal Remedies Act and California Unfair Competition Law).

ii. *AAFE Products/BNRI Corporation,* FTC File No. 152 3129 (2020) — FTC action pursuant to the FTC Act and Section 5 of the Restore Online Shoppers' Confidence Act ("ROSCA"), pursuant to which the FTC alleged that the defendants, a group of online marketers, offered "free" products, without clearly disclosing that by accepting the "free" product consumers were agreeing to be charged each month for a subscription if they did not cancel. The marketers also allegedly misrepresented their return, refund and cancellation policies. Under the settlement, the defendants were

prohibited from misrepresenting the cost of any good or service, that consumers will not be charged, that consumers can get something for a processing or shipping fee with no further obligation, and that a product or service is free. The orders also required the defendants to clearly disclose important details about any online negative option plan where consumers enter billing information, to get consumers' informed consent before charging them, and to offer a simple way for consumers to cancel recurring charges. In order to secure the $2+ million orders against the individual defendants, they were required to grant the FTC a security interest in real estate and other assets.

iii. *Kahn v. Walmart, Inc.*, 22 C 4177 (N.D. Ill. Mar. 21, 2023)– A Walmart shopper alleged that Walmart is engaging in deceptive pricing since shelf prices do not always reflect the price charged at point of sale. While the lower court granted Walmart's motion to dismiss, the federal appeals court is allowing the potential class action to proceed.

iv. *StubHub* (2024) – The District of Columbia Attorney General filed a lawsuit against StubHub alleging that the online ticket platform used dark patterns to mislead consumers about ticket prices in an effort to charge "junk fees".

E. Social and Digital Media

Intellectual Property Overview

Every marketer and agency developing a campaign must take into account the various intellectual property rights associated with advertising, media, and marketing. In particular, experiential campaigns and efforts to interact with consumers in real-time on social media can expose brands and advertisers to various risks. These include the risk of infringing upon third-party copyrights, trademarks, and rights of publicity when advertisers rush to post branded content without proper vetting. This risk has received even greater national attention due to the increasingly popular use of generative artificial intelligence (AI) tools to create new content, following the public release of ChatGPT in November 2022 and subsequent newer (and more powerful) models from both OpenAI and its competitors. Taking the time to carefully review and consider the IP rights incorporated into a social media post—as well as any public image implications that could arise based on the nature of the content—can help brands avoid legal problems often caused by impulsive action.

One area where brands can encounter issues is by posting or using copyrighted content—original works of authorship fixed in a tangible medium of expression—without permission. This includes photographs, videos, music, text, graphic designs, and more. Even if all underlying elements of the materials are independently conceived,

consider whether such elements are substantially similar to or otherwise infringe upon existing third-party intellectual property or the sources used as "inspiration" for the creative execution. The fact that copyrighted content may be widely shared online or even used by other advertisers does not eliminate the need for vetting or clearance. Moreover, providing attribution or a media credit to the source of the work is not a defense to a copyright claim and does not preclude the need to obtain permission. Images publicly available or posted on the internet are not necessarily in the public domain, and nearly all photographs posted on websites such as Instagram, X (formerly Twitter), Facebook, and other platforms are protected under copyright law, as are videos posted on sites like YouTube. Similarly, content available on one social media platform may not be authorized for use on all platforms. For instance, TikTok has licensed specific usage rights for copyrighted audio content on its platform, such as the music in its sound libraries and the robo voice in its text-to-speech feature. These materials are allowed to be used only by users engaging or sharing them within the TikTok platform, and not elsewhere. Consequently, advertisers should comply with each platform's restrictions to reduce the risk of an infringement claim.

With the rise of AI and AI-generated content, copyright law has faced new challenges, including debates regarding ownership of AI-generated work and whether the use of copyrighted content to develop AI algorithms can be considered fair use. This surge in the generative AI space has included lawsuits, regulatory challenges, legislative efforts, and evolving technological capabilities, impacting how AI tools are used in the marketing and communications industry.

In addition to the elevated risks posed by AI, courts have held that in-line linking, or "embedding," without permission from the rights owner may constitute copyright infringement. For example, in 2021, a judge refused to dismiss a lawsuit against BuzzFeed for embedding photos of the protests following George Floyd's murder, taken by several photographers and posted on their Instagram accounts. The case was ultimately resolved by stipulated dismissal in the spring of 2022 when all six photographer-plaintiffs agreed to drop the suit. In *McGucken v. Newsweek LLC* (S.D.N.Y. March 21, 2022), the District Court for the Southern District of New York determined that simply displaying someone else's photograph on social media without permission—regardless of whether and where the original embedded image was hosted—is a clear infringement of the author's exclusive right to "display" their work under the Copyright Act. In a similar case, *Hunley et al v. Instagram LLC* (No. 22-15293), photographers challenged how easily Instagram allows third-party websites to embed photos from its platform in an effort to overturn the Ninth Circuit's longstanding reliance on the "server" test. In July 2023, the Ninth Circuit affirmed the dismissal of the lawsuit, upholding the "server test," which holds that a website that embeds content hosted on a third-party server does not "display" a copy of the work for purposes of direct copyright infringement. However, the legal landscape remains uncertain, and

advertisers should exercise caution when embedding content from social media platforms.

The Supreme Court recently revisited the concept of "fair use" in the case of Andy Warhol Foundation v. Goldsmith. The question before the Court was whether pop artist Andy Warhol made a sufficiently transformative use of copyrighted photographs of Prince, taken by photographer Lynn Goldsmith, when he altered and reproduced them as artwork to accompany a Vanity Fair piece about the musician. In May 2023, the Supreme Court held that Warhol's use was not protected by fair use. Justice Sotomayor, writing for the majority, stated that the purpose and character of the use—including whether such use is of a commercial nature—weighed against fair use because Warhol's work was used for the same commercial purpose as Goldsmith's original photograph. Agencies and artists should consider whether their works serve a different purpose from the original when deciding how to use pre-existing work as inspiration for new creations. This analysis is particularly relevant with the rise of AI-generated content and the potential for an AI-generated work to be substantially similar to an original work of which the agency may be unaware.

In other news, while currently eclipsed by the international interest in AI, the "metaverse" continues to be popular and brings with it a number of potential copyright and other intellectual property issues. Since the concept of the metaverse was widely introduced to the public in 2021, numerous advertisers, agencies, and celebrities have tried to establish a foothold in this digital space. Meta (formerly Facebook) has continued to push for widespread adoption of the metaverse in both gaming and professional industries. Both Meta and Apple have been creating products designed for augmented reality (AR) experiences in the metaverse. In June 2023, Apple unveiled its Vision Pro headset, signaling its entry into the AR/VR market.

Traditional forms of intellectual property protection, like copyrights and trademarks, exist in the metaverse just as they do in the physical world. New original works of authorship are created inside the metaverse, and use of those works by third parties requires traditional licensing and permissions—just as it would in the "real world." Advertisers and their agencies must clear all third-party elements featured in their branded spaces and ensure the licenses they obtain provide sufficient rights to adapt physical items (like a piece of artwork) into digital form.

As with the metaverse, the introduction of non-fungible tokens (NFTs) into popular culture has continued to impact the advertising world, although the NFT market has experienced fluctuations. According to recent statistics, NFT sales have decreased significantly since their peak in 2021. Nevertheless, NFTs remain a significant industry.

Legal challenges involving NFTs and intellectual property have emerged. For example, in June 2023, a federal jury in the Southern District of New York ruled in favor of Hermès International in a trademark infringement lawsuit against artist Mason

Rothschild over his "MetaBirkins" NFTs, which depicted digital images of Hermès Birkin bags covered in faux fur. The jury found that Rothschild's NFTs infringed Hermès' trademark rights and were not protected by the First Amendment. However, this case is still ongoing - on November 6, 2023, the artist appealed the case to the US Court of Appeals for the Second Circuit. This case underscores the importance of respecting trademark rights in the creation and sale of NFTs.

While NFTs are simply digital certificates stored on a blockchain (typically within a third-party blockchain marketplace), they often confer rights to their owners regarding an underlying artistic or digital work. The scope of rights conferred on NFT purchasers should be set forth in Terms of Use; otherwise, the rights transferred from NFT seller to purchaser will occupy a legal gray area.

From the advertiser's perspective, the creation and transfer of NFTs present a host of IP issues. The works underlying NFTs could be a gateway for copyright infringement claims. While some NFTs feature brand-new works created solely for selling or licensing with their corresponding NFT, many NFTs feature pre-existing works like movie clips or sports highlights. Advertisers “minting” (or creating) NFTs based on an existing license to use pre-existing content must ensure they have sufficient rights to reproduce, create derivative works of, distribute, and publicly display the underlying work in media known at the time of the license grant and new media created after that date.

Developments in technology are also making it easier for copyright owners to identify potential infringements, increasing the practical risk of an advertiser receiving a claim. Automated bots allow copyright owners to scour the web for unauthorized uses of their content and send cease-and-desist letters demanding costly settlements or threatening lawsuits. YouTube’s Content ID uses artificial intelligence to flag content to copyright owners, who can then decide whether to leave the content in place and receive advertising revenue, have their content removed from the video, or have the entire video taken down. However, this AI is not perfect and can lead to unfounded claims, so advertisers should review any Content ID matches, including takedowns, as penalties can include loss of an advertiser’s YouTube account.

Advertisers must also refrain from infringing upon third-party trademarks by showing other brand names or logos, particularly in a manner that suggests an association with the advertiser or depicts the brand in a bad light. In the context of social media, this often means ensuring that photos and video footage do not include any third-party brand names, logos, slogans, or other trademarks in the clothing, props, accessories, and locations shown in the content. This also applies to the text included in a social media caption. For example, while it is inadvisable for an advertiser to broadcast a live stream from a red-carpet event on social media without permission, even mentioning the name of the event in social media posts can be highly risky—think the Academy Awards, Grammy Awards, the Super Bowl, and the Olympic Games. Most brands active on social

media maintain trademark registrations for hashtags that incorporate their brand names or slogans, and courts have increasingly confirmed that these hashtags have protectable status as trademarks. They can be infringed when a competitor uses the same or a confusingly similar hashtag to market competing products. Brands should monitor and enforce their branded hashtags just as they would any other trademark in their portfolio and should be mindful to avoid unlawful infringement of third-party branded hashtags. This can extend to using a third party's brand name as a hashtag, whether or not the party has sought to register the mark with the hashtag symbol. While some courts have held that hashtags are merely functional tools, others have held that using a competitor's mark within a hashtag can imply a false endorsement or association and thus fall outside the fair use doctrine. Advertisers should review the language used within hashtags and other publicly facing tags on social media with the same level of scrutiny as they would any other prominent text or image in the advertisement.

Certain marquee events, such as the Oscars and the Olympics, have been issuing guidelines to advertisers in recent years, regulating hashtag uses. While it can be challenging to determine whether the use of a branded hashtag constitutes trademark infringement—as compared to a non-infringing way to participate in a categorized social media conversation about a particular topic—advertisers seeking to mitigate their risks should err on the side of caution. If a branded event provides a blanket rule or restriction on hashtag use, advertisers would be well-advised to obey it to avoid the risk of a lawsuit, given the severity of potential monetary relief. Such relief can include profits attributable to the infringement (where willfulness is not necessarily a prerequisite for recovery), actual damages, costs, and reasonable attorneys' fees. In the case of a counterfeit trademark, penalties can range from $1,000 to $200,000 per registered trademark infringed, and up to $2,000,000 per infringement if done willfully. Another significant remedy for trademark infringement is injunctive relief, which could shut down an advertiser's entire campaign if it included an unlicensed third-party trademark.

Additionally, it is becoming increasingly important for advertisers and agencies to consider the public relations impact of their campaigns, especially when they incorporate third-party intellectual property. In an increasingly polarized and culturally sensitive society, advertisers must avoid inadvertently sending an offensive or thoughtless message in their campaigns. In addition to clearing rights and permissions for existing intellectual property works in a campaign, additional clearance must be conducted to determine whether the content is likely to conflict with social norms and expectations to the detriment of the advertiser.

Right of Publicity

The right of publicity is a state-law based right that prevents the unauthorized commercial use of a person's name, likeness or persona, such as one's voice, signature, or similar identifying features. Rights that a person has to control the commercial use of their name, image and likeness are often referred to as "NIL" rights or simply rights of publicity. Photos, videos or other content including depictions of or otherwise identifying specific people should not be used in a commercial campaign, including on an advertiser's branded social media channels, without permission. This applies not only to the use of people's names, but also to their quotes and even identifying social media handles.

a. Case Study: Generative AI Meets Publicity Rights in Voice Dubbing Applications

Generative AI presents new opportunities for optimizing performer publicity rights in a cost- and time-efficient manner. Generative AI can be used to achieve an efficiency and scale of production that producers of yesteryear could only dream of (think: quickly dubbing a commercial into 20+ foreign languages using the exact same voice as the original presenter's). If a celebrity's schedule can't accommodate a reshoot, or a time-consuming voice-over session is out of budget, advertisers and content producers can -- with a performer's approval -- train an AI model using prior recordings as source material and generate a believable "sound-alike" speaking the desired text. That's a deal that James Earl Jones has worked out with Respeecher, a Ukraine-based AI company, along with The Walt Disney Co. and Lucasfilm Ltd., so Jones' voice can continue to be used in "Star Wars" films and TV shows for the character of Darth Vader even after Jones' retirement and recent death.

Respeecher, along with similar AI technologies, is also being leveraged to create more personalized ad campaigns for different locales in a chain of stores. Using generative AI, a celebrity endorser can be hired to record one ad and then have their voice be used in numerous variations of the ad, individualized for each store in the chain (in exchange for appropriate compensation for the extended usage rights and versions). Thanks to AI, it will appear to viewers as if the celeb himself recorded a new, particularized message each time. The same approach can be adopted for the use of iconic voices of performers who are no longer living (such as Chris Farley or Orson Welles) – whereby their estate would need to authorize the creation of a voice clone, which could then be used to create numerous variations of new commercial spots, in exchange for appropriate compensation to the estate.

In 2024, a number of new state laws were adopted to protect against the unauthorized misappropriation of performers' voices, as detailed further below, so it is important to ensure that any plans to take advantage of the technologies described above be assessed for legal compliance.

b. Celebrities and Deepfakes

While rights of publicity generally apply to all individuals, the risk of right of publicity claims is significantly increased with respect to celebrities and public figures. For example, if the use of a particular celebrity's name or image in a brand's social media posts is likely to lead consumers to believe that the celebrity has endorsed or is otherwise affiliated with the brand, the celebrity could claim that the brand/agency infringed her right of publicity and is additionally liable under a theory of false endorsement. Although A-list celebrities typically possess the most valuable NIL rights, they are not the only holders of such rights. Other folks, ranging from influencers and celebrities with more modest spheres of influence, to ordinary people, may also benefit from NIL rights, for example, if their image is used on social media to promote a product without their consent.

c. Student-Athletes

The newest category of celebrities with lucrative NIL rights is student-athletes, who are finally able to contract and profit from the use of their NIL rights, without risking their NCAA athletic eligibility. When working with student-athletes, advertisers must ensure they comply with applicable state law (typically where the athlete's school is located), college/university, and NCAA rules. For example, under Mississippi law, student-athletes are required to disclose potential deals to their schools prior to signing endorsement deals, and student-athletes cannot sponsor products in the tobacco, electronic nicotine products, marijuana, alcohol, performance enhancing supplements, gambling, sports betting, and adult entertainment categories. Importantly, across all state laws and NCAA policies, there is currently no limit on how much a student-athlete may be compensated, although legislation in several states permits schools to set regulations to ensure no recruiting violations are taking place, and the NCAA will continue to monitor and challenge "pay-for-play" transactions that are not based on the fair market value of the student-athlete's NIL rights. These changes are introducing sweeping changes for the sports media and marketing landscapes, as advertisers rush to capitalize on players' popularity and recognition.

d. Live-Streaming Considerations

Real-time marketing also has the potential to give rise to right of publicity claims. As the popularity of livestreaming apps continues to grow, advertisers face bigger risks, because it can be difficult to avoid accidentally capturing an individual on camera who may object to being broadcast live. It has become important to exercise caution while filming at high profile places and events like the red carpet or sporting events, to make sure that celebrity images are not caught on camera.

e. Post-Mortem Rights

In many states, the right of publicity lasts after death, allowing the estate or heirs of a deceased person to bring claims for the unauthorized use of the decedent's name or likeness in advertising. Take, for example, Florida. The state allows the successor-in-interest of any individual, and if no successor was named, then the decedent's surviving spouse and children, to maintain the decedent's right of publicity or file a registration to enforce their right of publicity rights under the law for up to 40 years. Any person, firm, or corporation may be authorized in writing to license the commercial use of an individual's name or likeness. Performers and their lawyers should pay careful attention to publicity rights in the context of estate planning, and in view of emerging AI technologies, give specific consideration to whether to permit others to simulate their voice and performances after their death, a potentially lucrative revenue stream for a celebrity's heirs.

User-Generated Content

Social media sites are built upon the foundation of user-generated content (UGC). With platforms such as TikTok offering features that encourage the modification and re-sharing of UGC, such as "dueting" and "stitching," UGC has become more important than ever. Generally speaking, while users retain ownership rights to their content posted on social media platforms, they grant the platform and oftentimes other users (but not advertisers) a non-exclusive, royalty-free, transferable, sub-licensable, worldwide license to use, store, display, reproduce, modify, create derivate works, perform and distribute content. Brands understand the value of user-generated content in their advertising and increasingly find ways to incorporate users' photos and videos in their social media ads.

The use of UGC may expose advertisers to not only FTC sanctions but also to liability for trademark infringement, copyright infringement, right of publicity, and false endorsement claims. Advertisers should also remain wary of potential secondary liability for UGC that violates another party's trademark or copyright. These issues tend to arise in scenarios where users can create characters or content that is owned by one party (e.g., a copyrighted superhero figure as an avatar) and are using that third-party IP in connection with another party's channel or platform (e.g., in a video game). In the advertising context, advertisers should consider whether their branded channels or content could enable users to use third-party IP to create infringing content.

Several states such as New York, Massachusetts, Rhode Island and Illinois require written consent to use a person's name, image or likeness. Trademark and copyright laws prohibit brands from using UGC without permission. Rights clearance is also required by the terms of use of nearly all social media sites. However, with the growth of direct consumer interaction and real-time marketing on social media, formal consent procedures have given way to more convenient means such as "hashtag consent". The

following guidelines, although not legally verified, reflect some of the best practices with respect to such newer forms of consent:

a. Advertisers must get more than just #consent from users. It is recommended that advertisers request users to provide a unique hashtag to express their consent to have their content used by the advertiser. For example, PetSmart asks users to respond with #YesPetSmart, rather than simply "#yes" or "#consent."

b. Advertisers must comment on user's post to request permission.

c. Advertisers should disclose intended use in a call to action.

d. Advertisers must make "clear and conspicuous" disclosures on the UGC, and they cannot be buried in captions or at the end of a long post. Rather, advertisers should include disclosures early on in the caption or text overlay.

e. If there is a material connection between a brand and the user who created the UGC (e.g., free products, paid partnership, or any form of compensation), advertisers must clearly disclose it.

f. Advertisers should include a link to the terms and conditions of the applicable promotion (if any).

g. Finally, in the case of a minor, advertisers must always obtain consent from the minor's parents. While obtaining such consent does not avoid the need for written permission from the user in all instances, like using UGC in a national, multimedia advertising campaign, it helps mitigate risks to businesses seeking to use UGC outside the platform.

When brands simply encourage consumers to tag their social media photos with branded hashtags, this is not sufficient for brands to ensure that can lawfully use those consumer images in their advertising. There could be many circumstances in which users post a photo using a designated hashtag without being aware that it could submit them to the advertiser's campaign; and conversely, users could use such a hashtag ironically, without seriously intending to submit their photos to the campaign. For this reason, the best practice is for advertisers to affirmatively reach out to users to obtain their specific, written consent to use specific user-generated content in advertising.

Experiential Marketing

2024 has seen a large resurgence of experiential marketing, as both consumers and brands have rediscovered the allure of experiential marketing in a manner not witnessed since prior to 2020. While some advertisers are relying on time-tested activation ideas, like short-term pop-ups and selfie stations, there has been a palpable shift in focus towards technological advancements, with brands enthusiastically embracing generative AI and VR/AR as a pivotal element in their experiential activations.

As advertisers seek to innovate and captivate audiences in a rapidly evolving landscape, brands have begun to integrate VR into their activations. Adidas recently rolled out TERREX, a new line of outdoor gear, and gave customers VR headsets that allows them to climb a difficult rock-climbing route in Corsica. Consumers were able to experience virtually climbing the "Delicatessen" summit, learn best practices in rock climbing, enjoy the virtual outdoor scenery, and show the purpose of TERREX gear in extreme outdoor events. Similarly, Volvo recently created an activation, using VR goggles to let consumers drive their new XC90 automobile along a mountain path. The VR software gave consumers insight into 360-degree landscapes, the grip of the car on winding roads, and the ability to examine the XC90's interior. These activations allow consumers to "sit in the driver's seat" and experience not only the brand's product, but the type of experiences the product will enable in their daily lives. These transformative activations underscore the profound impact of innovation in redefining the landscape of marketing, setting the stage for an exciting and promising future in consumer-brand interactions.

AI continues to figure prominently in brand activations. This year, Sephora rolled out "Sephora Visual Artist', a mobile app that allows customers to demo different makeup products on their faces via an augmented reality software program. Additionally, Sephora created "Color IQ", a program that scans a customer's skin and uses AI to match them with the perfect foundation for their skin tone. Customers are able to use this app at home to try on makeup products without having to step inside a store, allowing Sephora to market their products to consumers anywhere. The continued growth of generative AI in brand activations allows brands to reach customers outside of traditional advertising methods and provide customized advertisements and solutions to consumers, thereby enhancing and personalizing consumer brand interactions.

In addition to bringing the latest technology to live events, advertisers continue to rely on tried and true methods, such as live pop-ups. For example, Fujifilm launched an "INSTAX Share the Joy Tour", where they promoted the new INSTAX Mini Link 3 INSTAX Printer and their cameras in well-known spaces across the country. The pop-up had an enormous inflatable INSTAX camera that consumers could explore, a decorative wall of INSTAX instant cameras and printers, fun games where consumers could win INSTAX swag, and a decorative backdrop for plenty of INSTAX selfies and photos. Other advertisers, like NBC, are raising excitement for live entertainment shows like "The Voice" by hosting a large activation in The Grove, a large outdoor shopping mall in Los Angeles, that let consumers sit in the famous "The Voice" swivel chairs, try their luck in an interactive singing tryout, and play a claw game to win various themed merchandise.

In this dynamic marketing landscape where tradition meets innovation, advertisers are redefining engagement strategies. While some are embracing the latest technological wonders like generative AI and VR/AR to create captivating brand experiences, others stay true to the classics, with live pop-up events that resonate with consumers seeking familiar yet exciting connections. These diverse approaches reflect the adaptability and

creativity of advertisers and the focus on personalizing advertisements for consumers, setting the stage for a promising future in consumer-brand interactions and actively engaged consumers, where tradition and technology intertwine seamlessly.

F. Generative Artificial Intelligence

Falling within the broad category of AI and machine learning, generative AI refers to algorithms underpinning tools such as ChatGPT, DALL-E, Stable Diffusion, and Midjourney that interpret user prompts (including text inputs or uploaded audio or visual material) to generate new content. The content generated by these tools can include images, video, audio, text, and software code based on data on which the algorithm was trained.

Several lawsuits have arisen since early 2023 involving the unauthorized use of original authors' or artists' works in the training data for AI algorithms. Groups of plaintiffs, including visual artists, music publishers, and prominent literary authors such as Jodi Picoult, George R.R. Martin, and comedian Sarah Silverman, have named AI companies like OpenAI and Stability AI as defendants in class-action lawsuits. They allege that these companies misused and infringed upon copyrighted literary and artistic works to train their AI platforms.

Additional risks of legal action abound when considering whether AI-generated output may infringe upon any pre-existing intellectual property rights. It's important that marketers and agencies evaluate an AI platform's Terms of Service or End User License Agreements, as well as the platform's disclosed training data set (if available), to determine if the platform takes sufficient steps to reduce the risk of producing arguably infringing output. For instance, AI platforms that have trained their algorithms solely on licensed data are less likely to generate infringing output compared to those that use algorithms built on data scraped from the internet without permission. To further minimize risk, marketers and agencies should ensure that their staff who use AI tools do not input prompts likely to produce infringing work—such as prompting the AI platform to generate content in the style of a particular artist, writer, or musician—which is more likely to result in content substantially similar to that individual's work.

Moreover, the U.S. Copyright Office has provided guidance on AI-generated works. In March 2023, the Copyright Office issued a policy statement clarifying that works generated entirely by AI are not eligible for copyright protection due to the lack of human authorship. However, if a human contributes creative expression to the work, such as by making artistic choices in the prompt or by modifying the AI-generated output, the human-authored portions may be eligible for copyright protection. The Copyright Office also announced plans to review existing registrations for works that include AI-generated content.

Generative AI presents enormous potential, and enormous risk, for the advertising industry. The use of AI has steadily gained traction over the last few years in industries ranging from advertising and public relations to fashion and technology, and it's not hard to see why. AI provides a myriad of opportunities and potential applications within these fields, but it can also be a double-edged sword presenting several potential legal issues.

To maximize the benefits of AI while mitigating legal risks of use, consider some best practices:

- Always familiarize yourself with the terms of a particular platform's services and use the outputs in accordance with those terms (e.g., do not use services with "personal use only" restrictions in commercial advertising). If you are going to use specialty features of an AI platform, additional terms may also apply.
- Always conduct a human review of AI's outputs and consider whether the elements depicted (persons, locations, etc.) identify someone or something known or recognizable. For example, in a commercial's depiction of a futuristic city in 2050, it would be problematic if a futuristic device resembled Apple's Airpods, the design of which is protected under patent law.
- Be careful of the inputs you contribute to AI platforms. For example, "create a better soft drink than Coca Cola" could be problematic if your client were a competing beverage company.
- Consult with legal counsel to discuss potential regulatory, data privacy, intellectual property, and right of publicity issues before implementing AI outputs, particularly in deliverables to clients.
- Lastly, be sensitive to claims of bias and inaccurate representation when asking AI services to present the viewpoint of an underrepresented group. For example, is it really possible for OpenAI to provide a certain person's perspective? Some might find this depiction problematic.

In instances where a particular individual's persona is not intended or consented to be used, efforts must made to ensure that AI-generated output does not infringe upon that individual's publicity rights. To reduce the risk of a right of publicity claim:

- Marketers should not use text prompts that may be likely to create an image, video or sound that looks or sounds like a specific person. For example, do not include names of living individuals (particularly celebrities or other public figures) in text prompts or other prompts intended to generate work that resembles a particular person.
- Marketers that may intend to modify images or voices of individuals with whom they have existing agreements should review the applicable talent or endorsement

agreements to determine whether and to what extent the company may produce and use such modified AI-generated content without additional consents.

- As an alternative to using AI-generated images of people, marketers could also consider populating AI-generated materials with licensed images of actual individuals. AI outputs identifying people (who may be entirely fictitious) can result in right of publicity claims from members of the general public who resemble the AI figure. Consider swapping the face of any AI-generated persons for a person whose likeness is fully and securely licensed (e.g., through talent the agency itself obtains or images from a reputable stock agency, like Getty Images or Shutterstock).

a. Key Sources of Law and Regulation

   i. FTC Act: The Federal Trade Commission (FTC) enforces the FTC Act, which prohibits deceptive or unfair business practices. For generative AI, this means companies must avoid misleading claims about AI capabilities or data handling, and ensure fair practices in AI-driven recommendations, data collection, and privacy.

   ii. FCC: The FCC's regulations are primarily focused on telecommunications and media but are increasingly relevant to AI in digital communication, particularly in AI-driven telecommunications services (such as robo-calls and auto-dialers) and information dissemination. With AI applications in speech recognition, customer service, and broadcasting, compliance with the FCC's rules on consumer privacy, transparency, and fair access in communications technologies is essential.

   iii. U.S. State Laws: With Congress yet to pass a comprehensive AI law, individual states have begun establishing their own AI regulations, a pattern seen after the EU enacted the AI Act. Colorado passed the Colorado AI Act (effective February 2026), which adopts a risk-based framework similar to the EU AI Act. This law requires transparency, impact assessments, and safeguards for "high-risk" AI systems that impact significant consumer decisions in fields like employment, finance, and healthcare. Other states, like Utah and Tennessee, are also taking steps; Utah's AI Policy Act mandates disclosure when generative AI interacts with consumers, while Tennessee's ELVIS Act addresses unauthorized AI replication of likeness and voice. California is similarly progressing, focusing on preventing algorithmic discrimination in relying on AI-powered hiring tools and establishing opt-out rights for automated decision-making. However, legislative success has been mixed; Connecticut's attempt to pass AI legislation failed, partly due to concerns that the bill would chill AI innovation in the state.

   iv. EU AI Act: The EU Artificial Intelligence Act, the world's first comprehensive AI regulatory framework, was formally adopted in 2024 and will gradually take

effect over the coming years. It regulates AI activities within the EU and, significantly, also applies to non-EU entities whose AI outputs impact the EU market. The Act uses a risk-based approach, restricting or prohibiting high-risk activities like social scoring, exploitative practices, and certain biometric uses. Both AI providers and users are required to ensure transparency, manage risks, and comply with stringent disclosure obligations to protect EU consumers and support ethical AI deployment. Generative AI tools may fall into these regulated categories, especially if they influence decision-making in sensitive areas like employment or legal analysis.

b. Recent Developments in Enforcement

i. FTC Enforcement: Recently, the FTC launched "Operation AI Comply," setting forth a number of case studies showcasing deceptive marketing practices that exploit AI's appeal. This enforcement sweep exposed five cases where companies allegedly misled consumers about AI-driven products, violating FTC consumer protection laws. The cases involve exaggerated claims about AI's capabilities, especially in "AI-powered" business opportunities promising rapid profits or fake review generation tools. Notable cases include DoNotPay, Ascend Ecom, and Rytr, where companies used AI buzzwords to attract customers but failed to deliver on those promises. Through these actions, the FTC warns businesses to be truthful about AI capabilities and avoid misleading advertisements, unverified claims, and fake reviews.

ii. FCC Enforcement: Under a recent proposal, the FCC seeks to define AI-generated calls and texts, mandate disclosure by callers regarding AI usage, and implement technologies to protect consumers from unwanted AI-generated communications. These proposals include transparency standards, such as requiring notification during each AI-generated call and supporting tools to identify and block illegal calls. The FCC also seeks to balance these protections with positive applications of AI, allowing AI tools that assist individuals with disabilities to continue without restrictions. Additionally, the FCC has clarified that voice cloning in scams, like those used to deceive or misinform the public, is illegal without express consent, and it has proposed significant fines for unauthorized AI-driven election misinformation.

c. Deepfakes

Consider the right of publicity issues raised by deepfakes, an AI-technology that uses synthetic media to create a hyper-realistic image, video, or sound of a person that (typically) did not participate in or consent to its creation. These digital impersonations are easily exploited by unsavory marketers, since it is often difficult for viewers to discern whether the celebrity's product plug is inauthentic. In the fall of 2023, Gayle King was spoofed to promote a weight loss supplement she neither

used nor heard of, and Tom Hanks found an AI version of himself promoting a scam dental plan. But it's not just A-listers like Tom Brady, Jennifer Lawrence, and Arnold Schwarzenegger who have fallen victim to deepfake controversies. MrBeast, a YouTube star, was surprised to open his TikTok app to a video of himself encouraging viewers to participate in "the world's largest iPhone 15 giveaway," and then there was President George W. Bush explaining the future of AI for Omnekey, an AI platform that generates personalized ads at scale. Each of these uses involved deepfakes that manipulated the person's face and voice without their express authorization.

The temptation to use emerging technologies to create digital replications of living individuals – for unauthorized marketing or more malicious purposes, as happened to Emma Watson in a deepfake reading of Adolf Hitler's *Mein Kampf* – is beginning to be challenged by rights-holders in court. Consider the recent federal suit brought against NeoCortext, a Ukrainian company that developed an app called Reface, which allows users to swap their faces with well-known individuals in scenes from popular shows and movies. Kyland Young, a finalist on "Big Brother" and contestant on "The Challenge: USA", filed a proposed class action against NeoCortext in California, arguing that he did not agree to NeoCortext's use of his image and never received compensation from Reface for its use of his image. Young seeks to represent a class of California residents whose name, voice, signature, photograph, or likeness has been displayed on the Reface app without their consent. NeoCortext argued unsuccessfully that the claims are preempted by the U.S. Copyright Act and the First Amendment, and the use in the context of deepfakes is "transformative."

G. Endorsements and Testimonials

State Laws Governing Child Influencers – Fair Compensation

Recently, several states have either passed or proposed legislation aimed at protecting child influencers from being unfairly exploited, by ensuring that children appearing in influencer content – whether their own, or their parents' – are being fairly compensated for their work and use of their likeness. These new laws require vloggers to set aside funds in a trust for the minors appearing in their content, and to maintain adequate records to enable calculation of the amounts that should be put into said trust and confirmation of deposits.

a. Passed Legislation:

   i. California (SB 764 and AB 1880) - Effective on January 1, 2025.

   ii. Illinois (SB 1782) - Effective as of July 1, 2024.

   iii. Minnesota (HF 3488) - Effective on July 1, 2025.

b. Pending Proposed Legislation:

The following states have introduced bills similar to California, Illinois, and Minnesota into their state legislatures.

i. Arizona (HB 2565)

ii. Georgia (HB 968)

iii. Maryland (HB 645)

iv. Missouri (HB No. 1998)

v. Ohio (H. B. No. 376)

vi. Pennsylvania (HB 2377)

vii. Washington (HB 1627)

FTC Rule Banning Fake Reviews – Trade Regulation Rule on the Use of Consumer Reviews and Testimonials

The FTC's mission to crack down on dark patterns and deceptive consumer review practices remains steady. In August 2024, the FTC approved its final rule banning fake reviews and testimonials (Trade Regulation Rule on the Use of Consumer Reviews and Testimonials, 16 C.F.R. § 465, October 2024), which prohibits deceptive 'fake review' practices, involving the sale, purchase, and distribution of biased and/or otherwise manipulated consumer reviews and testimonials. Specifically, the FTC's rule banning fake reviews and testimonials prohibits the following:

a. The creation, purchase or sale of fake or false consumer reviews, consumer testimonials, or celebrity testimonials (including AI-generated fake reviews) (§ 465.2).

b. Providing compensation in exchange for consumer reviews that express a particular sentiment (positive or negative) (§ 465.4).

c. Insider consumer reviews and consumer testimonials, without the inclusion of a clear and conspicuous disclosure of the material relationship to the business, unless, in the case of a consumer testimonial, the relationship is otherwise clear to the audience. Exception provided for generalized solicitations to purchasers for them to post reviews about their experiences with the product, service, or business (§ 465.5).

d. Misrepresentation that company-controlled review websites or entities provide independent reviews or opinions (other than consumer reviews) about a category of products or services that includes its own products or services (§ 465.6).

e. Make baseless threats in an attempt to suppress reviews or cause reviews to be

removed, and misrepresent that the consumers reviews being displayed represent all or most reviews, when reviews are being suppressed. Exceptions are provided for reviews that include trade secrets or confidential information, that are defamatory or otherwise offensive (as set forth in the rule), violate a third party, or are false or misleading (§ 465.7).

f. Sell, distribute, purchase or procure fake indicators of social media influence that can be used to materially misrepresent a party's influence or importance for a commercial purpose (§ 465.8).

Guides Concerning the Use of Endorsements and Testimonials in Advertising

After years of anticipation, in 2023, the Federal Trade Commission (FTC) issued revised Guides Concerning the Use of Endorsements and Testimonials in Advertising (the "Endorsement Guides"). (Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255 (July 2023), available at: https://www.federalregister.gov/documents/2023/07/26/2023-14795/guides-concerning-the-use-of-endorsements-and-testimonials-in-advertising.).

The revised Endorsement Guides echo the FTC's increasing focus on "dark patterns" and transparency. The revised Endorsement Guides include notable changes to key definitions, and provide additional clarity on disclosure requirements, taking into consideration target audiences and advancements in technology.

a. Updates to Key Definitions:

   i. Endorser: According to the revised Endorsement Guides, "[t]he party whose opinions, beliefs, findings, or experience the message appears to reflect will be called the endorser and could be or appear to be an individual, group, or institution". The word "appear" is important to note – as an endorser is not only an individual, group, or institution, but also any entity that appears to be one, such as a virtual influencer.

   ii. Endorsement: According to the revised Endorsement Guides, "an endorsement means any advertising, marketing, or promotional message for a product that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser. Verbal statements, tags in social media posts, demonstrations, depictions of the name, signature, likeness or other identifying personal characteristics of an individual, and the name or seal of an organization can be endorsements." The updated Endorsement Guides clarify that fake positive reviews and reviews by influencers who receive unsolicited products and post about them, even if not required to, are considered endorsements.

iii. Clear and Conspicuous: Going above and beyond the prior standard that in order for disclosures to be "clear and conspicuous," disclosures were to be "noticeable and easily understandable" – the revised Endorsement Guides now require that disclosures must be "unavoidable." "Unavoidable" means that a consumer cannot miss the disclosure and must not be required to click through or take other actions to see material information.

b. Updated Guidance on Disclosures:

i. Placement: The revised Endorsement Guides explain that disclosures should be placed where ordinary consumers will not miss them and displayed in an easy-to-read font that contrasts enough to stand out from its background. Of note, for audiovisual content, the FTC recommends including audio and visual disclosures if the endorsement is made via both mediums. The FTC also recommends that the disclosure be made up front or in close proximity to the representation that requires the disclosure, which may mean multiple or continuous disclosures throughout a video.

ii. Ordinary is Relative: Disclosures must be clear and conspicuous to ordinary consumers in the targeted group. If the ad is targeted at older adults, it must account for that demographic's vision or hearing abilities. Similarly, if an ad is in Spanish and targeting Spanish-speaking audiences, the disclosures must also be in Spanish.

iii. When in Doubt, Add the Brand: While the FTC continues to advise that starting a post with "Ad:", "Paid ad", "#ad", "Advertising", "Advertisement" "Sponsored" or "Promotion" might still be effective, it is now saying that disclosures like the following, that incorporate the brand name (XYZ) are clearer:

- "Sponsored by XYZ"
- "Promotion by XYZ"
- "I was given a free [name of product] from XYZ to review"
- #XYZ_sweepstakes.

iv. Don't Rely on Built-In Tools: The revised Endorsement Guides continue to caution that many forms of disclosure built into platforms may not be sufficient. As such, the FTC recommends that brands and influencers add their own disclosures – though the FTC has offered to work with platforms that want to improve their disclosure tools.

v. Reposts: Ensure disclosures remain attached to any reposts. Brands could face liability on a number of fronts, including for failing to disclose the relationship with an influencer if the original post's disclosure was ambiguous or obscured in the repost; or for failing to confirm that the

endorser still holds the same opinion of a product whose formulation has changed since the original post.

vi. Disclaim Atypical Results: Even when brands use a real customer's testimonial, if the results were atypical, they must say so and disclose the expected or typical results based on reliable scientific evidence. Moreover, advertisers cannot pair a testimonial with a misleading image – for example, when promoting an endorsement from a weight-loss customer who went from 300 pounds to 250 pounds, if the ad accompanies the testimonial with an image of a 100-pound person, it would be deceptive.

c. Special Concerns for Children: The revised Endorsement Guides end with a cautionary warning to advertisers that none of the examples provided apply to advertisements directed at children, which "may be of special concern because of the character of the audience." As the FTC noted in response to comments on the proposed rule, research shows that disclosures do not work for children as they do for adults. Thus, ads that include endorsements and are directed at kids may fall short of the FTC's requirements, even if they include a disclosure that any adult would find clear and conspicuous.

d. Shared Liability: As always, endorsements must reflect honest opinions of the endorser, advertising claims must be substantiated, an endorser's experience **should** be substantiated and representative of what consumers will generally achieve, expected performance must be clearly and conspicuously disclosed, an expert endorser's qualifications must actually give the endorser expertise, and material connections between advertisers and endorsers must be disclosed. Brands, as well as their PR, marketing, advertising, reputation management and other creative partners, could be liable if an endorser misrepresents a product's efficacy or their personal experience with the product. Brands who act in good faith and provide effective guidance may reduce the risk of facing an FTC enforcement action. Dot Com Disclosures: How to Make Effective Disclosures in Digital Advertising (.Com Disclosures).

In 2013, the FTC updated its .Com Disclosures guide to provide guidance on how to properly make advertising disclosures in various forms of new media, including online and in mobile. Most importantly, disclosures must be clear and conspicuous on all platforms and devices, and not be buried in hyperlinks. If a hyperlink is used, it must convey the nature and relevance of the information to which it leads.

In 2022, the FTC sought public comment on ways to modernize the .Com Disclosures, in keeping with its increased focus on "dark patterns". Updates to the .Com Disclosures remain pending, as other initiatives like proposed updates to the Negative Option Rule and proposed bans on "junk fees" have taken the

front seat.

FTC Enforcement under the new Endorsement Guides

In November 2023, the FTC's first high-profile enforcement efforts of the new Endorsement Guides were warning letters targeted at the American Beverage Association and the Canadian Sugar Institute, and several influencers they had engaged who the FTC believed did not clearly disclose their connection to these organizations.

FTC Issues Letters to More Than 700 Companies Warning of Violations of the Endorsement Guides

On October 13, 2021, the FTC sent warning letters to over 700 major brands, advertisers, and agencies stating that any violations of the FTC's Endorsement Guides could result in fines of up to $43,792 per incident. While the notices do not allege any wrongdoing by the companies, they show a dynamic shift in the FTC's focus, as the FTC seems prepared to closely monitor and respond to future wrongdoing with significant fines. Prior to these letters, the FTC has resolved most allegations of false or misleading endorsements without monetary penalties.

According to the letters, the FTC will be looking for violations such as "falsely claiming an endorsement by a third party; misrepresenting whether an endorser is an actual, current, or recent user; using an endorsement to make deceptive performance claims; failing to disclose an unexpected material connection with an endorser; and misrepresenting that the experience of endorsers represents consumers' typical or ordinary experience." The FTC is looking to take advantage of its so-called Penalty Offense Authority, pursuant to 15 USC 5(m)(1)(B), allowing the FTC to seek punitive civil fines without the need to prove financial harm to consumers. Instead, it can impose statutory-based fines of up to $43,792 per violation, and levy fines against first-time offenders, something that the FTC has not done since the 1980s. It is important to note that any company must have actual notice of the illegal conduct, hence the notices to over 700 of the country's most prominent advertisers and agencies.

The FTC's prior focus in this area is illustrated in its 2020 action against Teami, a health and wellness company, which settled with the FTC concerning allegations that, along with making unsubstantiated health claims, it hired influencers who did not adequately disclose that they were being paid to endorse their product on social media. The settlement required the defendants to take actionable steps to monitor their endorsers, which included providing hired talent with a statement of their disclosure responsibilities, creating a system to monitor their posts, declining to approve posts lacking disclosures, and terminating payments to any noncompliant endorsers. In connection with this action, the FTC sent warning letters to the ten influencers hired by Teami (including music and television personalities such as Cardi B and Jordin Sparks). Consistent with the FTC's prior guidance on influencer disclosures, the warning letters

reminded influencers that they should use unambiguous language that consumers would easily comprehend, and that consumers must be able to see disclosures without having to click to expand additional text. Specifically, the letters reiterated that endorsers should disclose any material connection above the "more" button on Instagram. Based on the examples the FTC appended to its complaint, the influencer's endorsement of the Teami products appeared within the post's video or photo or within the first two or three lines of the post's caption. However, any disclosure regarding the influencer's connection to Teami was not visible unless the consumer clicked the "more" button. This FTC action serves as another warning to advertisers and influencers alike that disclosures are still as important as ever.

H. Data Privacy and Security; Behavioral Advertising

Key Sources of Law and Regulation

a. Federal Trade Commission Act § 5

   i. As established in the 2015 *Wyndham* case discussed below, the FTC can use Section 5 of the FTC Act to regulate companies' privacy and data security safeguards.

   ii. Section 5 prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."

      1. Deception: misrepresentations or omissions likely to mislead consumers acting reasonably under the circumstances.

      2. Unfairness: causes or is likely to cause substantial consumer injury, not reasonably avoided by the consumer, and not outweighed by countervailing benefits to consumers or competition.

b. Children's Online Privacy Protection Act (COPPA)

   i. All website or online service operators who intend to reach children under the age of 13 and collect personal information from such children or that operate a general audience website or online service and have actual knowledge of the collection of personal information from children under the age of 13 must, among other things:

      1. Post an adequate privacy policy;
      2. Obtain "verifiable parental consent";
      3. Allow parent / legal guardian to revoke his/her consent, review the child's information, and direct the operator to delete the child's personal information; and
      4. Establish and maintain reasonable security procedures.

ii. In June 2024, the Senate overwhelmingly passed COPPA 2.0 legislation, which would update and expand the existing online privacy protections for children in the following ways:

1. Increasing the age requirement from 13 to 16 years old for companies to collect personal information from children without consent.
2. Banning targeted advertising to children and teens.
3. Revising COPPA's "actual knowledge" standard, covering platforms that are "reasonably likely to be used" by children and protecting users who are "reasonably likely to be" children or minors.
4. Creating an "Eraser Button" for parents and kids by requiring companies to permit users to eliminate personal information from a child or teen when technologically feasible.
5. Establishing a "Digital Marketing Bill of Rights for Teens" that limits the collection of personal information of teens.
6. Establishing a Youth Marketing and Privacy Division at the FTC.

The Senate simultaneously passed the Kids Online Safety Act (KOSA), which provides children and parents with the tools, safeguards and transparency to protect against online harms. It establishes a "duty of care" for online platforms and requires them to activate the most protective settings for kids by default, providing minors with options to protect their information, disable addictive product features and opt-out of personalized algorithmic recommendations.

COPPA 2.0 and KOSA are awaiting a vote by the House of Representatives.

c. Health Insurance Portability and Accountability Act (HIPAA)

i. Provides standards for the way Protected Health Information (PHI) is collected, handled, maintained and shared by Covered Entities and those third-party agents acting on their behalf (Business Associates).

1. "Protected Health Information" means individually identifiable health information.
2. "Covered Entity" means a health plan, health care clearing house or health care provider who transmits PHI electronically.

d. Gramm-Leach-Bliley Act (GLB)

i. Creates an affirmative obligation on financial institutions with respect to their collection, use and dissemination of a consumer's financial information.

ii. Specific requirements:

1. Privacy policy / GLB notice;
2. Annual notice;
3. Opt-out for sharing with nonaffiliated third parties; and
4. Security safeguard rules.

e. American Privacy Rights Act (APRA)

i. The United States is among the minority of large economies in the world without a comprehensive national privacy law. Members of the U.S. House of Representatives seeking to change this state of affairs have put forward a draft bill for the American Privacy Rights Act (APRA), most recently amended on June 20, 2024. Because the APRA's intent is to "establish a uniform national data privacy and data security standard in the United States," it would expressly preempt state laws that cover the same requirements, such as the California Consumer Privacy Act (discussed below). The APRA would apply to "covered entities," meaning any entity that determines the purposes of processing and is subject to the Federal Trade Commission (FTC) Act, except for those that meet the criteria of a "small business," defined as an entity: (1) with less than $40 million in annual revenue; (2) which annually processes the covered data of 200,000 individuals or less (with exceptions relating to payment processing); and (3) does not transfer covered data to a third party in exchange for revenue or anything of value. Key features include, but are not limited to:

1. Data minimization.
2. Privacy policy requirement.
3. Consumer rights of access, deletion, and correction, and right to opt out of targeted advertising and data transfers generally.
4. National data broker registry.
5. Heightened definitions for sensitive data.

f. State Privacy and Security Standards (Key Examples)

i. California Consumer Privacy Act of 2018 (CCPA). The CCPA took effect on January 1, 2020. It provides California consumers with an array of rights and imposes significant privacy-related obligations on certain for-profit entities that do business in that state. While the law only applies to residents of California, all companies serving those residents must ensure that their policies are compliant with the requirements under CCPA. Some highlights of the CCPA include the following:

1. Applies to for-profit entities that process personal information of California residents, determine the purposes and means of processing

such personal information, does business in California, and meet one or more of the following conditions:

a. Generates $25,000,000 or more in annual revenue;

b. Generate 50% or more of its annual revenue from selling or sharing consumers' personal information; or

c. Buy, sell, or share the personal information of 100,000 or more California consumers or households, annually.

2. Affords California residents an array of rights, including (i) the right to be informed (through a privacy policy and upon request) about what kinds of personal information companies have collected, the sources of such information, why it was collected, and with whom such information will be shared or sold; (ii) the right to have a business delete their personal information (with certain exceptions); (iii) the right to receive equal pricing and service even if a consumer has exercised his/her privacy rights under the Act; (iv) the right to opt out of sales of personal information or sharing of personal information for cross-context behavioral advertising (or, for consumers who are under 16 years old, the right not to have their personal information sold or shared absent their, or their parent's, opt-in); (v) the right to access personal information in a "readily useable format" in order to take it elsewhere; (vi) the right to correct inaccurate personal information; and (vii) the right to limit the use and disclosure of "sensitive personal information" (SPI).

3. Definition of Personal Information — The definition of personal information is broad and includes browsing and search history, geolocation data and inferences drawn from data to create a profile that reflects a consumer's trends, preferences and behavior.

4. Sensitive Personal Information—SPI is a subset of personal information that includes:

   a. Social security, driver's license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious or philosophical beliefs, or union membership; the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; or genetic data;

b. The processing of biometric information for the purpose of uniquely identifying a consumer;

c. Personal information collected and analyzed concerning a consumer's health; or

d. Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

5. Financial Damages — The Act provides a limited private right of action for consumers in the event of a data breach. In those instances, consumers may recover damages in an amount ranging from $100 to $750 per consumer per incident, or actual damages, whichever is greater. Should the company not cure any breach asserted by a consumer, and the attorney general decline to prosecute, consumers can mount a class action lawsuit.

ii. California Privacy Rights Act (CPRA)

1. The California Privacy Rights Act (CPRA) was approved by California voters on November 3, 2020. It significantly amends and expands upon the CCPA, and creates a new regulatory agency, the California Privacy Protection Agency (CPPA), which is vested with "full administrative power, authority, and jurisdiction to implement and enforce" the CPRA.

iii. California Age-Appropriate Design Code Act

1. On September 20, 2022, California Governor Gavin Newsom signed into law the Age-Appropriate Design Code Act (AADC), which had been scheduled to go into effect on July 1, 2024. The law would prohibit companies from collecting any minor's user data beyond what is absolutely necessary or leveraging children's personal information in any way "materially detrimental to the physical health, mental health, or well-being of a child." This law defines a child as anyone under 18 years of age, and would require affected companies to default users under 18 to the strongest privacy settings.

2. The AADC was temporarily blocked by a federal court judge who found that the law likely violates the First Amendment and does "not pass constitutional muster." The Ninth Circuit subsequently upheld the lower court's ruling in part, holding that the AADC's Data Protection Impact Assessment (DPIA) requirement fails fail First Amendment scrutiny, but sent other parts of the law back to the lower court to reconsider and vacated the rest of the preliminary injunction

on the basis that it is unclear if the rest of the AADC violates the First Amendment.

iv. Connecticut SB 3 – On June 26, 2024, Connecticut Senate Bill 3 ("SB 3") was signed into law. SB 3 amends the existing Connecticut Data Privacy Act (discussed below) to include new requirements concerning consumer health data and children's online protection. Notably, the law imposes requirements effective October 1, 2024, on controllers that offer online services, products, or features "to consumers whom such controller has actual knowledge, or willfully disregards, are minors," defined as consumers under 18 years old. This includes a prohibition on selling a minor's personal data or processing a minor's personal data for purposes of targeted advertising without the minor's opt-in consent, which will have a significant impact on the advertising industry.

v. Maryland Age-Appropriate Design Code ("MAADC") – The MAADC, effective, as of October 1, 2024, imposes requirements on online products that are "reasonably likely to be accessed by children," defined as consumers under 18. These include, but are not limited to, requirements to conduct data protection impact assessments, and configure all default privacy settings provided to children by the online product to offer a high level of privacy.

vi. Massachusetts 21 CMR 17.00 — Standards for the Protection of Personal Information of Residents of the Commonwealth

1. "Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written…"

2. Three Key Aspects of Regulations

   a. Develop a Written Information Security Program (WISP)
   b. Contractual obligations with third party service providers
   c. Encryption of PII on public networks and portable devices

vii. New York — Security Breach Notification SHIELD ACT

1. In 2019, New York State signed into law a bill that strengthens the state's existing security breach notification rules and imposes significant new obligations on companies that own or license the "private information" of New York residents. The Stop Hacks and Improve Electronic Data Security Act (SHIELD ACT), requires any business holding private information of a New York resident, to develop, implement and maintain reasonable safeguards to protect the integrity of that information. The program should be documented in a written information security policy to reflect the company's business, data and operations.

viii. Nevada SB 220

1. SB 220 adds to the current Nevada law and will require website and online service operators to provide Nevada residents with a right to opt-out of the "sale" of Covered Information collected online. Importantly, a "sale" is narrowly defined as the exchange of Covered Information for monetary consideration by the operator to a person to license or sell the covered information to additional persons. Covered Information includes name, contact information (i.e., email address, street address and phone number), social security number, identifiers that can be used to contact an individual either physically or online and any other information collected from a person in combination with an identifier that makes the information personally identifiable. In particular, operators will need to establish a "designated request address", that is, an email address, toll-free telephone number or website, through which a consumer may submit a verified request directing the operator not to make any sale of Covered Information collected or to be collected about the consumer. The update does not add a private right of action against operators. Nevada's Attorney General, however, is empowered to seek an injunction or a civil penalty, up to $5,000 for each violation, against an operator who does not establish a designated request address or who sells consumer information in violation of the law.

ix. State Data Broker Laws

1. Vermont's Data Broker Law, the first of its kind in the United States specifically governing data brokers, took effect January 1, 2019. A "data broker," defined as a business that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship,

must register annually with the State of Vermont, and provide information about its data collection activities, opt-out policies (in particular, whether it permits consumers to opt out of its collection of brokered personal information), purchaser credentialing practices, and certain information about security breaches that it has experienced during the prior year. The law also requires that data brokers adopt an information security program with administrative, technical, and physical safeguards to protect sensitive personal information.

2. California enacted its own Data Broker Registration law in October 2019, which requires data brokers to register annually with the California Attorney General. “Data brokers” are defined as CCPA businesses that knowingly collect and sell to third parties the personal information of a consumer with whom the business does not have a direct relationship. On October 10, 2023, California Governor Gavin Newsom signed into law the “Delete Act,” which amends certain aspects of the existing Data Broker Registration law and empowers the CPPA to develop a system to allow consumers to make a single data deletion request that is binding on all data brokers registered in California.

3. Texas signed into law SB 2105 on June 18, 2023, which requires data brokers to register with the State of Texas prior to doing business in the state. "Data broker" means a business entity whose principal source of revenue is derived from the collecting, processing, or transferring of personal data that the entity did not collect directly from the individual linked or linkable to the data. Similar to the Vermont law, Texas requires data brokers to implement a comprehensive information security program with physical, organizational, and technical security controls. While the scope and contents of these requirements are nearly identical to Vermont’s, they apply to a broader range of “personal data,” defined as “any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual,” including pseudonymous data when used in conjunction with additional data that can link it to an identified or identifiable individual.

4. Oregon’s data broker law, HB 2052, was signed into law on July 27, 2023. It defines “data broker” as a business that collects and sells or licenses to a third party the personal data of another person that the business does not have a direct relationship with. Data brokers must register with the State of Oregon prior to doing business in the state.

x. Washington "My Health My Data" Act and Nevada S.B. 370

1. The "My Health My Data" Act (MHMD) and Nevada's S.B. 370 each took effect on March 31, 2024. MHMD and S.B. 370 apply to any entity doing business in the state that collects "consumer health data," which has a broad and expansive scope that includes any information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present or future physical or mental health status (HIPAA-covered data is exempted). MHMD and S.B. 370 impose extensive transparency and disclosure obligations and set forth some of the strictest opt-in consent requirements of any U.S. privacy law to date. Notably, in order to sell consumer health data, businesses must obtain a prior authorization that includes the customer's signature and discloses, among other criteria: the specific data being sold; the name and contact information of the selling and purchasing entities; a description of the purpose for sale; a statement about the consumer's right to revoke consent at any time; and the authorization's one-year expiration date from the date of signature. MHMD also includes a private right of action, and businesses that violate it may face damages of up to $7,500 per violation, as well as additional damages, capped at $25,000, so there is an added litigation risk under Washington's law. In contrast, S.B. 370 is only enforceable by the Nevada Attorney General.

xi. State Comprehensive Privacy Laws

1. On March 2, 2021, the Virginia Consumer Data Protection Act was signed into law, followed by the Colorado Privacy Act on July 7, 2021. These states were shortly followed by Utah, which signed the Utah Consumer Privacy Act into law on March 24, 2022, and the Connecticut Data Privacy Act, signed on May 10, 2022. The following year saw the enactment of the Montana Consumer Data Privacy Act on May 19, 2023, the Texas Data Privacy and Security Act on June 18, 2023, and the Oregon Consumer Privacy Act on July 18, 2023. The Virginia, Colorado, Connecticut, and Utah laws became effective at varying points in 2023; the Texas and Oregon laws entered into force on July 1, 2024, and Montana's law went into effect on October 1, 2024.

2. Several additional states have enacted similar comprehensive privacy legislation, which have and will become effective at varying points between 202 and 2026. These laws are as follows:

a. Texas Data Privacy and Security Act (effective July 1, 2024).

b. Oregon Consumer Privacy Act (effective July 1, 2024).
c. Montana Consumer Data Privacy Act (effective October 1, 2024).
d. Iowa Consumer Data Protection Act (effective January 1, 2025).
e. Delaware Personal Data Privacy Act (effective January 1, 2025).
f. Nebraska Data Privacy Act (effective January 1, 2025).
g. New Hampshire Privacy Act (effective January 1, 2025).
h. New Jersey Privacy Act (effective January 15, 2025).
i. Tennessee Information Protection Act (effective July 1, 2025).
j. Minnesota Consumer Data Privacy Act (effective July 31, 2025).
k. Maryland Online Data Privacy Act (effective October 1, 2025).
l. Indiana Consumer Data Protection Act (effective January 1, 2026).
m. Kentucky Consumer Data Protection Act (effective January 1, 2026).
n. Rhode Island Data Transparency and Privacy Protection Act (effective January 1, 2026).

xii. State Data Breach Notification Laws

1. All 50 states, plus Washington D.C., Guam, Puerto Rico, and the U.S. Virgin Islands, have their own security breach notification laws.

2. At the core of these data breach notification laws is an obligation on the information holder to disclose a breach to residents of the applicable state whose personal information (as defined by the applicable state law) was acquired by an unauthorized person. Covered entities may also be required, under certain circumstances to provide notice to state regulators and consumer reporting agencies.

g. EEA, UK, and Switzerland — General Data Protection Regulation (GDPR)

i. As of May 25, 2018, the GDPR replaced the E.U. Data Protection Directive 95/46/EC (the "Directive") in protecting the privacy of personal data collected for or about E.U. "data subjects," especially as it relates to the processing, use, and exchange of such personal data. The UK Data Protection Act 2018, as amended in anticipation of Brexit, is the UK's implementation of the GDPR ("UK GDPR").

ii. Use of a regulation instead of a directive aims to harmonize data protection across Member States, since a regulation does not require implementation of each of the Member States. However, there are still many national derogations.

iii. The core rules of the GDPR include six general principles and certain processing conditions. The six principles:

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Retention
6. Integrity and Confidentiality

iv. Key GDPR Components to Note

1. Extraterritorial Reach — The GDPR applies to businesses established in the EU and businesses based outside the EU but offer goods and services to or monitor individuals in the EU.
2. Children — A child is someone under 16, although Member States can choose to reduce this age to 13. Under the GDPR, children will have a stronger "right to be forgotten."
3. Consent — Under the Directive, obtaining valid consent will be much more difficult.
4. Privacy Notices — The GDPR increases the amount of information to be included in privacy notices.
5. Data Subjects — Data subjects under the GDPR have new rights such as data portability, right to be forgotten, right to restrict processing, and right to object.
6. Accountability — The GDPR puts in place various accountability mechanisms, such as: requiring companies conducting high risk processing to do privacy impact assessments and demonstrating compliance to the regulations by signing up to a code of practice or becoming certified.

v. U.S.-E.U. Cross Border Data Transfers. Unless relying on certain limited exceptions, personal data subject to the GDPR may only be transferred to the U.S. if the controller or processor has provided certain safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The safeguards specifically enumerated under the GDPR include:

1. Standard contractual clauses (SCCs) adopted by the EU Commission or that are adopted by a supervisory authority and approved by the EU Commission; or, with respect to transfers of UK personal data, the International Data Transfer Agreement (IDTA) or IDTA Addendum to the SCCs adopted by the UK Secretary of State;
2. Binding Corporate Rules (BCRs); or
3. Approved codes of conducts or certification mechanisms.

vi. EU-U.S. Data Privacy Framework — On July 10, 2023, the European Commission adopted an adequacy decision implementing the new EU-U.S. Data Privacy Framework (DPF), soon followed by the UK government's approval of a "UK Extension" to the DPF on September 21, 2023. The DPF provides an additional mechanism for parties on both sides of the Atlantic to ensure lawful cross-border data transfers, giving businesses an alternative to SCCs or BCRs. These developments followed the Court of Justice of the European Union's 2020 decision invalidating the predecessor EU-US Privacy Shield Framework.

h. EU/UK — ePrivacy Directive/PECR

i. Directive 2002/58/EC, the Privacy and Electronic Communications Directive ("ePrivacy Directive"), applies to processing of personal data in connection with the provision of publicly available e-communications services in EU public communications networks. Each of the EU member states were required to implement the provisions of the ePrivacy Directive into national law as of October 31, 2003. The UK's local implementation of the ePrivacy Directive, the Privacy and Electronic Communications Regulations ("PECR"), is still in effect post-Brexit.

ii. The ePrivacy Directive has been amended several times since its inception. Two important aspects of the law are as follows:

1. Most forms of digital marketing (including marketing calls, texts, emails, and faxes) require prior opt-in consent, with a limited opt-out exception for marketing to existing customers; and
2. Storing of or access to cookies on user's equipment is only allowed on condition that user has given informed consent, unless cookies are used solely for the purpose of: (1) carrying out communication transmissions of over an e-communication network; or (2) to provide services requested by a user.

i. Other International Data Privacy Regimes

i. Brazilian General Data Protection Law (LGPD)

1. The LGPD, effective as of September 2020, became enforceable starting in August 2021.
2. Comprehensive data privacy law that applies to any processing operation carried out by a natural person or a legal entity in or outside of Brazil, so long as: (1) the processing operation is carried out in Brazil; (2) the purpose of the processing activity is to offer or provide goods or services to, or process the data of, individuals located in Brazil; or (3) the personal data was collected in Brazil.

ii. China — Personal Information Protection Law (PIPL)

1. The PIPL is a comprehensive privacy law similar to GDPR that was promulgated in August 2021 and became effective November 2021. The PIPL extends its territorial scope to the processing of personal information conducted outside of China where the purpose of the processing is: (1) to provide products or services to individuals in China; (2) to "analyze" or "assess" the behavior of individuals in China; or (3) for other purposes to be specified by laws and regulations.
2. The PIPL has strict rules regarding the export of Chinese personal information outside of the PRC, including a requirement to obtain individual consent from data subjects. Companies transferring personal information to other jurisdictions may be required to use model contractual clauses or conduct a security assessment approved by China's National Cyberspace Administration.

iii. India – Digital Personal Data Protection Act (DPDP Act)

1. The DPDP Act, passed on August 11, 2023, will come into effect on a date to be decided by the government, which is authorized to determine different dates for entry into force of various provisions of the legislation.
2. The DPDP Act applies to the processing of digital personal data [broadly defined as data in digital form (whether collected in digital form, or in non-digital form and then digitized) about an individual, who is identifiable by such data] in India, and also outside India if such processing is in connection with offering goods or services to data subjects who reside in India.
3. Similar to the GDPR, the DPDP Act imposes various obligations on data controllers, including, but not limited to, with respect to consent, notice, recordkeeping, data transfers, and data breaches. The DPDP Act also provides data subjects with various rights, including the right of access, data correction, deletion, and grievance redressal.

Recent Developments in Enforcement

a. Federal Trade Commission

i. In January 2024, the FTC issued an order prohibiting data broker X-Mode and its successor Outlogic from sharing or selling any sensitive location data to settle allegations that the company sold precise location data that could be used to track people's visits to sensitive locations such as medical and reproductive health clinics and places of worship. The FTC alleged that X-Mode/Outlogic did not remove sensitive locations from the raw location data that it sold to third parties and did not implement reasonable safeguards against downstream use of the precise location data it sold.

ii. The FTC investigated digital marketing and data aggregator InMarket for failing to fully inform consumers about how their location data—including sensitive information about where they live, work, and worship—would be used and that it would be combined with other data about those users for targeted advertising. It also failed to ensure that third-party apps that used its products obtained informed consent from consumers. In May 2024, the FTC issued an order that, among other items, prohibited InMarket from selling, sharing, or licensing any precise location data and any product or service that categorizes or targets consumers based on sensitive location data.

iii. In June 2024, the FTC finalized an order banning software provider Avast from selling, disclosing, or licensing any web browsing data for advertising purposes, and issuing penalties of $16.5 million. The FTC alleged that Avast, through its subsidiary, collected consumers' browsing information through the company's browser extensions and antivirus software, stored it indefinitely, and sold it without adequate notice and without consumer consent. Additionally, Avast allegedly deceived users by claiming that the software would protect consumers' privacy by blocking third party tracking, but it failed to adequately inform consumers that it would sell their detailed, re-identifiable browsing data.

iv. In June 2023, the FTC reached a whopping $20 million settlement with Microsoft over XBOX's COPPA violations. In violation of COPPA, Microsoft gathered and stored personal information from children through their XBOX gaming systems without obtaining consent from their parents. Due to a pre-checked box on their platform, users unknowingly consented to Microsoft sharing children's data with third parties. In addition to a $20 million settlement with the FTC, Microsoft also agreed to notify parents of additional privacy protections, delete personal information if consent is

not provided within two weeks of the collection date and disclose which personal information comes from children to third-parties. The case emphasized that the FTC is enforcing COPPA strictly, even for third parties that receive data like avatars, health details and other personal identifying information from children.

v. OpenX (2021) – The FTC charged and settled with OpenX Technologies, Inc. over multiple privacy-related claims, including that OpenX collected geolocation information from users who asked not to be tracked. OpenX was ordered to pay $2 million in the settlement, and OpenX was required to delete all ad request data it collected to serve targeted ads. OpenX is also prohibited from collecting location information through its software development kits for mobile applications without first obtaining consent.

b. European Supervisory Authorities

i. On July 10, 2023, the European Commission adopted an adequacy decision on the EU-U.S. Data Privacy Framework ("DPF"). Following the 2020 decision by the Court of Justice of the European Union to invalidate the prior EU-U.S. Privacy Shield Framework, U.S. companies could no longer rely on their privacy shield certification as a lawful means to transfer EU personal data. However, the DPF now provides an alternative mechanism – instead of standard contractual clauses or binding corporate rules– to ensure the lawful transfer of data across the Atlantic. Companies that retained their certification under the Privacy Shield have access to a simplified procedure to self-certify under the new DPF.

ii. In February 2022, the Belgian Data Protection Authority ("APD") issued a gut-punching decision, invalidating the viability of the IAB Europe's so-called "Transparency and Consent Framework ("TCF"). The TCF's set of technical standards and policies was designed to help the entire digital advertising ecosystem comply with GDPR and the ePrivacy Directive. TCF worked by encoding and signaling users' privacy preferences in transparency and consent strings. This decision called the practice into question, sticking the IAB Europe with a hefty fine. IAB Europe is currently appealing the decision. In January 2023, the APD approved an action plan put forward by IAB Europe to update TCF, and the implementation timeline is currently under review. The entire advertising ecosystem must anxiously await the APD's response to the appeal and the implementation of the action plan.

Privacy in the Mobile Space

a. *Facebook*, FTC File No. 092 3184 (April 2021) — The U.S. District Court for the District of Columbia approved the 2019 settlement between Facebook and the FTC and the U.S. Department of Justice. The settlement addressed allegations that Facebook had misled users as to the degree of control they would have over their personal information and, among other things, imposed a $5 billion penalty, the largest ever imposed on a company in respect of consumer privacy violations.

b. *Flo*, FTC File No. 192 3133 (January 2021) — Flo Health, the developer of a popular fertility-tracking app, settled FTC allegations that the company disclosed user health data (e.g., the fact that a user was pregnant) to third party analytics providers without user authorization and without adequately limiting the ways in which the data could be used. The settlement requires, among other things, (i) that Flo pursue an independent audit of its privacy and security measures, (ii) that it get affirmative user consent before disclosing their health information, (iii) that it be transparent about the purposes for which user data is collected or used, to whom it is disclosed and for what purposes, and (iv) notifying users whose personal data was improperly disclosed and instructing the unauthorized recipients of that data to destroy it.

c. *Zoom*, FTC File, No. 192 3167 (November 2020) — Zoom settled with the FTC regarding allegations that it had misled users of its conferencing application by, among other things, making false claims about the level and extent of encryption technologies used to secure user communications. The settlement prohibited Zoom from making misrepresentations as to its privacy practices and required Zoom to implement a comprehensive privacy and security program, including implementing measures specifically targeted at addressing the issues identified in the complaint. Zoom must also obtain periodic independent security assessments, which the FTC may approve, and must notify the FTC of any data breaches it experiences.

d. *California v. Glow*, No. CGC-2 0-5 86·611 (September 17, 2020) — The California Attorney General reached a settlement with Glow, Inc., the developers of a mobile app that tracks fertility and ovulation, following allegations that the app had a number of privacy and security inadequacies, including failure to adequately authenticate requests for information sharing between users and to verify the identity of users requesting account password changes. No data security incident gave rise to the settlement; rather, it was targeted at the privacy and security design of the app's operations. The settlement included a $250,000 civil penalty in addition to imposing a broad range of injunctive obligations on Glow, among them (i) requiring Glow to obtain affirmative

consent before disclosing user data to third parties; (ii) implementing privacy-by-design and security-by-design processes for the app; and (iii) in developing such processes, specifically addressing gender-based risks and the disparate impact that privacy and security incidents may have on women.

e. *TikTok*, FTC File No. 172 3004 (February 2019) — The video social networking app TikTok agreed to a consent decree with the FCC under which TikTok will pay a $5.7 million fine following allegations that it violated the Children's Online Privacy Protection Act and the FTC's Children's Online Privacy Protection Rule by collecting personal information (including email address, first and last name and phone number) from children under the age of 13 without obtaining parental consent. As part of the consent decree, TikTok agreed to comply with COPPA and delete videos uploaded by children younger than 13.

f. TikTok (2022) — The ever-present viral video app TikTok has been making headlines in the privacy realm throughout 2022. In June, leaked video from internal TikTok meetings show that US user data has been repeatedly accessed from China, raising privacy and security concerns. In response, U.S. lawmakers sounded the alarm in July, with some calling for a national privacy protection law and several Republican lawmakers expressing concerns in a letter to TikTok.

g. Apple (2021-2022) — In 2021, Apple released a company-wide privacy-first approach. iPhone and iPad users can now determine whether they want to allow apps to track activity across other companies' apps and websites. Demonstrating the impact across the ecosystem, Facebook stated in February 2022 that Apple's privacy change will decrease Facebook's 2022 sales by about $10 billion.

h. Meta (Facebook) (2022) — As Facebook rebranded to Meta, the company was forced to contend with whistleblower allegations that Facebook/Meta failed to handle users' harmful behavior. Meta was subject to an additional whistleblower claim from a South African content moderator. Meta attempted to silence the whistleblower. These whistleblower allegations highlight the issues facing Meta as it contends with content moderation and how to handle users' harmful behavior and content, an issue facing the social media ecosystem at large.

i. *Meta* (Instagram) (2022) — In September 2022, Irish privacy regulators slapped Meta with a massive €405 fine under its GDPR enforcement authority in connection with Instagram's' processing of children's data for business accounts.

j. *Meta*, No. 18-md-02843-VC (2022-2023) — In a settlement signed in 2022, Meta agreed to a $725 million class action settlement over Facebook's longstanding privacy violations. The settlement is part of the ongoing fallout from Facebook's Cambridge Analytica scandal.

k. *Google*, No. 512-cv-04177-HRL (2023) — On January 5, 2023, Google agreed to pay $23 million to resolve a class action lawsuit based in California. The plaintiffs claimed that Google shared personal search queries with third party advertisers without permission, further alleging that marketers and advertisers paid Google to learn about customer click behaviors.

l. *T-Mobile*, No. 4:21-MD-03019-BCW (2023) — T-Mobile reached a settlement in June 2023 over the 2021 T-Mobile data breach. Under the settlement, T-Mobile agreed to pay affected consumers $350 million over the breach.

m. *TikTok*, FTC File No. 172 3004 (2024) – The Department of Justice, through a referral from the FTC, filed a lawsuit against TikTok and its parent company for multiple violations of COPPA and its implementing regulations, and the FTC. The complaint alleged that despite the court order that had been in place since 2019, TikTok continued to knowingly permit children under the age of 13 to create accounts and to create, view, and share short-form videos and messages with adults and others on the TikTok platform. TikTok also allegedly collected and retained a wide variety of personal information from children – including persistent identifiers that were used to build profiles and target advertising to them – without notifying parents or obtaining the legally required consent from them.

n. Self-Regulation — The self-regulatory Mobile Location Analytics Code of Conduct promotes consumer privacy and transparency in retail environments. It enumerates principles such as notice, limited collection, choice, limited retention, and consumer education. Entities engaged by retailers to deploy in-store tracking technology should take steps to ensure that such retailers display conspicuous signage informing consumers about the presence of location-based data collection. Signage should be connected to an opt-out mechanism, alerting consumers of their right to opt-out and decline permission for their mobile devices to be tracked for retail analytics.

Shopper Marketing and Deceptive Dark Patterns

a. Dark Patterns -- Since 2021, the FTC has been focused on "dark patterns" (or, design features used to deceive consumers into making purchases they otherwise would not, such as signing up for subscription services). The FTC issued an Enforcement Policy Statement Regarding Negative Option Marketing which—importantly—noted that under ROSCA sellers must obtain the

consumer's express informed consent before charging them for a product or service, *separately from any portion of the entire transaction*. The FTC staff also issued a report on dark patterns, noting that deceptive subscription practices, highlighting that:

- Dark patterns can obscure material terms (e.g., the fact that a free trial will convert to a paid subscription absent cancellation).
- Dark patterns can also mislead the consumer into providing consent by failing to disclose that the consumer is signing up for recurring charges (common among mobile apps that target children, who may believe that they are playing a game, as opposed to making an actual purchase).
- Dark patterns can discourage or prevent the consumer from canceling the subscription (by making it difficult to find the cancellation option or subjecting the consumer to additional promotions and offers prior to permitting cancellation).

i. FTC Enforcement

1. *Adobe*, FTC File No. 222 3055 (2024) – Upon notification and referral from the FTC, the Department of Justice filed a complaint against Adobe Inc, and two of its executives, alleging violations of ROSCA by failing to disclose the early termination fee for Adobe subscriptions. The complaint also alleges that Adobe uses the early termination fee to "ambush" consumers to dissuade consumers from canceling their subscriptions, and that Adobe's cancelation processes are designed to make the cancelation process difficult, requiring consumers to navigate multiple pages in order to cancel their subscription.
2. *Amazon*, FTC File No. 1910129 (2023) – The FTC has filed a complaint, which was amended in September of 2023, alleging violations of Section 5 of the FTC Act and ROSCA against Amazon for the use of "dark patterns" to deceive millions of consumers into enrolling in their Prime membership program including interface interference whereby Amazon used repetition and color to direct consumer attention to the words "free shipping" and away from the actual price of Prime. The FTC named Amazon leadership as individual defendants in the case, noting that they slowed or rejected changes that would have made it easier for users to cancel Prime because those changes adversely affected Amazon's bottom line. The FTC is seeking a permanent injunction to prevent future violations of the FTC Act and ROSCA as well as monetary relief.

3. *CRI Genetics*, No. 2:23-CV-9824 (C. D. Cal. Nov. 20, 2023) – The FTC and California Attorney General charged and settled with CRI Genetics, LLC over multiple claims, including that CRI used dark patterns in its online billing process to deceive consumers into purchasing additional products. The FTC alleges that CRI deceived customers into paying for products they did not want and did not agree to buy by confusing consumers with pop-up pages, promoting false "special rewards", trapping consumers by saying their order "was not complete". CRI also allegedly told consumers that they would have a chance to review orders before being charged, but then immediately charged for those orders. CRI was ordered to pay $700,000 in the settlement and is prohibited from misrepresenting when orders are complete, when charges will take place, and whether consumers can change their orders before being charged. Under the settlement, CRI is also required to disclose to consumers the total cost of all products, when they will be charged, and whether the consumer can confirm, edit, or delete products before they are charged.

ii. Government Regulatory Actions. State Attorneys General have been focusing on egregious violations:

1. *Sephora* (2022) — Settled with California AG for $1.2 million. The AG alleged that Sephora failed to provide its customers with sufficient notice of the sale of personal information; failed to provide a "Do Not Sell My Personal Information" link, as required by the CCPA; failed to provide two or more methods to opt-out of such sale; and, significantly, failed to process requests to opt-out via user-enabled Global Privacy Controls (GPC).

2. *Fareportal Inc.* (March 16, 2022) — The New York Attorney General, Letitia James, ordered travel website Fareportal to pay the state $2.6 Million at the conclusion of the state's investigation into Fareportal's practice of falsely claiming that there were a limited amount of air travel tickets available at the advertised price, the use of fake countdown clocks, and false claims that a specific number of consumers were currently looking at the same tickets.

iii. Self-Regulatory Enforcement. In 2023, the National Advertising Division recommended that Pier 1 Imports Online, Inc.'s practice of automatically adding a paid subscription-based customer loyalty program (Pier 1 Rewards) to a consumer's cart (as a pre-selected option) was misleading and recommended that material terms of the subscription be clearly and conspicuously disclosed.

DAVIS + GILBERT

I. Basics of Brand Activation

E-mail Marketing — The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)

a. This watershed law, passed in 2003, applies to all commercial electronic mail messages that include a commercial advertisement or promotion. The contents of the law have generally been unchanged over the past several years. CAN-SPAM requires that the sender of a commercial e-mail and the e-mail itself comply with the following requirements: (1) the "From" "To" and "Subject" lines must be accurate and not misleading; (2) the message must be identified as an advertisement; (3) a clear and conspicuous explanation of how the recipient can opt-out (unsubscribe) must be included and the opt-out must be honored within ten business days; (4) a physical postal address must be included; (5) the sender must monitor that any third parties engaged by the sender are also complying with CAN-SPAM.

Note that CAN SPAM defines a "commercial message" as one with a primary purpose of commercial advertisement. Messages containing both advertising and transactional or informational content have a commercial primary purpose if: (i) the recipient would interpret the subject line to mean that the message contains commercial advertising; or (ii) determine from the body of the message that the message's primary purpose is commercial advertising (e.g., if the commercial advertising is at the beginning of the message, is the majority of the message, or otherwise is very prominent).

CAN-SPAM generally preempts state laws that also govern spam e-mail or other commercial electronic messages. Each separate e-mail sent in violation of CAN-SPAM may be subject to penalties of up to $16,000.

i. In August 2023, the U.S. DOJ and the FTC entered into a settlement with Experian Consumer Services to resolve allegations that Experian sent marketing emails disguised as transactional or informational messages in violation of CAN-SPAM. The settlement required Experian to pay $650,000 and be subject to injunctive provisions prohibiting similar practices in the future.

ii. In December of 2019, the FTC settled a complaint against Effen Ads, LLC and an affiliate marketing network, W4 LLC. Effen Ads and W4 promoted a work-from-home scheme by sending emails with misleading "from" lines (indicating that they were sent by news organizations such as CNN and Fox News) and "subject" lines. The emails themselves linked to fake news stories and celebrity endorsements. The CEO of W4 agreed to pay $1.3 million and is permanently banned from marketing work-from-home

programs. The owners of Effen Ads agreed to pay $25,000 and $121,948 (as satisfaction of a suspended $11.3 million judgment), respectively, and are permanently banned from marketing business opportunities or business coaching products.

iii. In February of 2019, the FTC completed a review of its rule implementing CAN-SPAM and voted unanimously to keep the rule in effect as-is. As part of its review process, the FTC reviewed 92 public comments.

iv. In June of 2018, the FTC settled a challenge against Mobile Money Code, a company that advertised "get rich quick" schemes through e-mail marketing. In addition to the false and deceptive claims aspect, the FTC alleged multiple violations of CAN-SPAM. The FTC says the Mobile Money Code's CAN-SPAM violations included using deceptive header and subject lines, failing to identify email as an ad, failing to include a valid physical address, and failing to give recipients a way to opt out of future messages. The violators are also subject to a lifetime ban on further e-mail marketing activities.

v. In August 2015, the FTC did a "question and answer" session which clarified several recurring questions about CAN-SPAM. Among other things, the FTC reiterated that the identification of an e-mail as commercial does not have to appear in the subject line, that CAN-SPAM does not contain an "opt-in" requirement, and that cell phone spam can fall under CAN-SPAM if it relates to unwanted commercial messages referencing an internet domain name assigned by wireless carriers for delivery to a subscriber's cell phone.

Canada's Anti-Spam Legislation (CASL)

a. In 2014, Canada initiated strict new requirements for sending commercial messages that include a requirement that solicitors have at least implied consent. Express consent has been required since 2016, and as of July 2017 marketers, can no longer rely on "transitional implied consent" stemming from pre-2014 relationships with customers. Moving forward, implied consent is only valid in a limited number of circumstances, such as when the recipient has made a purchase from the company in the two years prior to the message, when the recipient has an existing written contract with the sender, or certain other existing business relationships. The express consent requirement can be satisfied orally or in writing, and all commercially messages require identification information and an unsubscribe mechanism. The law may apply to commercial electronic messages sent to or from a computer system located in Canada.

b. In January 2015, Canada rolled out the requirements under CASL regarding installing computer devices on customer systems. CASL prohibits the installation of computer programs on another person's computing device (which is read broadly to include smartphones, gaming consoles and other connected devices) in the course of commercial activity without the owner's express consent. This severely restricts automatic installation of software by websites and automatic update (however, it does not apply to cookies or HTML). Installers can obtain express consent by "clearly and simply" notifying customers of (i) who they are and how they can be contacted (ii) the reason they are seeking consent, (iii) a statement indicating that consent can be later withdrawn and (iv) a general description of the functions and purpose of the program to be installed.

c. CASL provided for a private right of action that would have allowed lawsuits to be filed against individuals and organizations for alleged violations. These provisions were scheduled to come into force on July 1, 2017. However, based on broad-based concern from business, charities, and non-profit organizations, the Canadian government has postponed the private right of action until an as-yet unknown future date.

d. In June of 2020, the Canadian Federal Court of Appeal upheld the constitutionality of CASL.

e. In September of 2020, the Canadian Radio-television and Telecommunications Commission (CRTC) entered into a $100,000 settlement with OneClass, an online educational platform. According to the CRTC, OneClass sent promotional messages without obtaining consent from the recipients and installed a Chrome extension on its users' computers case without obtaining consent from those users.

f. In January 2022, the CRTC penalized four Canadian individuals a total of $300,000 for allegedly sending fraudulent emails mimicking well-known brands to obtain sensitive personal information in connection with a dark web marketplace known as "Canadian Head Quarters."

g. In October 2023, the CRTC penalized a Quebec resident $40,000 for conducting a high-volume phishing campaign in violation of CASL's prohibition against sending commercial electronic messages without consent.

Calling and Texting Campaigns

The federal government regulates phone calls and text messages from companies to consumers through the Telephone Consumer Protection Act, 47 U.S.C. § 227 (TCPA) and accompanying regulations, which are enforced by the FCC, and the Telemarketing and Consumer Fraud and Abuse Prevention Act (the Telemarketing

Act), 15 U.S.C. §§ 6101-6108 and accompanying regulations, including the Telemarketing Sales Rule (TSR), 16 C.F.R. §310, which is enforced by the FTC. Both the TCPA and TSR apply to telephone calls and text messages. Many states also have their own applicable laws and regulations.

a. Telephone Consumer Protection Act

The TCPA is a federal statute that: (i) regulates and restricts the use of automated technology to initiate outbound phone calls (both informational and marketing calls) and (ii) applies to voice calls, voice messages, AI-voice messages, SMS text messages and faxes. The TCPA does not regulate inbound telephone calls.

The TCPA requires consent for certain types of automated calls, including text messages, to residential landlines and mobile phones. The level of consent that's required may vary depending on whether a business is calling a residential landline or a mobile telephone.

The level of consent that's required also varies depending on if the outbound call or text is informational, or telemarketing. Generally, informational communications have fewer restrictions than telemarketing messages, but the line between the two types of content is not always clear.

- Informational communications require prior express consent (oral or written). Prior express consent is evidenced by showing that: (i) The text message recipient voluntarily provided their phone number; and (ii) The communication is within the scope of consent provided by the text message recipient.
- Telemarketing communications require prior express written consent. This has very strict requirements, including: indicating an affirmative agreement (i.e., I agree/consent); obtaining the signature of the person who will be called (this can be done electronically); specifying the phone number at which the consumer is consenting to receive promotional calls; including a statement that the consumer is authorizing the caller to deliver telemarketing messages via automated means; and including a statement that the consumer is not required to consent or agree to the consent request as a condition of purchasing any property, goods, or services.

The TCPA imposes more than consent requirements. It requires that: (i) telemarketing calls only be made between 8:00 AM and 9:00 PM; (ii) the telemarketer disclose the name of the caller, name of the person or entity on whose behalf the call is being made and a telephone number or address at which the person or entity may be contacted; (iii) caller ID must include calling

party number identification or automatic number identification that is answered during normal business hours and where technologically possible, the name of the advertiser; and (iv) telemarketers may not call any telephone numbers listed on the federal Do Not Call Registry. The FCC also prohibits initiating any telephone solicitation to a residential telephone subscriber unless the person or entity has instituted procedures for maintaining its own internal list of people who do not wish to receive telephone solicitations made by or on behalf of that person or entity.

It is worth noting that the TCPA permits private lawsuits by consumers against telemarketers, with damages of up to $1,500 *per violation*. Consumer class actions under the TCPA are frequent, and companies routinely enter into settlements for tens of millions of dollars. Note that state laws apply and may have more restrictive requirements.

The FCC recently made several critical changes to the TCPA, including:

- Clarifying that consumers can revoke consent at any time, through any reasonable means.
- Requiring that opt-out requests be honored within 10 business days.
- Requiring that consent be provided "one to one," meaning that consumers can only give prior express written consent to a single seller at a time, and calls must be "topically or logically" related to the transaction giving rise to the consent.

b. Telemarketing Sales Rule

The TSR, which was created to prohibit deceptive and abusive telemarketing practices, regulates the sale of goods and services through interstate phone calls. The TSR applies to both telemarketers and the sellers on whose behalf the calls are made. The TSR requires that (i) telemarketing calls only be made between 8:00 AM and 9:00 PM; (ii) the telemarketer promptly disclose the identity of the seller, that the purpose of call is to sell goods or services, and the nature of the goods or services; (iii) the telemarketer disclose other relevant issues, such as cost, quantity, material restrictions, limitations or conditions, refund policies, and prize promotion disclosures; (iv) caller ID must include the phone number of the seller or service bureau or the customer service number that will be answered during normal business hours and, if technologically possible, the name of the seller or service bureau; and (v) telemarketers may not call any telephone numbers listed on the federal Do Not Call Registry. The FTC states that it is an abusive telemarketing act or practice and a violation of the TSR to initiate an outbound telephone call to a person when that person previously has stated that he or she does not wish to receive an outbound

telephone call made by or on behalf of the seller. Note that state laws apply and may have more restrictive requirements (including around calling times).

The FTC recently revised the TSR in part to require that sellers and telemarketers maintain additional records of telemarketing transactions, and prohibit material misrepresentations and false or misleading statements in business to business (B2B) telemarketing calls.

c. Recent Telemarketing and Text Message Marketing Developments

i. Autodialers

In April 2021, the U.S. Supreme Court helped resolve a circuit split regarding how broadly to define the types of automated technology regulated under the TCPA led to this case. In *Facebook Inc. v. Duguid*, the Supreme Court narrowly construed the definition of an automatic telephone dialing system, or autodialer, under the Telephone Consumer Protection Act (TCPA).

Under the TCPA, autodialers are defined as "equipment which has the capacity to store or produce telephone numbers to be called, using a random or sequential number generator; and to dial such numbers."

The Court held that "Congress' definition of an autodialer requires that in all cases, whether storing or producing numbers to be called, the equipment in question must use a random or sequential number generator." In other words, equipment that can store and dial telephone numbers, but does not use a random or sequential number generator does not constitute an autodialer.

ii. State Laws Developments

Note that there are a number of state laws that govern outbound communications, colloquially known as "mini-TCPA" statutes. Notably, in 2021 Florida has amended its Do Not Call Act and Florida Telemarketing Act to require the prior express written consent (PEWC) of the called party to make a "telephonic sales call" involving "an automated system for the selection or dialing of telephone numbers or the playing of a recorded message when a connection is completed." The amended law also requires PEWC to use an automated system to make telephonic sales calls, even if in response to consumers who had initiated the call (e.g., via a call to action) or where a consumer had previously purchased a product from the business. An amendment to the Florida Telephone Solicitation Act (FTSA) in May 2023 narrowed the categories of equipment that are covered by the statute (while still including the transmission of a prerecorded voicemail), expanded the definition of "signature" to allow acts such as checking a box, and created a 15-day notice and cure period before a plaintiff can file suit in text message

cases.

Throughout 2021 and 2022, there has been a wave of lawsuits brought under the FTSA largely because it has a more expansive definition of an autodialer than the federal TCPA.

In 2022, Washington and Oklahoma also passed new "mini-TCPA" laws. The Washington law is more limited than Florida's, but governs "telephone solicitation," defined as an "unsolicited initiation of a telephone call … for the purpose of encouraging the person to purchase property, goods, or services or soliciting donations[.]" The Oklahoma law largely tracks the FTSA—it applies to telephonic sales calls that involve "an automated system for the selection or dialing of telephone numbers or the playing of a recorded message when a connection is completed to a number called." Like Florida, an "automated system" under the Oklahoma law is not limited to equipment that would qualify as an autodialer under the federal TCPA. Several other states are moving to enact similar legislation.

Additional states have followed with more mini-TCPA laws. Maryland's Stop the Spam Calls Act mirrors the initial language of the FTSA (that resulted in a deluge of suits) and took effect in January 2024.

Mobile Marketing Guidelines

Mobile marketing incorporates advertising on mobile devices, including in mobile applications, and is device neutral (e.g., covers smartphones, tablets and other personal devices). General advertising guidelines apply to mobile marketing. The federal government regulates mobile marketing through the Federal Trade Commission Act (FTC Act), Children's Online Privacy Protection Act (COPPA) and the regulations promulgated thereunder. 15 U.S.C. §§ 41-58; 5 U.S.C. §§ 6501-6505. Mobile marketing of prescription pharmaceuticals is also regulated under the Federal Food, Drug and Cosmetics Act (FDCA). 21 U.S.C. § 301 *et seq*. Mobile marketing is also self-regulated through the Digital Advertising Alliance (DAA) and other trade groups, including the National Advertising Initiative (NAI).

a. FTC Act

   i. The FTC's prohibition on "unfair and deceptive acts" applies to mobile marketing. Disclosures in online and mobile advertising should be clear and conspicuous.

b. COPPA

   i. Mobile marketers that operate websites and apps directed to children or that operate websites and apps with actual knowledge that they are collecting the personal information of children are required to comply with

COPPA. COPPA requires mobile marketers to obtain verifiable parental consent before collecting, using, or disclosing the personal information of children under thirteen years of age.

c. FDA

   i. The Food and Drug Administration's general advertising guidelines for prescription pharmaceutical advertising apply in the context of mobile marketing. Marketers must present risk information "comparable in content and prominence" to the benefit claims. Marketers may provide truthful and non-misleading corrective information in response to the misinformation posted by third parties. However, marketers may not respond to the misinformation by providing promotional materials about the product.

d. Wiretapping Laws

   i. There has been a significant number of class action lawsuits filed in California, where class action lawyers have been bringing claims under the California Invasion of Privacy Act ("CIPA") against websites and mobile apps that use chat bots and similar features to engage with consumers; alleging that doing so involves intercepting communications without consent under the CIPA. In the recent case *Javier vs. Assurance IQ, LLC and Active Prospect, Inc*., the 9th Circuit interpreted CIPA, holding that retroactive consent is insufficient – website operators should obtain targeted consent *before* using tools like chat bots or other interactions that may be subject to the statute. Section 631(a) of CIPA prohibits (1) intentional wiretapping, (2) willfully attempting to learn the content of communications in transit, and (3) attempting to use or communicate information obtained through the first two prohibitions. In the *Javier* case, the plaintiff visited an insurance website that used a product to record users' interactions with the site. Before requesting an insurance quote, the plaintiff answered a series of demographic and medical history questions – a process that was recorded in real time by the site's "TrustedForm" feature. The *Javier* plaintiff was not prompted to accept the company's privacy policy until after the recording. The court ruled that CIPA requires prior express consent of all parties – retroactive consent, as in the *Javier* case, is not sufficient. While the court in *Javier* did not address what valid consent may have looked like, the court confirmed that retroactive or implied consent are insufficient under CIPA. Importantly, the *Javier* ruling is limited in scope. The ruling simply reversed the lower court's decision that retroactive consent defeated the plaintiff's CIPA wiretapping claim, sending the case back down to the lower court. In a footnote, the 9th

Circuit explained that the plaintiff's claim should be dismissed on other grounds, including that the website operator could not have wiretapped its own website, as it was a party to the communication involved.

e. DAA

   i. The DAA has promulgated Self-Regulatory Principles for Online Behavioral Advertising and Self-Regulatory Principles for Multi-Site Data ("DAA Principles") as well as three supplementary guidance documents: Application of Self-Regulatory Principles to the Mobile Environment (the "Mobile Environment Guidance"), Application of the DAA Principles of Transparency and Control to Data Used Across Devices (the "Cross Device Guidance"), and Application of the DAA Principles of Transparency & Accountability to Political Advertising (together with the Mobile Environment Guidance and the Cross Device Guidance, the "DAA Guidance"). The DAA Principles and DAA Guidance apply to app and website owners and controllers and third parties that collect certain data through non-affiliated web sites and devices, including data collected from a particular device for use on a different device. The DAA Principles and DAA Guidance impose transparency, notice (including "enhanced" or "just-in-time" notice where information is collected for interest-based advertising purposes) and consumer control requirements with respect to the collection, use and/or transfer of cross-app data, precise location-based data, personal directory data and multi-site data, subject to some exceptions. The DAA Principles and DAA Guidance generally prohibit the collection and use of such data (i) that includes financial account numbers, Social Security numbers, and non-de-identified pharmaceutical prescriptions or medical records (except for operations or systems management purposes) and (ii) for employment eligibility, credit eligibility, health care treatment eligibility or insurance eligibility or underwriting or pricing. Entities are also required to maintain appropriate safeguards to protect such data.

f. NAI

   i. The NAI Code of Conduct released in 2020 represented "the most comprehensive overhaul of the NAI's self-regulatory requirements since the release of the original Code of Conduct in 2000." The 2020 Code of Conduct extends NAI coverage to digital advertising technologies as well as reinforcing existing requirements with respect to the collection and use of data for digital advertising. The Code of Conduct imposes transparency, notice, user control (including opt-out/opt-in mechanisms), and data security and retention requirements on NAI members with respect to

cross-app advertising, ad delivery and reporting and interest-based advertising. Furthermore, the Code of Conduct formalizes restrictions around the use of data originating offline to target ads across websites, mobile applications, TV screens, and other devices; expands requirements relating to the use of precise location information; and imposes restrictions around the collection and use of sensor information, including microphone, camera, or any sensor that collects biometric data.

g. Enforcement

   i. The Digital Advertising Accountability Program ("DAAP") has been actively handling mobile enforcement actions for the last ten years, enforcing the DAA Principles with a particular focus on enhanced transparency, consumer choice in interest based advertising, and mobile device enforcement. The Accountability Program has now issued over 120 decisions since its inception in 2011.

Charitable Solicitation Laws

In recent years, great social upheaval, economic distress, and multiple environmental catastrophes have motivated marketers to support charitable causes like never before.

Cause marketing refers to promotional campaigns offered by for-profit companies in cooperation with non-profit corporations, which represent to the public the purchase or use of the for-product company's products is to provide some benefit to the mission of the non-profit. For example, in light of the drastic loss of jobs in the service sector during the COVID-19 pandemic lockdowns in 2020, many beer, wine, and liquor companies announced charitable partnerships intended to benefit restaurant and bar workers.

And while the FTC has stressed the importance of disclosure in connection with cause marketing and other charitable solicitation campaigns, the majority of not-for-profit governance is done by the states. To determine which state laws may apply to a particular charitable-related campaign, not-for-profit corporations, as well as the for-profit companies working with them or soliciting donations on their behalf, should generally look at (a) where such entities are registered or doing business, and (b) where they are soliciting donations. The type and amount of activity that triggers state registration requirements for charities and the organizations doing business with them varies by state. In light of the particular difficulties of determining "connection" with a state in online-only solicitation, the National Association of State Charity Officials (NASCO) released a set of guidelines in 2001, titled The Charleston Principles. These Principles suggest that an out-of-state organization soliciting contributions through an interactive website (i.e., a website

that processes online donations), should register in a particular state if the organization either: "(i) Specifically targets persons physically located in the state for solicitation, or (ii) Receives contributions from the state on a repeated and ongoing basis or a substantial basis through its Web site." *The Charleston Principles at Section III(B), available at http://www.nasconet.org/wp-content/uploads/2011/05/Charleston-Principles-Final.pdf*.

Cause marketing and commercial co-ventures continue to be scrutinized by state AGs. For one, major natural disasters create an easy opportunity for illegitimate non-profits to solicit money from unwitting individuals hoping to donate to disaster relief. For reasons such as this, regulators remain vigilant about investigating non-profits and ensuring that commercial co-ventures are in compliance with law. In this process, regulators often uncover seemingly legitimate co-ventures that are not in compliance with law. For example, in 2023, the Minnesota Attorney General filed an Assurance of Discontinuance that prohibited a Minnesota physician and his practice from soliciting contributions for a charity that did not exist and falsely claiming that the fees paid to his clinic benefited charity and were tax-deductible. In 2020, the New York Attorney General issued a cease-and-desist order against the Black Lives Matter Foundation, an organization that accepted over $4 million in donations intended to address racial injustice in America, even though it had no affiliation with the Black Lives Matter movement. Similar actions have been brought against charities intending to benefit hurricane and wildfire victims. Similarly, in 2018 a seemingly legitimate partnership between Harris Jewelry (a retailer) and Operation Troop Aid (a non-profit) was investigated and the non-profit ultimately shut down for failure to comply with state law, in part due to the fact that the donations made by Harris Jewelry failed to match what was advertised.

a. Cause Marketing Requirements for the Commercial Co-Venturer

    i. While the definition of "commercial co-venturer" varies among the states that actively regulate such entities, in general, commercial co-venturer statutes pertain to for-profit entities, which represent that the purchase or use of goods or services offered by the commercial co-venturer will benefit, in whole or in part, a charitable organization. In certain states, this model applies when the for-profit entity conducts any type of event that is advertised in conjunction with the name of a charitable organization. *See*, *e.g.*, Ala. Code § 13A-9-70(4); Cal. Bus. & Prof. Code § 12599.2(a); Ga. Code Sec. 43-17-2(5); M.G.L.A. 68 § 18; N.Y. EXEC. LAW § 171-a; T.C.A. § 48-101-501(2).

    ii. Use of a commercial co-venturer for a promotion in a state may trigger registration and/or bonding requirements on the part of both the charity and the co-venturer. *See*, *e.g.*, Ala. Code § 13A-9-71(h) (requiring a

registration form, $100 filing fee, and $10,000 bond); Cal. Bus. & Prof. Code § 12599.2 (exempting co-venturers who enter a contract signed by two officers of their charity, transfer all funds earned every 90 days during a campaign, and provide a full accounting with each transfer from otherwise-applicable registration requirements).

iii. The commercial co-venturer statutes commonly require that charitable organizations and commercial co-venturers execute a written contract or agreement prior to engaging in any charitable advertising or sales promotion. In general, these contracts should include: (i) a statement describing the purpose of the promotion; (ii) the time period within which the promotion will take place; (iii) the per-unit amount of money that the charitable organization will receive; (iv) the manner in which the charitable organization's name will be used and (v) the date and manner by which the proceeds will be transferred to the charitable organization. *See, e.g.*, N.Y. EXEC. LAW § 174-a (requiring that certain statements and information be included in a contract between the co-venturer and charitable organization).

iv. Many of the state commercial co-venturer laws also contain advertising and marketing disclosure requirements. The advertising/disclosure requirements break down roughly into two (2) categories: (i) those requirements that relate specifically to advertising distributed by commercial co-venturers; and (ii) those requirements that relate to all "solicitations" in the state. *See*, *e.g.*, Ark. Code § 4-28-408(c); M.G.L.A. 68-23; N.J. STAT. § 45:17A-29(d). As a general matter, in order to comply with the requirements relating to commercial co-venturers in each state, commercial co-venturers need to make the following disclosures in their advertising materials: i) Name, address and phone number of charitable organization; ii) Charitable purpose for which the funds will be used; iii) How to obtain more information about the charitable organization's financial filings; iv) Per unit dollar amount or percentage of purchase price that will be donated to the charitable organization (if this amount is not known, it should be estimated); v) The percentage of the purchase price that is tax deductible to the purchaser or a statement that "This purchase is not tax deductible"; and vi) The name of the commercial co-venturer.

v. In addition, many of the state charitable solicitation statutes, the term "solicitation" is defined broadly enough to cover offers made by commercial co-venturers. Therefore, in order to comply with the "solicitation" disclosures required by each state, the commercial co-venturer would need to include the specific information required by that state for "solicitations".

b. Cause Marketing Requirements for the Charitable Organization

i. Most states require that a charitable organization file a registration statement prior to soliciting contributions within that state. In connection with the charitable organization's initial and/or annual filing with the state, certain states require that the charitable organization disclose specific information (including name, address, telephone number, email address) regarding any commercial co-venturer who conducted a sales promotion on behalf of the charitable organization.

1. As of June 12, 2024, businesses who solicit charitable contributions – including "round up" or donate-at-checkout programs – will need to register in California. Businesses that promise donations based on user purchases or activities may also need to register.

ii. Certain states require that the charitable organizations' annual financial reports include information regarding the amounts received from each commercial co-venturer used by the charitable organization. In addition to the foregoing requirements, many states require that the charitable organization obtain a written agreement from the commercial co-venturer and file a copy of such agreement (or similar information) with the state prior to the commencement of the applicable sales promotion.

c. Professional Fundraiser

i. A professional fundraiser is usually distinguished from a commercial co-venturer in that it directly solicits donations on a charitable organization's behalf (in exchange for compensation) and will not usually do so by offering goods or services; individuals or organizations who plan or manage fundraising campaigns may also be counted as professional fundraisers. See, e.g., MCL 400.272; N.M. STAT. § 57-22; R.I. Gen. Laws § 5-53.1-1(10). Professional fundraisers may be subject to bonding, registration, and disclosure requirements similar to those applied to commercial co-venturers.

Negative Option, Buying Clubs, Automatic Renewal and Free Trial Offers

a. Negative Option, Buying Clubs, Automatic Renewal and Free Trial Offers

Under negative option plans, sellers ship merchandise or provide services automatically to their subscribers, and bill them for the merchandise or services if they do not expressly reject them within a prescribed time. Negative option plans are governed by the FTC's Negative Option Rule.

In October 2024, the FTC released significant revisions to the Negative Option Rule, which expand the scope of the rule from prenotification plans (e.g., book-

of-the-month and record clubs) to virtually all negative option offers in all forms of media (e.g., telephone, internet, print media and in-person transactions. Importantly, the revised Negative Option Rule:

- Requires disclosure of all material terms upfront, including charges, cancellation deadlines and renewal terms.
- Requires that a cancellation mechanism be as simple to use – in terms of time, burden, expense, ease of use, and the like – as the enrollment mechanism.
- Prohibits sellers from making any material misrepresentations about any aspects or facts related to a negative option transaction (which would include claims about the product).

In the wake of *Loper Bright*, it is possible that the Negative Option Rule may be challenged, and implementation delayed. Several industry groups have already challenged the new Rule in federal court.

Negative option plans are also governed by state laws. California's automatic renewal law is a generally restrictive law, and in part requires e-commerce sellers doing business in California to provide notice to consumers prior to any free gift or trial offer expires, and requires that a consumer be able to cancel online without taking "any further steps that obstruct or delay the consumer's ability to terminate the automatic renewal or continuous service immediately." California recently amended this law, and effective January 1, 2025, will require that:

- Companies obtain consumers' "express affirmative consent" to the automatic renewal and keep a record of such consent for three years or one year after the contract is terminated, whichever is longer.
- Permit consumers to cancel their subscriptions "in the same medium" that the consumer used to enter the autorenewal.
- Permit businesses to present a consumer with a "save" offer (such as a discount or other retention benefit) under limited circumstances. Online, companies are permitted one save attempt, provided that the business simultaneously displays "a prominently located and continuously and proximately displayed direct link or button" clearly allowing the consumer to cancel.

Although private suits have been brought under California's law over the years, in September of 2020, a California appellate court ruled that there is no private right of action under the state's automatic renewal law, stating that the text of the statute did not provide "a clear indication" that a private right of action is

allowed under the automatic renewal statute. Now, plaintiffs will be only be allowed to enforce California's automatic renewal law through other remedial laws, such as California's Unfair Competition Law, which only allows claims by those who have suffered financial or property losses.

Many other states enacted or updated automatic renewal laws recently. Although these laws are similar in certain respects to California's automatic renewal law, the Vermont, Delaware, and D.C. laws do contain certain important distinctions from the California law. The Vermont, Delaware, and D.C. laws require that companies issue consumers a 30–60-day notice prior to renewals of 12 months or more (while California's current law is silent on this point). Vermont's law has been interpreted to require (i) automatic renewal terms for a subscription term of 12 months or longer be in **bold face type**, and (ii) that consumers must affirmatively opt in to automatic renewals in addition to accepting the underlying contract/full terms. Under Colorado law, consumers on monthly automatically renewing plans must be provided notice prior to the anniversary (and each subsequent anniversary) of their subscription.

b. FTC $8.5 million settlement with Care.com

In August 2024, the FTC took action against Care.com, alleging that the platform used inflated job numbers and unsubstantiated earnings claims to "lure" caregivers onto its platform and that it further "used deceptive design practices to trap consumers in subscriptions" they could not easily cancel. are agreed to a settlement that requires it to turn over $8.5 million in consumer restitution, as well as to cease future deceptive earnings claims and to provide users with a simple cancellation method for any negative option subscriptions available on the site.

c. FTC Complaint against Amazon

In 2023, the FTC filed a complaint against Amazon alleging that the company engaged in "dark patterns" to trick millions of consumers into enrolling in their Prime membership program. The FTC specifically cited Amazon's failure to provide simple cancellation mechanism as a Restore Online Shoppers' Confidence Act (ROSCA) violation, stating that the company "fails to provide simple mechanisms for a consumer to stop recurring charges for the good or service to the consumer's credit card, debit card, bank account, or other financial account." Echoing its "click to cancel" and "mirror cancellation" updates to the Negative Option Rule, the FTC highlighted Amazon's "knowingly complicated cancellation process."

d. FTC settlement with ABCmouse for $10 million over Negative Option Subscriptions

In September of 2020, the FTC settled with Age of Learning, Inc. d/b/a ABCmouse, an online learning tool that offers memberships to its online content, over multiple allegations, including that ABCmouse failed to disclose that such memberships would renew automatically. The FTC also alleged that ABCmouse offered a "free trial" membership, but did not disclose that at the end of the free trial, the membership would automatically renew. As part of the settlement, ABCmouse agreed to pay the FTC $10 million and is required to make certain disclosures in connection with its negative option offers and to offer customers a simple mechanism to cancel their subscriptions.

Practice Tips

These cases serve as an important reminder to advertisers to "give clear, honest information about charges," Jessica Rich, Director of the FTC's Bureau of Consumer Protection, said in a statement about the Bunzai case. "If a company advertises a 'risk-free trial,' then that's what it must provide."

The general FTC guidance on clear and conspicuous disclosures apply in the context of negative option and buying clubs (including where offering consumers services such as meal kits and cleaning services), as well: the consumer must understand if and when he or she is enrolling in a membership or subscription and subject to continual charges. Such terms should not be hidden in fine print or require additional charges or unreasonable efforts by the consumer to un-enroll.