Online Advertising and Marketing: Overview (US)

by Hannah Taylor, Terri Seligman, Dorian Slater Thomas, and Daniel Goldberg, Frankfurt Kurnit Klein & Selz, P.C.

Practice note: overview | Law stated as of 01-Aug-2023 | United States

A Practice Note providing an overview of the legal issues surrounding online advertising and marketing in the US. This Note considers issues like disclosures and privacy concerns and addresses specific forms of online advertising and marketing, including company websites, online behavioral advertising, social media, native advertising, and influencer marketing.

Given the explosive growth of digital media, online advertising and marketing has become a critical means for businesses to advertise and market their goods and services. The general advertising and marketing legal principles that apply to traditional media (like television, print, and radio) also apply to the online world. However, the digital space poses unique legal challenges and risks.

This Note focuses on the legal issues specifically related to the online conduct of advertising and marketing in the US. It is intended be a broad overview of the issues raised. Although email marketing takes place digitally, it is a form of direct marketing and is covered in Practice Note, Direct Marketing in the US: Overview.

This Note discusses:

- The legal framework governing online advertising and marketing.
- Key legal issues raised by recognizing company websites as advertising, including certain online tactics related to enhancing and driving traffic to websites like:
    - linking;
    - framing and embedding;
    - search engine optimization, including use of metatags and keywords; and
    - affiliate marketing.
- Key legal issues raised by other specific types of online advertising and marketing, including:
    - online behavioral advertising and other targeted advertising;
    - social media;
    - user-generated content (including consumer reviews);
    - native advertising; and
    - influencer marketing.

This Note also provides tips and best practices for engaging in online advertising and marketing.

Legal Framework for Online Advertising and Marketing

Online advertising and marketing is subject to an array of laws and regulations. In addition to the fundamental laws governing advertising and marketing in traditional media, advertisers must comply with data privacy laws and regulations and other restrictions peculiar to the digital space.

Fundamental Advertising Principles

The same federal consumer protection laws that apply to traditional types of advertising and marketing materials, like Section 5 of the Federal Trade Commission Act (FTC Act) which prohibits unfair and deceptive trade practices, also apply to advertisements appearing online, including in social media and on mobile devices. Therefore, on the internet and on mobile devices, like elsewhere:

- Advertising must be truthful and not misleading.
- Advertisers must have evidence to substantiate the claims made in their advertising prior to disseminating the advertising.
- Advertisements cannot be unfair.
- All disclosures that are required to prevent an advertisement from being misleading must be clear and conspicuous.

To ensure that advertisers understand how to make clear and conspicuous disclosures in online advertising, the Federal Trade Commission (FTC) issued guidelines, .com Disclosures: How to Make Effective Disclosures in Digital Advertising (.com Disclosure Guidelines). The .com Disclosure Guidelines address issues specific to the internet and mobile marketplace, like:

- Scrolling.
- Hyperlinks.
- Space-constrained mobile screens.
- Character limitations in social media.

The .com Disclosure Guidelines help businesses evaluate whether disclosures are likely to be clear and conspicuous in online advertisements and use a series of mock ads to illustrate certain areas of concern. According to the guidelines, when businesses are evaluating online ads they should consider whether:

- The placement of the disclosure is as close as possible to the claim it is qualifying.
- The disclosure is prominently displayed by evaluating its size, color, and graphic treatment in relation to other parts of the web page.
- The items in other parts of the ad, like moving graphics or other visual elements, distract attention from the disclosure.
- The ad is so lengthy that the disclosure needs to be repeated.

- The disclosures in audio messages are presented in an adequate volume and cadence and visual disclosures appear for a sufficient duration.
- The language of the disclosure is understandable to the intended audience (for example, using the word "Ad" at the beginning of a Tweet, as opposed to "Spon," which consumers might not recognize as shorthand for "sponsored").
- The disclosure is unavoidable, meaning the consumer cannot proceed with a transaction without scrolling through the disclosure.
- Consumers can enter the site at different locations or travel through the site on paths that may cause them to miss the disclosure.

In addition to providing these evaluative factors, the .com Disclosure Guidelines state that:

- Disclosures must be clear and conspicuous on all devices and platforms on which consumers will view the ad, for example in a mobile-optimized version.
- If disclosure cannot be made clearly and conspicuously on a device or platform, that device or platform should not be used.
- The use of pop-up disclosures should be avoided unless certain precautions are taken.
- Use of hyperlinks to disclosures should be avoided, but if a hyperlink is necessary, advertisers should:
    - make the hyperlink obvious and as close as possible to the relevant ad claim;
    - label the hyperlink as specifically as possible to convey the importance of the information it leads to;
    - use hyperlink styles consistently so that consumers know when a link is available;
    - take consumers directly to the disclosure on the click-through page;
    - assess the effectiveness of the hyperlink by monitoring click-through rates and make changes accordingly; and
    - consider how hyperlinks will function on various programs and devices.

(See .com Disclosures: How to Make Effective Disclosures in Digital Advertising.) Note that the FTC has announced that it plans to update the .com Disclosure Guidelines and is seeking public comment.

The FTC has also published a guide for mobile app developers intended to help mobile app developers observe truth-in-advertising and basic privacy principles. For more information, see FTC: Marketing Your Mobile App: Get It Right from the Start.

For additional information on advertising laws in the US, see Country Q&A, Advertising in the United States: Overview.

Data Privacy Laws

Because online advertising and marketing frequently involve the collection, use, and sharing of consumer personal information, data privacy laws and regulations play an important role. Social media platforms and tracking technologies such as cookies and pixels allow advertisers to collect personal information about consumers. Advertisers that integrate with social media platforms,

deploy tracking technologies, or otherwise collect personal information need to disclose their information collection practices in compliance with state and federal laws, and in some cases international law.

The US does not have a national comprehensive privacy law. Instead, a patchwork of federal laws protect individual data privacy issues like children's privacy and privacy of health information. In the absence of a comprehensive federal law, the states have begun to pass their own privacy laws. The FTC also uses its authority under Section 5 of the FTC Act to provide guidance on privacy issues and bring enforcement action against companies that do not honor their privacy promises. All of these initiatives affect the collection, sharing, and use of consumer data in connection with online advertising and marketing.

Furthermore, companies in possession of consumers' personal information are required by state and federal laws to implement reasonable physical, technical, and administrative safeguards to prevent the unauthorized access, acquisition, exfiltration, theft, or disclosure or personal information.

For more information on privacy laws in the US, see Practice Note, US Privacy and Data Security Law: Overview.

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6501 to 6506) applies to the collection of personal information from children under the age of 13. COPPA requires, in part, that commercial websites and online services (including mobile apps) directed to, or that knowingly collect information from, children under 13:

- Post a privacy notice on their sites informing parents about their policies and practices regarding their collection, use, and disclosure of personal information from children.
- With certain statutory exceptions, obtain verifiable parental consent before collecting, using, or disclosing personal information from children.
- On request, provide parents of children who have given personal information with a description of the types of personal information collected, an opportunity to prevent any further use or collection of information and reasonable means to obtain the specific information collected.
- Maintain procedures to ensure the confidentiality, security, and integrity of the personal information collected.

The FTC has issued a rule to implement COPPA (COPPA Rule). The COPPA Rule provides requirements for businesses to comply with COPPA. For example, the COPPA Rule:

- Defines personal information, which includes:
    - screen or user names that function in the same way as an email address or other online contact information;
    - geolocation information that can identify a street name and town or city name;
    - a persistent identifier that can track a user over time and across different websites or online services such as a customer ID stored in a cookie, an IP address, or a unique device identifier; and
    - a photograph, video, or audio file that contains a child's image or voice.
- Includes parental notice provisions to ensure that the required notices are concise and timely.
- Provides companies with approval processes for getting verifiable parental consent.

- Requires covered website operators and online service providers to take reasonable steps to make sure that children's personal information is only released to companies that are capable of maintaining the confidentiality, security, and integrity of the information.
- Provides for the FTC's oversight of self-regulatory safe harbor programs.

The FTC has published guidance on the COPPA Rule, including:

- Complying with COPPA: Frequently Asked Questions (COPPA FAQs) that provides more detailed information on the COPPA Rule for parents and operators of commercial websites, mobile apps, and other online services.
- Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business that provides a six-step plan for determining if a company is covered by COPPA and what to do to comply with the COPPA Rule, including:
    - determining if the website or online service collects personal information from children under 13;
    - posting a privacy policy that complies with COPPA;
    - notifying parents directly before collecting information from their children;
    - getting parents' verifiable consent before collecting personal information from their children;
    - honoring parents' ongoing rights with respect to personal information collected from their children; and
    - implementing reasonable procedures to protect the security of children's personal information.

The FTC vigorously enforces COPPA against owners and operators of websites, mobile apps, and other online services. For a detailed discussion of the FTC's COPPA enforcement activities, see Practice Note, Children's Online Privacy: COPPA Compliance: Box: COPPA Federal and State Enforcement Actions.

In June 2019, the FTC announced a formal review of the COPPA Rule and opened for public comment whether changes are needed due to rapid technological changes and increased use of educational technology products. Well over 100,000 public comments have been submitted so far and the rulemaking process is currently ongoing.

For more information on COPPA, see Practice Note, Children's Online Privacy: COPPA Compliance.

State Privacy Laws

All 50 states have laws analogous to the FTC Act that prohibit unfair or deceptive acts or practices. In addition, there are also state-specific privacy laws that affect the collection, use, and sharing of personal information for online advertising and marketing purposes. For example, California has issued the most robust series of privacy laws, including:

- **CalOPPA.** CalOPPA is considered the first US online privacy law and requires businesses that collect the personal information of California residents from websites, apps, or other online services to post and honor their privacy policies. Because many businesses market to California residents, CalOPPA essentially makes national in scope the requirement for companies that collect personal information to post privacy policies.
- **California Consumer Privacy Act of 2018 (CCPA).** The CCPA is California's current comprehensive privacy law that imposes robust obligations on businesses that process the personal information of California residents, and provides California residents with the rights to know, delete, and opt-out of the sale of their personal information to

third parties. The law also regulates service providers and other third parties that receive personal information from businesses.

- **California Privacy Rights Act of 2020 (CPRA).** The CPRA replaced the CCPA beginning on 1 January 2023 and became applicable to personal information collected by the business beginning on or after 1 January 2022. Under the CPRA, many of the CCPA obligations and restrictions continue to be applicable. Some of the additional consumer rights include the right to correct incorrect personal information held by the business about the consumer, to opt out of the sharing of personal information to third parties for cross-context behavioral advertising, and to limit the use and sharing of their sensitive personal information.
- **California Age-Appropriate Design Code Act (AADC).** The AADC, signed into law on 20 September 2022, goes into effect 1 July 2024. Modeled after the United Kingdom's Age-Appropriate Design Code, the AADC is intended to increase protections for children 17 and under by requiring businesses that provide online services, products, and features likely to be accessed by children to comply with a number of new requirements. These requirements include restrictions on collecting certain information from children, implementing design changes, conducting Data Protection Impact Assessments, and modifying privacy notices to make them more accessible to children.
- **California "Shine the Light" Law.** This law requires businesses to disclose certain information regarding how they share personal information of California residents with third parties for those third parties' own direct marketing purposes.
- **Privacy Rights for California Minors in the Digital World Act (Eraser Law)**. This law requires businesses to permit minors who have an online account with the business to remove from public view content posted by them through their account.
- **Song Beverly Credit Card Act.** This law regulates the collection of personal identification information in connection with credit card transactions.
- **Student Online Personal Information Protection Act.** This law prohibits the sharing of certain student information for targeted advertising purposes.

For more information on California's privacy laws, see Practice Note, California Privacy and Data Security Law: Overview.

Other states also have privacy laws, including:

- **Virginia Consumer Data Protection Act (CDPA).** Virginia was the second state, behind California, to enact a comprehensive privacy law that also imposes robust obligations on controllers that process the personal data of Virginia residents. Under the CDPA, consumers have the right to know, correct, delete, and opt-out of the sale of their personal data, targeted advertising, and certain profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." In addition, controllers need affirmative opt-in consent before processing sensitive data. The law also regulates processors and other third parties that receive personal data from controllers.
- **Colorado, Connecticut, Iowa, Indiana, Montana, Tennessee, Texas, and Utah.** These states have also recently passed comprehensive consumer data privacy laws that, like their predecessors, provide the right to access and delete personal information and to opt-out of the sale of personal information. In addition, several other states have similar data privacy laws moving through the legislative process.
- **Nevada Sale Law.** This law gives Nevada residents the right to opt-out of the sale of their covered information.
- **Data Broker Laws.** Vermont and California have laws requiring data brokers to register with the state on an annual basis.

- **Biometric Privacy Laws.** Several states and municipalities have biometric privacy laws, the most notable of which is the Illinois Biometric Privacy Act (BIPA). BIPA prohibits companies from collecting or using biometric information without prior consent.
- **Washington My Health My Data Act (MHMD Act).** Signed into law on 27 April 2023, the MHMD Act regulates nearly all entities doing business in or directed at Washington State. It introduces many new obligations regarding "consumer health data," a broadly defined category of data related to consumer health and wellness. The MHMD Act is notable for creating a private right of action for violations, in addition to enforcement by the Washington Attorney General. Among its many requirements, the MHMD Act:
    - creates new notice guidelines regarding entities' practices for handling consumer health data;
    - prohibits regulated entities from collecting or sharing consumer health data without consent; and
    - requires that regulated entities obtain written authorizations from consumers prior to selling or offering to sell consumer health data.
- **Other Sectoral Laws.** Many states and municipalities have laws governing specific types of information such as video, health, financial, and student information.
- **State Data Breach Laws.** All 50 states and US territories have data breach notification laws.

For more information on US state privacy laws generally, see Practice Note, US Privacy and Data Security Law: Overview: State Laws.

FTC Guidance and Enforcement

Although there is no comprehensive federal law requiring businesses to post privacy policies, the FTC advises that online companies and commercial websites post privacy policies on their sites if they collect personal information from visitors. The FTC asserts several core principles for companies collecting personal information from users, including:

- **Notice.** Consumers should be given notice of the site's information practices.
- **Choice.** Consumers should be given the choice as to how their personal information is used, including the choice to opt out of third-party distribution of the information collected from or about them.
- **Access.** Consumers should be given reasonable access to information the site has collected about them and stored by the company.
- **Security.** Appropriate steps should be taken to ensure the security and integrity of any information collected from consumers.
- **Enforcement.** A mechanism should be in place to enforce these principles of privacy protection and means of redress for injured parties.

In addition, as a general matter, the FTC has made clear that if a company posts a policy and then uses the information it collects online in any way other than that specified in its privacy policy, or collects other information than that stated in its policy, it can be liable for damages. This lack of transparency in a privacy policy can be found to be an unfair or deceptive practice under the FTC’s enforcement powers under Section 5 of the FTC Act. Further, if a company does not post a privacy policy, it still may be liable for how it uses the data it collects.

The FTC has also provided guidance on privacy issues related to mobile apps. In February 2013, the FTC released a report titled Mobile Privacy Disclosures: Building Trust Through Transparency that aimed to promote more effective mobile privacy disclosures. The report recognizes the unique privacy challenges associated with mobile technology and sets out recommendations for mobile privacy policy best practices. The report recommends that all mobile platforms should:

- Provide just-in-time disclosures to consumers (immediately before the collection of sensitive information like geolocation data) and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation.
- Provide just-in-time disclosures and obtain affirmative express consent for other content that consumers would find sensitive in many contexts, such as contacts, photos, calendar entries, or the recording of audio or video content.
- Allow consumers to review the types of content accessed by the apps they have downloaded.
- Create icons to depict the transmission of user data.
- Promote app developer best practices. For example, platforms can require developers to make privacy disclosures, reasonably enforce these requirements, and educate app developers.
- Provide consumers with clear disclosures about the extent to which platforms review apps before making them available for download in the app stores and conduct compliance checks after the apps have been placed in the app stores.
- Offer a Do Not Track (DNT) mechanism for smartphone users. A mobile DNT mechanism, endorsed by a majority of the FTC, allows consumers to choose to prevent tracking by ad networks or other third parties as they navigate among apps on their devices.

The report also contains recommendations for mobile app developers.

In 2023, the FTC published an analysis of pixel tracking technologies. Referencing its recent enforcement actions against GoodRx and Betterhelp, the FTC made clear it is taking an in-depth look at companies' tracking tools, particularly as they relate to the collection and sharing of sensitive data related to consumer health. The analysis provides a comprehensive explanation of the backend functionality of pixel tracking, identifying three primary concerns with the technology: consumer consent, lack of clarity, and deidentification.

Restrictions on Cross-Border Transfers of Personal Data of Data Subjects in the EU and the UK

The EU's General Data Protection Regulation (GDPR) applies to the collection of personal data of data subjects in the EU and the UK, including where the collection has taken place in the US in connection with a US online advertising campaign.

The GDPR prohibits the export of personal data outside the EU and UK unless one of the following conditions is satisfied:

- The recipient (known as the "data importer") is based in a country that has been deemed adequate by the EU.
- The exporter (known as the "data exporter") has taken appropriate safeguards.
- An exception applies.

Because the EU has not deemed the US to be an adequate country, data importers located in the US have had to rely on other conditions. Between 2016 and 2020, many US data importers relied on the Privacy Shield Framework agreed to by the EU Commission and the US for data transfers, and enforced by the US Department of Commerce and the FTC through co-operation with EU data protection authorities. However, in July 2020, the Court of Justice of the European Union (CJEU) invalidated

Privacy Shield as a transfer mechanism in the *Schrems II* case (see *Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, Case C-311/18 (July 16, 2020)*). Data transfers reliant on Privacy Shield are no longer lawful, and US data importers that relied on Privacy Shield had to update their policies and practices, as well as turn to an alternative transfer mechanism.

Now most US data importers rely on Standard Contractual Clauses (SCCs), which are form, non-negotiable agreements approved by EU regulators, executed by data exporters and data importers to ensure appropriate safeguards for the transfer of personal data from the EU. For the UK, data importers must rely on the International Data Transfer Agreement.

For additional information on the GDPR, see Practice Note, Overview of EU General Data Protection Regulation.

Additional Laws, Regulations, and Rules Governing Online Advertising and Marketing

Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA) (17 U.S.C. § 512) addresses certain copyright issues raised by the use of digital media for distributing copyrighted materials, like:

- Restricting the circumvention of technological measures (also known as digital rights management or DRM) used to protect copyrighted works.
- Limiting the exposure of online service providers to copyright infringement liability for activities of their users by providing safe harbors for online service providers for:
    - Serving as a conduit for transmitting material through its system or network.
    - System caching.
    - Storing information at the direction of users.
    - Providing links or other tools for locating material.

To be eligible generally for the safe harbors, an entity must:

- Fall within the DMCA's definition of a service provider.
- Adopt and implement a policy that provides for termination of the accounts of repeat infringers.
- Accommodate and not interfere with certain technical measures that copyright owners use to identify or protect copyrighted works.

To qualify for a safe harbor with respect to the unknowing storage of, or linking to, infringing material, the service provider must also:

- Receive no financial benefit directly attributable to the infringing activity if it has the right and ability to control the underlying activity.
- Expeditiously remove or disable access to the infringing material on obtaining knowledge of it, including by receiving proper notification.

- File with the US Copyright Office a designation of agent to receive notifications of claimed infringement.

(17 U.S.C. § 512.)

However, there remains significant potential for liability for direct or secondary (vicarious or contributory) copyright infringement for entities that either:

- Are not service providers as defined under the DMCA.
- Fail to meet the relevant safe harbor requirements.

For a discussion of the DMCA safe harbor provisions, see Practice Note, Digital Millennium Copyright Act (DMCA): Safe Harbors for Online Service Providers.

Section 230 Immunity Under the Communications Decency Act

Section 230 of the Communications Decency Act creates a safe harbor for providers of interactive computer services acting solely as intermediaries for another party's content (47 U.S.C. § 230). Providers of interactive computer services include:

- Website operators.
- Online retailers.
- Search engines.
- Message board operators.
- Product and service review platforms.

For example, the safe harbor provided by Section 230 can protect websites and review platforms from liability for defamatory statements posted by users.

Section 230 immunity, however, only applies to the extent that an interactive computer service provider is not also the information content provider for the statement or publication at issue. The CDA defines an information content provider as any person or entity that is responsible, in whole or in part, for the creation or development of information provided through an interactive computer service (47 U.S.C. § 230(f)(3)). An interactive computer service provider may become an information content provider if it materially contributes to or aids in the development of the content at issue.

Providing content-neutral tools, like a product rating and review system, does not generally lead to the loss of Section 230 immunity.

For more information on the Section 230 safe harbor, see Practice Note, Communications Decency Act: Section 230 Immunity.

Self-Regulatory Programs and Codes Governing Online Advertising and Marketing

Self-regulation plays an important role in the advertising industry. Industry groups have promulgated respected and widely-followed self-regulatory codes and many advertising disputes are resolved through self-regulatory dispute mechanisms. However, voluntary regulations and codes of practice do not have legal force and entities complying with these codes and regulations still must comply with all laws and government rules.

Relevant industry groups that provide self-regulatory programs and codes of practice covering online advertising and marketing include:

- National Advertising Division (NAD) (see NAD).
- The Children's Advertising Review Unit (CARU) (see CARU).
- The Digital Advertising Alliance (DAA) (see DAA and the Digital Advertising Accountability Program).
- National Advertising Initiative (NAI) (see NAI).

For more information on these programs and self-regulation of the advertising industry generally, see Practice Note, Advertising Self-Regulation in the US: Overview.

NAD

Administered by BBB National Programs, Inc. (BBBNP), the NAD reviews national advertising, in all media, brought to its attention by a consumer or competitor challenge or through its monitoring program. The NAD evaluates advertising compliance in accordance with accepted standards of disclosure and substantiation, deferring to FTC guidance. Upon reviewing the advertising, the NAD informs the advertiser of the claims it finds in the ad and asks for the advertiser's substantiation. The NAD makes its own determination of the communication, but also considers evidence of consumer perception.

The NAD has a substantial body of precedent and participants typically adhere to its recommendations. The NAD refers to the FTC and other regulators with jurisdiction over the claims at issue advertisers who choose not to participate in NAD proceedings or refuse to comply with its decisions. For more information on the NAD, see Practice Note, Advertising Self-Regulation in the US: Overview: NAD.

CARU

Also administered by BBBNP, CARU reviews national advertising directed to children in all media and issues with the online collection of personal information from children for compliance with its guidelines:

- Self-Regulatory Guidelines for Children's Advertising, which address advertising to children under 13 in any medium (CARU Advertising Guidelines).
- Self-Regulatory Guidelines for Children's Online Privacy Protection, which address data collection from children under 13 through online advertising and marketing (CARU Privacy Guidelines).

Although these guidelines are voluntary, they are extremely influential.

The CARU Privacy Guidelines align with COPPA and provide, for example, that:

- In all cases, the information collection or tracking practices and information uses must be clearly disclosed, along with the means of correcting or removing the information.
- When personal information, such as email addresses or screen names, are to be publicly posted, enabling others to communicate directly with a child online, the company must obtain prior verifiable parental consent.
- When personal information is to be shared or distributed to third parties, the company must obtain prior verifiable parental consent.

- When personal information is obtained for a company's internal use and there is no disclosure of the information, parental consent may be obtained through the use of email coupled with some additional steps to provide assurance that the person providing consent is the parent.
- When online contact information is collected and retained to respond directly more than once to a child's specific request and not used for any other purpose, the company must directly notify the parent of the nature and intended uses of the information collected and permit access sufficient to allow a parent to remove or correct the information.

CARU operates one of the FTC-approved safe harbors under COPPA. Companies that participate in the CARU safe harbor program and adhere to the CARU Guidelines are deemed compliant with COPPA, protecting them from FTC enforcement action. Conversely, companies that refuse to co-operate with CARU's self-regulatory program may be referred to the FTC for enforcement. For more information on CARU, see Practice Note, Advertising Self-Regulation in the US: Overview: CARU.

DAA and the Digital Advertising Accountability Program

The DAA was formed by several leading advertising and marketing associations, like BBBNP, the Association of National Advertisers (ANA), and the Interactive Advertising Bureau (IAB), to advance industry self-regulation of online behavioral advertising (OBA). The DAA establishes and enforces self-regulatory principles to protect consumer privacy in relation to OBA and multi-site data collection (DAA Principles):

- Its foundational set of principles, Self-Regulatory Principles for Online Behavioral Advertising, includes seven principles to protect consumer privacy in OBA, specifically:
  - education;
  - transparency;
  - consumer control;
  - data security;
  - material changes;
  - sensitive data; and
  - accountability.
- Its subsequent principles, Self-Regulatory Principles for Multi-Site Data, cover the collection of data across multiple sites over time, the same as the data collected for OBA, but for purposes other than OBA.

The DAA has also issued guidelines (DAA Guidelines) for applying the DAA Principles to:

- The mobile environment.
- Data used across devices.
- Political advertising.

The DAA's YourAdChoices Program (Choices Program) is based on the DAA Principles. The Program includes, among other things:

- A clickable advertising option icon to be displayed on ads shown based on information collected for OBA purposes, linking to information about the data collection and a mechanism to opt-out of being shown targeted ads from DAA participants.
- Requirements for companies engaged in OBA to provide notice and choice regarding their practices.

However, compliance with the Choices Program may not be sufficient to meet obligations under the CCPA and other privacy laws, and companies should evaluate their obligations.

The Digital Advertising Accountability Program (Accountability Program) was established to enforce industry compliance with the DAA Principles. BBBNP and the ANA administer the Accountability Program by monitoring compliance with the DAA Principles and the DAA Guidelines and initiating and handling complaints and issuing decisions. It operates similarly to other self-regulatory programs administered by BBBNP.

For more information on the DAA and the Accountability Program, see Practice Note, Advertising Self-Regulation in the US: Overview: Digital Advertising Alliance and Accountability Program.

NAI

The NAI is a self-regulatory membership organization comprised exclusively of third-party digital advertising companies. The organization's members include internet advertisers, like Google and Yahoo, that collect and use consumer information for OBA. NAI members must comply with the self-regulatory NAI Code of Conduct (NAI Code) in addition to the DAA Principles and DAA Guidelines. The NAI Code covers data collection and use through both the internet and mobile apps. It imposes notice, choice, accountability, data security, and use limitation requirements on NAI member companies.

Compliance and enforcement programs include:

- Annual reviews.
- Ongoing technical monitoring.
- Mechanisms for accepting and investigating complaints of non-compliance.
- Sanction procedures.

The NAI issued an updated NAI Code in 2020. This updated code makes several changes to the previous version, including:

- Prohibiting behavioral targeting of children under 16 (raised from under 13) without verifiable parental consent.
- Requiring NAI members to obtain consumers' opt-in consent before collecting and targeting sensitive data, such as geolocation data and health information, for:
    - ad targeting;
    - ad delivery; and
    - ad reporting.
- Requiring NAI members to disclose the political audience targeting segments they use for digital advertising.

For more information on the 2020 NAI Code, see Legal Update, Network Advertising Initiative (NAI) Prohibits Behavioral Targeting of Users Under 16.

In addition, in conjunction with the DAA, the NAI has developed an OBA opt-out tool for consumers. The tool gives consumers the ability to prevent NAI members from serving OBA on the consumer's web browser.

When a consumer opts out, NAI members can still advertise on the consumer's browser, but it can no longer customize ads based on the consumer's interests and web-usage patterns using cookie-based technology. For more information on the NAI, see Practice Note, Advertising Self-Regulation in the US: Overview: NAI.

Restrictions and Risks Associated with Specific Types of Online Advertising and Marketing

Certain types of online advertising and marketing strategies present their own unique challenges. Depending on regulations and risks that apply specifically to these strategies, companies may need to exercise extra care when:

- Building and optimizing company websites (see Company Websites).
- Engaging in targeted advertising (see OBA and Other Targeted Advertising).
- Advertising and marketing through social media (see Social Media).
- Encouraging, collecting, and using user-generated content (see User-Generated Content).
- Encouraging, collecting, and using consumer reviews (see Consumer Reviews).
- Engaging in native advertising (see Native Advertising).
- Conducting influencer marketing (see Influencer Marketing).

Company Websites

Companies use websites for many different reasons, like providing an online shopping experience, an alternative way to contact the company, or just basic company information. Company websites are also a key way to advertise to customers. Representations on company websites must comply with the same advertising principles as claims made in traditional media.

Websites typically include terms of use and privacy policies to manage user expectations and help protect the company from liability. For information on website terms of use in the US, see Standard Document, Website Terms of Use. For information on privacy policies in the US, see Standard Document, Website Privacy Policy.

In addition, businesses use a variety of tactics to enhance the content of their websites and drive traffic to their websites, some of which pose certain risks, like:

- Linking (see Linking).
- Framing and embedding (see Framing and Embedding).
- Metatags, keywords, and other search engine optimization issues (see Metatags and Keywords).
- Pop-up advertising (see Pop-Up Ads).

- Affiliate marketing (see Affiliate Marketing).

The risks involved with using these tactics vary and the law remains unclear in several areas.

Linking

Hyperlinks provide the ability for internet users to navigate websites by clicking on a link to move quickly from one web page directly to the relevant part of another page on the same or a different website. Deep links are hyperlinks that point to a specific page or image within another website, instead of simply to that website's homepage.

A basic hyperlink from one party's website to another, without more, generally does not pose intellectual property (IP) infringement risks or other legal risks, particularly where the initial site provides the user notice that the user is leaving its site. Even where that hyperlink contains the other party's trade mark the risk of infringement is low. However, there are some risks, including where a defendant:

- Capitalizes on what courts have called the "initial interest confusion" of the user so that the user thinks that the defendant's website is connected to the claimant's, the hyperlink can be actionable for trade mark infringement (see *Nissan Motor Co. v. Nissan Comput. Corp.*, 378 F.3d 1002 (9th Cir. 2004)).
- Posts links on its website to a third-party website that has unauthorized copies of the plaintiff's copyrighted material and encourages users to view that material, the defendant can be held liable for contributory copyright infringement (see *Intell. Rsrv., Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999)).

The DMCA does provide a limited safe harbor from copyright infringement liability for online service providers when their users provide links to infringing materials as long as they meet the safe harbor requirements. For example, actual knowledge or awareness of facts or circumstances indicating specific and identifiable instances of infringement can disqualify an online service provider from the DMCA safe harbor (*Viacom v. YouTube*, 676 F.3d 19 (2d Cir. 2012)).

Deep linking poses similar risks to basic hyperlinking in the areas of copyright and trade mark infringement. As for the risk of unfair competition, deep linking is not in itself an act of unfair competition, but could become unfair if the person providing the deep link falsely suggests or implies an association with the targeted website.

In addition, deep linking can pose a risk of breach of contract. If a website's terms and conditions expressly prohibit deep linking, a third party could be liable for breach of contract if it either:

- Accepts the terms and conditions (for example, by clicking on an "I agree" button) before going further into the site.
- Had knowledge of the terms and conditions (including the deep-linking prohibition) and facts show an implied agreement to them.

(*Ticketmaster v. Tickets.com, Inc.*, 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003).)

Framing and Embedding

Framing refers to the practice of displaying, within a frame or border of a website, content from another website. The effect is that the content of the linked site looks as if it is part of the framing website. Framing involves the copying of a significant amount of the linked site's content and may therefore be more likely to amount to copyright infringement than linking.

Embedding through in-line linking refers to the practice of integrating a social media post or website content into a third-party's website in a way that links back to the original post or content without creating a copy of that post or content. Embedding displays the post or content on the embedder's website directly from the original server but does not create or store an additional copy of the material on the embedder’s server.

Framing and embedding have been subject to a wide variety of claims and the law remains unsettled. In *Washington Post Co. v. Total News Inc.*, the defendant's website linked to the plaintiff's and other news organizations' sites within a frame decorated with the defendant's logo, cutting off some of the borders of the plaintiff's and others' sites. The plaintiff sued for numerous claims under federal and state law, including misappropriation, trade mark and copyright infringement, and unfair competition under New York state law. The plaintiffs argued that this practice devalued their sites' content and contended that it was unfair for the defendant to run its own advertising on its site, which was dedicated exclusively to running third-party content in frames. The case settled and the defendant agreed to link to, but not frame, the third-party sites. (97 Civ. 1190 (S.D.N.Y. Complaint filed Feb. 20, 1997).)

Framing can also raise breach of contract risks. In *Hard Rock Café International (USA) Inc. v. Morton*, the plaintiff entered into a licensing agreement for use of the defendant's trade marks. The license prohibited the use of these trade marks in connection with the sale of merchandise online. The defendant's website on which the licensed trade marks were prominently featured included a button that opened a window on which consumers could purchase music CDs. Although the button actually linked to a third-party site on which the CDs were sold, the court determined that the third-party site was framed in such a way as to make it nearly impossible for the consumer to know that they were not buying the CDs from the defendant's site. The court held that this violated the licensing agreement. (1999 WL 701388 (S.D.N.Y. Sept. 9, 1999).)

Framing of another entity's website may constitute an infringing derivative work subjecting the "framer" to copyright liability. For example, an image search engine was held to have made fair use of photographs that it indexed and displayed as small, low-resolution thumbnail images on a search results page but may have infringed when it framed full-sized images within its own page content (see *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003)).

In another case, a search engine operator was found not to have infringed an adult website's copyright when the search engine provided frames and in-line links to full-size images on the adult website. The court held that the adult website actually "served" the images that were being displayed to users, not the search engine. Under this holding, a website publisher (or in this case, a search engine) is liable only if the allegedly infringed material is copied and hosted on that publisher's own server but not if the material is embedded or linked from the original third-party server. (*Perfect 10, Inc. v. Amazon.com. Inc.*, 508 F.3d 1146 (9th Cir. 2007); see also *Hunley v. Instagram, LLC*, 73 F.4th 1060 (9th Cir. 2023) (applying the server test adopted in *Perfect 10*, holding that Instagram's embedding feature does not infringe the exclusive display right of Section 106(5) of the Copyright Act).)

This "server test" seemed to be a solid defense to copyright infringement claims related to embedding until more recent developments.

In 2018, the Southern District Court of New York rejected the *Perfect 10* decision and held that embedding a third-party tweet on a website violates the Copyright Act's exclusive display right (*Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585 (S.D.N.Y. 2018)). *Goldman* rejected *Perfect 10's* server test. Instead, the Goldman court relied on the Copyright Act's definition of public display as including transmission from "any device or process." The steps involved with embedding the tweet constituted such a process and therefore the court held that the plaintiff's exclusive right to public display was infringed. For more information, see Legal Update, Even Without Copying, Embedded Tweet of Tom Brady Photo Violates Copyright Act: S.D.N.Y.

More recently, the Southern District Court of New York rejected the server test again. In *Nicklen v. Sinclair Broadcast Group, Inc.*, the court held that embedding a video on a website violates the exclusive display right under the Copyright Act (2021 WL 3239510 (S.D.N.Y. July 30, 2021)). It specifically rejected the server test as contrary to the text and legislative history of the

Copyright Act because it makes the display right a subset of the reproduction right. According to the court, infringement of the display right should not be contingent on the alleged infringer making a copy of the materials at issue. For more information, see Legal Update, Embedding Video Violates Display Right: S.D.N.Y.

Until the discrepancy between the Ninth Circuit server test and the New York Southern District Court's decisions have been resolved, using in-line linking should not be considered a guaranteed defense against liability for copyright infringement.

Metatags

A metatag is a word, usually a name or a descriptive term, placed by a website operator in the hidden programming code of a website, pop-up ad, or banner ad, which is used by internet search engines to some extent to find, classify, and rank websites for internet users. Metatags are a means by which website owners seeking to promote their websites can attract more traffic.

Embedding metatags or hidden text in the code of a site could lead to legal action on various grounds. Website owners should be careful when using names, logos, registered trademarks, or other materials belonging to third parties (in particular where they are competitors) as a means of obtaining more hits from search engines.

Some courts have held that use of a third party's trade mark as a metatag can result in trade mark infringement. For example, in *Horphag Research Ltd. v. Pellegrini*, the defendant used the plaintiff's registered trade mark as a metatag but claimed a fair use defense. The court rejected this defense and held that defendant's use of plaintiff's mark as a metatag created a likelihood of consumer confusion resulting in infringement (337 F.3d 1036 (9th Cir. 2003)). Note, however, that a fair use defense can be successful where a defendant shows that the trade mark used as a metatag was descriptive and used in an editorial fashion (*Playboy Enters., Inc. v. Welles*, 7 F. Supp.2d 1098 (S.D. Cal. 1998)).

The Seventh Circuit has also held that a defendant's use of a plaintiff's trade mark in the defendant's metatags was likely to cause initial interest confusion in consumers (*Promatek Indus., Ltd. v. Equitrac Corp.*, 300 F.3d 808, 812 (7th Cir. 2002)).

However, other courts have held the opposite. In *Standard Process, Inc. v. Banks*, the court rejected the argument that metatags create initial interest confusion (and therefore result in trade mark infringement) in part because metatags are immaterial (554 F.Supp.2d 866 (E.D. Wis. 2008)). In another case, *Fragrancenet.com, Inc. v. FragranceX.com, Inc.*, the court found that both keywords and metatags are not a trade mark use in commerce and therefore cannot constitute infringement (493 F.Supp.2d 545 (E.D.N.Y. 2007)).

In addition, metatags that can be construed as advertising claims can present the risk of false advertising. For example, the FTC brought a complaint against Liverite Products, a dietary supplement maker, charging that Liverite made false claims about the efficacy of its product by claiming that it could, among other things, prevent and treat alcohol-induced liver disease. The FTC further charged that Liverite's website made deceptive use of metatags, which included the terms hepatitis, cirrhosis, hangover, and liver disease. The FTC, Liverite, and its owners entered into a settlement agreement providing for a permanent injunction and monetary relief. (*FTC v. Liverite Prods., Inc.*, 2001 WL 34134897 (C.D. Cal. Aug. 21, 2001).)

Keywords

Keyword advertising is a type of online and mobile advertising where an advertiser pays for its ad or sponsored link to appear based on the relevance of a specified term or phrase typed in by a user, commonly referred to as a keyword. The advertiser in effect purchases the keyword from a search engine, such as Google, but the keyword does not necessarily need to appear in the ad or sponsored link. Some search engines allow advertisers to purchase third-party trade marks as keywords.

For example, Google's trade mark policy permits advertisers to purchase trademarked keywords without restriction. Google also permits advertisers to use third-party trade marks in the text of advertisements only under the following four conditions:

- The term is used in its generic or descriptive sense.
- The advertiser sells the trade marked product.
- The advertiser sells parts or products compatible with the trade marked product.
- The ad's landing page provides legitimate information about the trade marked product. A competitor may not use the trade marked term in the ad text to sell its competing products.

Many courts have addressed the issue of trade mark infringement for purchasing other parties' trade marks as keywords for search engines. To find infringement under the Lanham Act, the plaintiff must show that the defendant used the mark "in commerce" and that use caused a likelihood of consumer confusion (15 U.S.C. § 1114).

Various district courts have found purchasing or selling keywords to be a use in commerce under the Lanham Act, therefore making the purchasers or sellers susceptible to potential liability (see, for example, *Morningware, Inc. v. Hearthware Home Prods., Inc.*, 673 F. Supp. 2d 630 (N.D. Ill. 2009); *Hearts on Fire v. Blue Nile, Inc.*, 603 F.Supp.2d 274 (D. Mass. 2009); *Hysitron v. MTS Systems Corp.*, 2008 WL 3161969 (D. Minn. Aug. 1, 2008)).

Despite this growing consensus, the federal district courts in New York initially resisted this trend holding that the purchase of trade marks as keywords was **not** use in commerce. However, a 2009 Second Circuit decision changed that trajectory. In *Rescuecom Corp. v. Google, Inc.*, the Second Circuit found that Google's practice of displaying, offering, and selling Rescuecom's mark to Google's advertising customers when selling its advertising services constituted a trade mark use in commerce. *Rescuecom* involved Google's sale of keyword trade marks, rather than an advertiser's purchase of keyword advertising. (562 F.3d 123 (2d Cir. 2009).)

Subsequent cases in the New York federal district courts extended *Rescuecom's* holding to the advertiser's purchase of keywords (for example, see *CJ Prods. LLC v. Snuggly Plushez LLC*, 809 F.Supp.2d 127 (E.D.N.Y. 2011)). The Ninth Circuit has also relied on *Rescuecom* to hold that the purchase of trade marks as keywords is a use in commerce (see *Network Automation, Inc. v. Advanced Sys. Concepts, Inc.*, 638 F.3d 1137, 1145 (9th Cir. 2011)).

The courts now seem to have reached a consensus that the purchase of trade marks as keywords is a use in commerce.

Various courts have also examined whether the use of third-party trade marks as keywords causes a likelihood of confusion. Although courts analyze likelihood of confusion on a case-by-case basis, they have tended to hold that the practice of using third-party trade marks as keywords is:

- Likely to cause confusion and lead to trade mark infringement when coupled with the use of that trade mark in the keyword-triggered sponsored ads or links (see *Storus Corp. v. Aroa Mktg., Inc.*, 2008 WL 449835 (N.D. Cal. Feb. 15, 2008) (holding that referencing the trade mark in the ad copy creates a likelihood of consumer confusion); *Gov't Emps. Ins. Co. v. Google Inc.*, 2005 WL 1903128 (E.D. Va. Aug. 8, 2005) (holding that competitors of Geico purchasing GEICO as a keyword to trigger sponsored ads that included the GEICO mark was likely to cause confusion and was infringing); *Multi Time Mach., Inc. v. Amazon.com, Inc*. 804 F.3d 930 (9th Cir. 2015) (holding that confusion was unlikely because the keyword-triggered search results on Amazon did not include the plaintiff's trade mark and clearly identified the listed products with the brand name, model number, and photographs)).
- Less likely to cause confusion and be non-infringing when the resulting sponsored ads or links do not display the plaintiff's trade mark (see *1-800 Contacts, Inc. v. Lens.com, Inc.*, 722 F.3d 1229 (10th Cir. 2013); *Network Automation, Inc. v. Advanced Sys. Concepts*, 638 F.3d 1137, 1151-54 (9th Cir. 2011); *Allied Interstate LLC v. Kimmel & Silverman P.C.*, 2013 WL 4245987, at *6 (S.D.N.Y. Aug. 12, 2013)).

Although courts are less likely to find a likelihood of confusion based on keyword use when the plaintiff's mark does not appear in the search results, this outcome is not guaranteed. At least one court has allowed an infringement claim to proceed where the ads triggered by defendant's use of plaintiff's trade mark as a keyword did not depict the plaintiff's mark. In *Jim S. Adler, P.C. v. McNeil Consultants, L.L.C.*, the court held that although the defendant's keyword-triggered ads were generic and unlabeled, they could nevertheless mislead consumers to believe that the plaintiff was affiliated with the advertisements (10 F.4th 422, 429 (5th Cir. 2021) (concluding that whether an advertisement displays the plaintiff's trade mark is a relevant but not dispositive factor in assessing likelihood of confusion)).

On the other hand, where the plaintiff's trade mark is not distinctive, even its appearance in keyword-triggered advertisements may be insufficient to support a likelihood of confusion finding (see *Passport Health, LLC v. Avance Health Sys., Inc.*, 2018 WL 6620914, at *3 (E.D.N.C. Dec. 18, 2018), appeal filed Jan. 14, 2019 (holding no likelihood of confusion given that PASSPORT HEALTH mark was non-distinctive and appeared in a different context in an ad linking to a website that clearly identified its source); *Alzheimer's Disease & Related Disorders Ass'n, Inc. v. Alzheimer's Found. of Am., Inc.*, 307 F.Supp.3d 260 (S.D.N.Y. Apr. 20, 2018) (holding no likelihood of confusion where the plaintiff's mark was weak and there was little actual evidence of consumer confusion)).

Given the fact-specific analysis necessary for determining the likelihood of confusion, advertisers should proceed with caution when considering the purchase of a competitor's trade mark for keyword advertising. For more information on trade mark infringement generally, see Practice Note, Trademark Infringement and Dilution Claims, Remedies, and Defenses. For more information on keyword advertising and trade mark infringement, see Practice Note, Brand Protection Online: Keyword Advertising.

Pop-Up Ads

Similar to keyword advertising, pop-ads appear in response to consumers' own internet searches. Advertisers use pop-up ads to target and engage consumers based on consumer behavior.

Website owners have raised concerns about third-party pop-up ads that are triggered when a user visits their websites because the trigger typically is a user's use of the website owner's trade mark (like typing in the website owner's trade mark or website address in a search). The website owners have claimed that these pop-up ads may confuse internet users into believing that the pop-up ads were approved by or are associated with them in violation of the Lanham Act.

However, several trade mark infringement cases against WhenU.com have resulted in what seems to be a consensus that if pop-up ads appear in a separate window and do not use another's trade mark in the advertisement itself, they generally do not violate the Lanham Act (see *1-800 Contacts, Inc. v. WhenU.com, Inc.*, 309 F. Supp. 2d 467 (S.D.N.Y. 2003), *rev'd and remanded sub nom.*, 414 F.3d 400 (2d Cir. 2005)*; Wells Fargo & Co. v. WhenU.com, Inc.*, 293 F. Supp. 2d 734 (E.D. Mich. 2003); *U-Haul Int'l, Inc. v. WhenU.com, Inc.*, 279 F. Supp. 2d 723 (E.D. Va. 2003)).

For more information on pop-up advertising and trade mark infringement, see Practice Note, Brand Protection Online: Pop-Up Advertisements.

Affiliate Marketing

Affiliate marketing is the use of third parties to generate traffic to a company's website or other digital content in an exchange for a commission. An affiliate marketer typically discusses products or services on their own website or social media page and provides links to where the products or services can be purchased.

Under the FTC's Guides Concerning the Use of Endorsements and Testimonials in Advertising (Endorsement Guides) (16 C.F.R. §§ 255.0 to 255.6), affiliate marketers who receive commission for driving traffic to a company's website or for purchases made through their links have a material connection with the companies they feature. They must disclose their relationship

with those companies so that consumers understand they are being paid. The disclosure must be clear and conspicuous. The FTC specifically addresses affiliate marketers' obligations under the Endorsement Guides in its detailed guidance on material connections and disclosure obligations (see FTC's Endorsement Guides: What People Are Asking) (Endorsement FAQs).

The FTC issued updated Endorsement Guides and Endorsement FAQs on June 29, 2023. The Endorsement FAQs include a detailed scenario about affiliate marketing that makes several recommendations, including:

- Affiliate marketers must disclose their relationship to retailers clearly and conspicuously.
- Readers should be able to see both the review containing the disclosure and the affiliate link at the same time.
- The closer the affiliate marketer's disclosure is to the recommendation the better.
- Certain disclosure language is not adequate, like:
    - "affiliate link";
    - "commissionable link"; or
    - a "buy now" button.

The updated Endorsement Guides provide a more restrictive definition of clear and conspicuous. For more information about material connections and disclosures under the updated Endorsement Guides, see Influencer Marketing.

OBA and Other Targeted Advertising

OBA, also known as interest-based advertising, is the practice of collecting information about users' activities across sites over time and using this information to deliver targeted advertising based on users' interests. Privacy concerns have become the driver of regulation and enforcement around OBA.

In February 2009, the FTC released a set of principles for the self-regulation of online behavioral advertising. The principles are still applicable today and include:

- **Transparency and control.** Companies engaged in online behavioral advertising should disclose the practice and allow consumers to opt out.
- **Reasonable security and limited data retention.** Companies engaged in online behavioral advertising should maintain reasonable security and limit the amount of data retained.
- **Material changes to privacy policies.** Companies should obtain express consent before using previously collected data in a way that differs from the disclosures in the privacy policy set out at the time of collection.
- **Sensitive data.** Companies should obtain express consent before using sensitive data, such as data about children, health, or finances, for purposes of online behavioral advertising.

In July 2009, in response to calls from the FTC for comprehensive self-regulation in this area, the advertising industry formed the DAA and the NAI to advance industry self-regulation of OBA. The DAA Principles, the DAA Guidelines and the NAI Code have been the primary programs for self-regulation of OBA (see Self-Regulatory Programs and Codes Governing Online Advertising and Marketing).

For nearly a decade, OBA in the US was regulated primarily through a combination of self-regulation and enforcement of sector-specific laws (such as COPPA) and consumer protection laws. The enactment of the EU's GDPR, however, started a trend of increased scrutiny around OBA in the US. As a result, regulation in the US fundamentally changed in January 2020 when the CCPA came into effect.

Under the CCPA, California consumers have the right to opt out of the sale of their personal information. Although many businesses may not sell information in the traditional sense, the term "sale" is broadly defined under the CCPA, and the California Attorney General's Office has indicated that the right is meant to allow California consumers to opt-out of the disclosure of their information for OBA purposes. In response to the CCPA, the advertising industry developed frameworks and technical specifications designed to help businesses address the opt-out right. The IAB, in particular, developed a framework to restrict the use of information passed through tracking technologies, not just the display of targeted advertising (as with the DAA's opt-out).

Browser and platform operators have also shaped OBA. In its current form, the ad-tech ecosystem relies heavily on the collection of identifiers through tracking technologies, such as cookies and pixels. Over the past several years, major browsers have implemented measures to restrict third-party cookies. For example, Mozilla FireFox and Apple Safari now block third-party cookies by default. Google has announced its intent to phase out of third-party cookies for Chrome in 2024. With the introduction of iOS14.5, Apple now requires companies to provide additional transparency and obtain opt-in consent for tracking within apps.

In 2023, several additional state-specific laws are taking effect that directly impact OBA:

- The CPRA (which replaced the CCPA) and the CDPA on 1 January 2023.
- Connecticut's and Colorado's privacy laws on 1 July 2023.
- Utah's privacy law on 31 December 2023.

These laws provide individuals with the right to opt-out of certain processing of their information for OBA purposes and other states have passed similar laws that take effect in 2024 and 2025 (see State Privacy Laws). Companies engaged OBA should start preparing for compliance with these laws.

Social Media

Social media has become an essential way for companies to advertise, promote brand awareness, and interact and communicate with consumers. Through social media, consumers are not just targeted for advertising, but can also be participants in the creation and distribution of it.

Although just another online vehicle for advertising and marketing, social media poses some unique challenges regarding:

- Compliance with the terms and conditions set by social media platforms (see Third-Party Terms of Use).
- Content posted by users (see User-Generated Content).
- Endorsements (see Influencer Marketing).
- Native advertising (see Native Advertising).

Despite the seemingly casual nature of social media, all the advertising laws, data privacy laws, and other laws that apply to online advertising and marketing generally (and traditional advertising for that matter) also apply to social media platforms.

In addition, many government agencies and departments have issued specific guidance to address the risks of advertising on social media, for example:

- The Federal Financial Institutions Examination Council released proposed guidance on the applicability of consumer protection and compliance laws, regulations, and policies to activities conducted via social media by banks, savings associations, and credit unions, as well as non-bank entities supervised by the Consumer Financial Protection Bureau and state regulators (see Social Media: Consumer Compliance Risk Management Guidance).
- The Department of Transportation issued guidance entitled Advertising Air Fares on Social Media Sites.
- The Securities Exchange Commission issued guidance on the use of social media (see Investment Advisor Use of Social Media and SEC Says Social Media OK for Company Announcements if Investors Are Alerted).
- The Alcohol and Tobacco Tax and Trade Bureau issued guidance entitled Department of the Treasury: Use of Social Media in the Advertising of Alcohol Beverages.
- The Food and Drug Administration has issued draft guidance regarding the promotion of prescription drugs and medical devices using the internet and social media, including:
    - Internet/Social Media Platforms with Character Space Limitations Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices; and
    - Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices.

In addition, the FTC recently ordered social media platforms (including Meta, Instagram, YouTube, Twitter, and other platforms) to provide information on their advertising practices. The orders seek information from 2019 through 2023 so that the FTC can "study relevant business conduct since the start of the COVID-19 pandemic." The FTC explained that it intends the study:

- To "help the Commission better understand how prevalent deceptive advertising is on social media and video streaming platforms, the consumers who may be harmed by that advertising, and the effectiveness of the platforms' oversight of advertisers, including whether the companies treat English-language and Spanish-language ads differently."
- To show "how the platforms create ads, including any use of generative artificial intelligence, and track, and classify ads, as well as the ad formats offered to advertisers, including shoppable ads, which allow consumers to purchase products or service directly through the ad, and virtual reality and other extended reality ads."

Third-Party Terms of Use

If a company creates a branded page hosted by a third-party platform, such as Facebook or Twitter, it must register and agree to abide by the terms of use and policies that apply to that service and host company. The company should consider carefully terms relating to:

- Rights and restrictions on promotional and advertising practices, including products the platform does not permit to be advertised on its service.
- The actions of users who access, use, and interact with the service.

- Takedown notices received under the safe harbor provisions of the DMCA.
- Age limits for users.
- Ownership of IP such as copyrights and trademarks, as well as of customer or user information collected through the site.
- Licenses or other grants allowing use of the company's name or other IP by the site owner or other third parties.
- Privacy of the information collected by the third-party service or the company.
- Recourse for users in the event of a breach of any protections.

Although the platform bears primary responsibility for regulating the actions of the users of its service, a company should still monitor its branded page for issues such as:

- Offensive or inappropriate content.
- IP infringement.
- Submissions made by or using the personal information of children.

Further, companies running promotions, such as sweepstakes and contests, within social media platforms, must, in addition to following all applicable laws, abide by the relevant third party's terms of service, which may include restrictions beyond those imposed by law. A company also should consider:

- Establishing requirements for user-generated content that prohibit infringing, libelous, or otherwise offensive content.
- Limiting eligibility to certain states or countries.
- Linking to the company's privacy policy (which may need to comply with COPPA, depending on who is eligible for the sweepstakes or contest).

Regardless of the platform on which a promotion is run, the same state and federal laws apply online as in offline contests. For an overview of the laws governing these types of promotions, see Practice Notes, Sales Promotions, Contests, and Sweepstakes and Running a Sweepstakes or a Contest in the US.

User-Generated Content

User-generated content (UGC) can take many forms, such as:

- Product and service reviews.
- Videos.
- Contest entries.

When a company accepts UGC for its website, social media page, or other mobile or online service whether for a contest entry or other purpose, it should consider the risks posed by the UGC, like potential:

- Copyright, trade mark, and other IP infringement.

- Violations of publicity or privacy rights.
- False claims.
- Defamatory statements.

The DMCA and CDA provide limited protections for the online service provider against liability for problematic content posted by users (see Additional Laws, Regulations, and Rules Governing Online Advertising and Marketing). Neither law, however, protects a company when it uses the UGC for its own purposes, like posting it on another social media platform or including it in advertising.

To help avoid or reduce the risk of liability for UGC, companies should:

- Establish standards for UGC and clearly communicate them.
- For UGC submitted on social media, review and comply with the platform's rules and guidelines.
- Obtain all necessary permissions to use any UGC, including reposting it within the same social media platform.
- For contests that involve the submission of UGC, include standards for entries in the official rules and disqualify any entries that violate the rules.

For more information on UGC, see User-Generated Content (UGC) in Advertising and Promotions Checklist and Practice Note, Advertising and Promotions in Social Media: User-Generated Content.

Consumer Reviews

Consumer reviews are a type of UGC. The Consumer Review Fairness Act (CRFA) prohibits businesses from using non-disparagement clauses in form contracts or otherwise impeding customers from posting negative reviews (15 U.S.C. § 45b). It protects customers who write reviews of products, services, and business conduct in any media, including social media. Although not addressed by the CRFA, the FTC has made it clear that companies should also refrain from suppressing the display of negative reviews online, treating such suppression in multiple enforcement actions as a violation of the FTC Act.

The Endorsement Guides apply to incentivized customer reviews. When a company provides incentives to customers to post a review (through free products, discounts, sweepstakes entries, or other benefits), the FTC considers those customers to have a material connection to the company. That material connection must be disclosed clearly and conspicuously (see Influencer Marketing).

The updated Endorsement Guides include an extensive section on handling consumer reviews to avoid deception and provides several examples of deceptive practices. Specifically, the Endorsement Guides now state that "in procuring, suppressing, boosting, organizing, publishing, upvoting, downvoting, reporting, or editing consumer reviews of their products, advertisers should not take actions that have the effect of distorting or otherwise misrepresenting what consumers think of their products, regardless of whether the reviews are considered endorsements under the Guides." (16 C.F.R. § 255.2.) The Endorsement FAQs also include additional scenarios related to the handling of consumer reviews (see FTC's Endorsement Guides: What People Are Asking).

When using customer reviews for advertising purposes (whether online or offline), advertisers should:

- Use only reviews that:

  - reflect the honest opinions, beliefs, and experiences of their customers; and
  - are not out of the ordinary.

- Ensure any claims in the reviews are substantiated.
- Obtain adequate permission to use the reviews and the customers' identities.
- Avoid rephrasing, changing, or taking customers' opinions out of context.

Companies should also use caution when aggregating online ratings to substantiate a claim or making claims about the aggregate number of high ratings to avoid deceptive claims.

For more information on customer reviews, see Practice Note, Consumer Reviews in the Era of Social Media.

Native Advertising

The legal and ethical issues around integration of brands into various content, sometimes called native advertising, have become a focus of regulatory concern with the increase in native advertising placed online. Digital media offer various opportunities to integrate brand messaging seamlessly into editorial spaces often blurring the line between content and advertising even more so than in traditional media. Native advertising on social media, particularly in form of influencer endorsements, also presents difficulties in distinguishing it from editorial content.

In response the rise of native advertising in online media, the FTC published:

- Native Advertising: A Guide for Businesses.
- Enforcement Policy Statement on Deceptively Formatted Advertisements (Policy Statement).

This guidance provides insight into the FTC's interpretation of what constitutes advertising and standards about how, where, and when disclosures must be made. Although the FTC does not formally define native advertising in this guidance, the Policy Statement notes that native advertising encompasses a broad range of advertising and promotional messages that match the design, style, and behavior of the digital media in which it is disseminated.

The guidance emphasizes that transparency is critical. The FTC clarifies that native advertising is deceptive when consumers do not realize that an advertiser is behind the content they are viewing. The more a native ad is similar in format and topic to content on the publisher's site, the more likely that a disclosure will be needed to prevent deception. A disclosure must be clear and conspicuous within the context of the native ad. Disclosures may be necessary on both the publisher's site and on linked pages where the content appears.

For more information on issues raised by native advertising, see Practice Note, Native Advertising.

Influencer Marketing

The FTC's Endorsement Guides provide guidelines to assist advertisers in meeting their legal obligations when using endorsements in advertising (16 C.F.R. §§ 255.0 to 255.6). Social media posts made by speakers who are sponsored by an advertiser, like influencers, are endorsements covered by the Endorsement Guides.

The FTC considers endorsers to be sponsored by an advertiser when a material connection exists between the advertiser and the endorser and a significant minority of the audience for an endorsement does not understand or expect the connection. A material connection is one that affects the weight or credibility the audience gives to the endorsement. Examples include paying influencers to engage on social media and providing consumers with free samples to review. The 2023 updates to the Endorsement Guides expand the definition of endorsers and endorsements on social media to include:

- Virtual influencers.
- Tagging.
- Fake positive reviews.

Sponsored endorsers must disclose their material connections to advertisers clearly and conspicuously on their social media posts. The updated Endorsement Guides provide a more restrictive definition of clear and conspicuous, clarifying that to be clear and conspicuous:

- Online disclosures must be unavoidable.
- An online disclosure cannot be hidden behind a "more" button or another link.
- Disclosures must be in the same format as the triggering claim (so if the claim is made both visually and verbally, the disclosure must be made in both formats too).

The FTC also explained that it considers the target audience (for example, children or the elderly) when determining whether a disclosure is clear and conspicuous.

The updated Endorsement Guide FAQs provide expanded examples of what constitutes a material connection and a clear and conspicuous disclosure (see FTC's Endorsement Guides: What People Are Asking). For example, providing early access to products and publicity opportunities can be material connections.

The updated Endorsement Guides indicate additional FTC enforcement priorities. They provide that, among other things:

- In addition to advertisers and endorsers being subject to liability for deceptive endorsements, intermediaries like ad agencies and public relations firms can be held liable for their role in creating deceptive endorsements.
- Endorsements in ads directed to children are of special concern because of the character of the audience. Practices that are acceptable for adult audiences may not be acceptable when directed to children.
- Certain practices relating to displaying, soliciting, and using consumer reviews may be deceptive (see Consumer Reviews).
- Review sites that make themselves appear independent, but are not, are deceptive even if they disclose that rankings are affected by payments.

In recent years, the FTC has increasingly scrutinized social media endorsements and settled numerous enforcement actions against advertisers that did not disclose their relationships with endorsers. Although the FTC primarily pursues advertisers for failure to post a clear and conspicuous material connection disclosure, it has also sent warning letters to influencers. In fact, to emphasize that influencers have liability, the FTC issued in 2019 both a guide and video directed to influencers about their disclosure responsibilities under the Endorsement Guides (see FTC: Disclosures 101 for Social Media Influencers and FTC: Do you endorse things on social media?).

FTC guidance on and enforcement of the Endorsement Guides as they relate to social media have made clear that companies wanting to avoid liability for engaging individuals to speak on their behalf in social media must:

- Establish a social media endorsement policy that complies with the Endorsement Guides.
- Train their employees, agencies, and endorsers on their policy.
- Monitor the posts of their endorsers.
- Correct failures to comply with their policy, including, if necessary, terminating their relationships with sponsored endorsers.

In addition, influencer liability is a current hot topic. For example, a number of investors have recently filed class actions against athletes and celebrities for their roles in promoting cryptocurrencies and non-fungible token projects (see, for example, *Huegerich v. Gentile*, No. 2:22-cv-00163 (C.D. Cal. 2022); *Adonis Real v. Yuga Labs*, 2:2022-cv-08909 (C.D. Cal. 2022); *Garrison v. Sam Bankman-Fried*, 1:22-cv-23753 (S.D. Fla. 2022)).

The SEC has also taken an interest in influencers promoting cryptocurrencies. For information on the SEC's role in pursuing influencers involved in promoting cryptocurrencies, see Legal Updates:

- SEC Settles Charges Against Paul Pierce for Unlawful Touting of Crypto Assets.
- SEC Settles Charges Against Kim Kardashian for Unlawful Touting of Crypto Assets.
- SEC Charges Celebrities and Crypto Entities Affiliated with Justin Sun with Securities Laws Violations.

For more information on the FTC's enforcement actions, see Practice Note, Advertising and Promotions in Social Media: FTC Investigations. For more information on working with social media influencers, see Practice Note, Social Media Influencer Marketing: Practical Tips for Managing Legal and Reputational Risks and Social Media Influencer Marketing Campaigns: Legal Issues Checklist.

Additional Issues

The increase in charitable promotions, health product claims, and dark patterns have caught the attention of regulators and self-regulatory programs resulting in guidelines to help companies navigate these areas.

Online Giving Portals

In June 2018, the FTC issued guidance on "giving portals," which include social media platforms, crowd funding websites, online retailers, and other online platforms that allow users to support charities directly through the online platform. In particular, the FTC advises that giving portals should clearly and conspicuously disclose prior to the user making a donation:

- Where the particular donation will go and who will distribute the funds to the designated charity.
- Whether there are any fees associated with using the giving portal by providing the total amount or percentage of the donation that will actually go to the designated charity.
- The time period in which it will take the donation to reach the designated charity and what happens if the portal is unable to successfully deliver the donation to the designated charity.

- Whether the donor’s personal information will be shared with the designated charity or anyone else, including the public.

Some states have also promulgated laws governing online giving portals, notably California.

Health Product Claims

The FTC issued new guidance for health product claims in December 2022, Health Products Compliance Guidance (Health Products Guidance) which updates and replaces the FTC’s previous guidance on dietary supplements from 1998. As noted in the introduction, the document "provides guidance from FTC staff on how to ensure that claims about the benefits and safety of health-related products are truthful, not misleading, and supported by science."

The Health Products Guidance makes two significant changes to the prior guidance:

- Applying far beyond dietary supplements, it applies to all health claims, whether for a supplement, drug, food, health app, or other health-related product.
- Although continuing to require competent and reliable scientific evidence as substantiation, it narrows that standard (except in limited circumstances) to high quality, randomized, controlled human clinical trials (RCTs) and provides detailed guidance on what constitutes a high quality RCT.

The Health Products Guidance also reiterates some basic, and very important, principles:

- The materials covered are broad, stretching across all advertising subject to truth-in-advertising requirements and includes: statements or depictions on packaging and labeling; promotional materials such as brochures or booklets; online and digital content; social media and influencer marketing content; statements in press releases, press interviews, or other media appearances; statements and materials at trade shows, conferences, and seminars; and statements made through healthcare practitioners or other intermediaries.
- All "parties who participate directly in marketing and promotion, or who have authority to control those practices, have an obligation to make sure that claims are presented truthfully and to check the adequacy of the support for those claims," may be liable for violations, including the marketers themselves, as well as individual owners and corporate officers of the marketer, ad agencies, distributors, retailers, catalog companies, infomercial producers, and expert endorsers.

For more detailed information the Health Products Guidance, see Practice Note, Substantiation of Advertising Claims: Health Claims.

Dark Patterns

Dark patterns have become a recent priority for regulators. Defined by the FTC as "design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm," the FTC warned marketers in a 2022 staff report that "these traps will not be tolerated." In the staff report, the FTC identified common types of dark patterns, and then gave recommendations to marketers about how not to engage in these types of practices. The report ended with a warning to marketers that, "[w]hile dark patterns may manipulate consumers in stealth, these practices are squarely on the FTC's radar."

The FTC report identified several categories of dark patterns, including:

- **Design Elements That Induce False Beliefs.** This type of dark pattern is one that uses "design elements that induce false beliefs." This type could be something as simple as a false claim or it could be a design element that "creates a misleading impression to spur a consumer into making a purchase they would not otherwise make."
- **Design Elements That Hide or Delay Disclosure of Material Information.** This type of dark pattern uses design elements to "hide or delay disclosure of material information." The FTC explained that some dark patterns operate by "hiding or obscuring material information from consumers, such as burying key limitations of the product or service in dense Terms of Service documents that consumers don't see before purchase."
- **Design Elements That Lead to Unauthorized Charges.** This type of dark pattern uses design elements that "lead to unauthorized charges." The FTC described it as a "common dark pattern" that "involves tricking someone into paying for goods or services that they did not want or intend to buy, whether the transaction involves single charges or recurring charges."
- **Design Elements That Obscure or Subvert Privacy Choices.** The FTC described this type as a "pervasive dark pattern" that uses design elements to obscure or subvert consumers' privacy choices. The FTC explained that, because of this dark pattern, "consumers may be unaware of the privacy choices they have online or what those choices might mean."

The FTC gave a number of examples of ways in which companies incorporate dark patterns into their products, and steps marketers should take to avoid regulatory scrutiny. For more information on dark patterns, see Article, Dark Patterns: Trends and Developments.

END OF DOCUMENT

