Concurrences
Antitrust Publications & Events

orrick

ANALYSIS GROUP

Jon Direnfeld
Partner
Orrick
Washington, DC

Andrew Smith
Director
Bureau of Consumer Protection,
Federal Trade Commission
Washington, DC

Moderator:
Aaron Yeater
Managing Principal
Analysis Group
Boston

Platforms and Advertising: Implications of Digital Advertising for Competition and Consumer Protection

Webinar - 08 October 2020*

The speakers focused on the competition law analysis of advertising markets, while discussing implications for communications and technology law, and consumer protection regulation as well.

Panel Discussion

Moderator, **Aaron Yeater** (Analysis Group) began the discussion by noting the qualities unique to digital advertising. Digital ads involve a certain reliance on digital data generated by users or collected by third parties to use at some point in a different process. Data is used primarily to target and deliver ads to the individual, and verifying when a sale or conversion occurs as a result of a click or watching a video. The digital environment also increases the flow of information online, which opens up room for more potentially misleading information, whether intentional or not. At the same time there are more opportunities for firms to make disclosures and inform consumers on what they need to know. The choices to be made about what prominence to give those inform a lot of the relationship between advertising and marketing and disclosing information to consumers. Finally, digital advertising in the context of digital e-commerce affords opportunities for smaller firms or entrants to reach consumers they would otherwise not have reached, which is good from a competition point of view, thought it comes with corollary effects.

"ONE OF THE IMPORTANT THINGS THAT WE TALK WITH CLIENTS ABOUT THAT IS THAT YOU NEED TO HAVE SYNERGY BETWEEN THE LEGAL AND BUSINESS SIDES TO MAKE SURE THAT AS COMPANIES MOVE INTO NEW VERTICALS OR NEW AREAS, THAT IS ALIGNED WITH WHAT THEY ACTUALLY HAVE IN THEIR TERMS OF SERVICE..."
JON DIRENFELD

Mr. Yeater also brought up the question of whether ads should be viewed as a financing mechanism for content, or whether they should be viewed as part of the overall integrated user experience. He observed that this question is important to wrestling both the competition and consumer protection issues raised with cases involving digital advertising.

* Concurrences drafted the present synthesis. The views and opinions expressed in this Document do not necessarily represent those of the speakers' institution or clients.

The moderator then turned to **Andrew Smith** (U.S. Federal Trade Commission) to discuss his views from a law enforcement standpoint. Mr. Smith explained three general concerns raised by online digital advertising, including privacy, regulation of ads, and disclosures associated with products sold online.

"THINGS ARE CONSTANTLY CHANGING. FIVE OR TEN YEARS AGO, WE WOULD HAVE TALKED ABOUT BANNER ADS AND PAID SEARCH AND OPEN DISPLAY; NOW WE ARE TALKING ABOUT MOBILE; AND WHO KNOWS WHAT WE ARE GOING TO BE TALKING ABOUT TOMORROW?"
ANDREW SMITH

With respect to privacy issues, Mr. Smith spoke about the Commission's enforcement action against YouTube and Google for dropping cookies and tracking users of child-directed content to target ads, in violation of the Children's Online Privacy Protection Act (COPPA). He explained that COPPA prohibits the collection and use of personally identifiable information (PII) about children without getting verifiable parental consent for the collection of that information.

Mr. Smith also spoke about the Commission's authority to bring action against deceptive practices by companies. As an example, he mentioned the FTC's action against Facebook in which Facebook was fined a $5 billion penalty, and ordered to engage in privacy impact assessments and create a board to oversee privacy matters. In that case, the FTC alleged that Facebook engaged in a deceptive act by collecting personal information from its users purportedly to be used for multi-factor authentication for security purposes, while actually using that information to target ads, in addition to the multi-factor authentication. Facebook's deception lay in the fact that it failed to notify users that the information collected would be used for targeted marketing. Facebook also engaged in a deceptive act by telling its users that it provided settings that would limit the sharing of information to a particular audience, such as friends, when in fact, that information was also being shared with apps that were used by the users' friends, allowing app developers, like Cambridge Analytica, access to personal information through that backdoor.

Mr. Smith then discussed other forms of advertising that the Commission has been actively going after. When it is difficult to distinguish between an ad or content, the general rule is that if it is an ad, it should look like an ad and tagged as a "sponsored content." The same would apply to influencers with "hashtag sponsored." The Commission has also gone after ranking and ratings sites that claim to rank, for example, the best student loan companies when in fact their ranking is not based on price or performance but on how much the company paid the ranking site. Mr. Smith also noted affiliate marketing and lead generation as issues unique to the digital advertising space, and that the Commission holds advertisers liable for misrepresentation made by their lead generators (entities publishing these ads), even if they are two or three generations removed from the advertisers.

To better understand the digital ad marketing industry, Mr. Smith informed that the Consumer Protection Bureau has compelled Internet service providers to turn over information about how they collect, use, and share information under Section 6(b) of the Federal Trade Commission Act. The Bureau is also in the process of creating a "digital markets intelligence unit" by hiring digital marketing professionals and businesspeople who understand the inventory side of digital marketing.

Next, **Jon Direnfeld** (Orrick) discussed general advice he provides to his clients to defend against challenges brought by enforcement agencies in the digital advertising space.

Mr. Direnfeld advises marketers that the claim on the ads must be able to stand on itself to the extent possible and not rely heavily on disclaimers and qualifications that are not attached to the actual claim on the ad itself. If additional qualifiers are needed, the best practice is to include it directly or closeby the claim. For influencers, he suggests putting the sponsored hashtag clearly up-front rather burying it under a cascade of hashtags or below the jump on an Instagram or Facebook post. Ratings and review sites should make it clear in the review itself that it is a paid review, and not relying on disclosures made in the terms and conditions stating that the site makes compensation from some of the entities it reviews. He observed that marketing teams are usually very creative, and if pushed, can come up with better solutions.

Additionally, Mr. Direnfeld advises that companies must have reasonable substantiation for anything claimed on an ad. In the digital space, there are smaller potential areas for text or pictures, and companies must ensure that they have reasonable substantiation based on the actual experience relating to the product, particularly if an ad contains a picture may give a certain perspective. The more objective a claim is, the higher the level of substantiation may be.

Sometimes, companies may fare better if they substantiate the claim through rigorous data that is related to consumer experience with the product.

Mr. Direnfeld also spoke broadly on issues relating to consent. Companies, when collecting or disclosing data, must ensure that they accurately inform users of the purpose for collecting such data and its use. He observed that sometimes, innovative start-up companies that are quickly developing, fail to look back on their initial terms of services to properly reflect the practice that they are engaging in the present. As companies grow, they must review and update their policies accordingly and obtain the requisite consent to move into new areas. In getting user consent, companies should try to obtain it in a manner that is as close as possible to express consent, such as having the user affirmatively click a checkbox, and not by relying heavily on quick clickwrap agreements or click-through agreements. However, Mr. Direnfeld stated that it is not a silver bullet and that obtaining consent depends on how the company frames it. If it is just simply "click here to agree to our terms of use," that is better than a clickwrap, but there may still be issues of whether the terms of use are clearly presented in a manner such that a reasonable consumer would understand it.

"IT IS A LOT HARDER TO KNOW WHAT WILL HAVE AN IMPACT ON CONSUMERS BECAUSE THE CONSUMERS THEMSELVES ARE DRIVING THEIR DECISIONS ABOUT WHAT INFORMATION TO COLLECT, WHERE TO COLLECT IT, WHO TO BELIEVE, WHEN TO BELIEVE THEM, AND WHAT TO DO ONCE THEY HAVE THE INFORMATION."
AARON YEATER

The moderator, then, asked the panelists to discuss the relationship between competition and consumer protection in digital advertising.

Mr. Smith said that if there is tension, it derives from the privacy issues discussed earlier and advertisements that don't fully disclose the price and material conditions of the product to the consumers. He suggested that privacy should be considered a non-price component of consumer welfare. Therefore, merger analysis should include whether there are risks to consumers' privacy associated with the transaction. Another tension is that competition law might favor the sharing of data to increase competition, whereas pro-privacy policies would be to lock information down, and collect and disclose as little data as possible.

Mr. Yeater commented that from an economic perspective, privacy as an aspect of quality is a sensible approach, but that there is no particular consensus in economic literature on how much consumers ultimately value privacy. However, Mr. Yeater believes that consumers care about privacy in particular ways and they feel like they receive the "right" kind of privacy from particular actions. He mentioned that Catherine Tucker, a researcher at MIT, found that if consumers' expectations of the use of their data are consistent with how they are actually used, then consumers will be more comfortable with sharing a certain amount of information. When the use does not comport with consumer expectation, then there may be more concern for consumer privacy. Mr. Yeater believes we are going to have to apply very industry-specific and tool-specific expectations about the interaction between privacy and competition.

Mr. Direnfeld commented that from a competition perspective, it would be difficult to put a uniform price on data privacy in a merger review, which would make it hard to predict whether a merger would be approved. On the consumer welfare side, the perception of privacy can change based on the nature of the company and the nature of the data.

Questions & Answers

One attendee asked Mr. Smith whether the FTC uses AI/IT tools to discover unfair practices and how the FTC uses online mystery shopping.

As to the first part of the question, **Mr. Smith** stated that the Commission welcomes such tools. He explained that during the beginning of the pandemic, the Commission looked for domain names that had various spellings for the terms "coronavirus," and "Covid" using web crawlers, to weed out possibly deceptive advertisements claiming to treat or detect coronavirus. Another area where such tools might help is in social media. Mr. Smith explained that some ads

pop up and disappear so quickly on social media that the Commission is unable to investigate those marketers even if consumers have been injured by it. As for mystery shopping, Mr. Smith said that his bureau does not always need to mystery shop in order to find violations, but it does do a lot of undercover buys.

Mr. Yeater commented that using investigatory options that technology provides gives rise to opportunities to evaluate questions being asked during an investigation or in litigation that are different as a result of the data that exists. For example, when obtaining user consent, explicit consent is always preferable, but sometimes, through data, companies may be able to infer consent about the way people behave *ex post*. Mr. Yeater also raised the issue of experiments or exercises undertaken for litigation purposes that may be done in real-world contexts. Companies must establish the extent user activity will become part of data that they provide to agencies or litigation, but there are increasing discussions about what kinds of data a company has to evaluate the materiality of those disclosures before or during the litigation process.

Mr. Direnfeld added that there are digital advertising tools, both from an advocacy standpoint as well as a compliance standpoint, that can be used in terms of both monitoring click-through rates and disclosures, for instance. If a company relies on hyperlink disclosure, the FTC Guidelines identify monitoring click rates as an effective method of compliance. If a company has a high click rate, then it can feel relatively better about the fact that people are actually seeing the hyperlink and clicking through the disclosure.

Another attendee asked: "From an economic perspective, would it be fair to apply the concept of bounded rationality to privacy? Consumers might value more privacy in certain situations than others." **Mr. Yeater** commented that the question was interesting to him because it almost implies that when consumers care about privacy, it is rational, and when they don't it is not, which he was unsure is the case. He thought that there are instances in which consumers can have a preference for having their data treated in a particular way, but they are weighing that against other kinds of commercial activity. **Mr. Smith** commented that one way the U.S. has addressed privacy concerns without a standard privacy protection statute is by regulating specific types of information collected (i.e. financial, medical or information from children). Another approach is through the Fair Credit and Reporting Act. **Mr. Yeater** commented that one way to address some of the questions raised is by thinking through the remedies to improve privacy. If the expectation is that a merger is going to concentrate data from people who would prefer to not have their data concentrated, then presumably rejecting that merger will remedy that problem. But there are some cases where it is not too obvious that the potential remedy imposed to enhance competition will enhance privacy. **Mr. Smith** added that the FTC has not gotten to the point where the agency considers data concentration and the risk to consumers presented by merging two data sets.

Finally, an attendee asked the panelists to what extent unfair trading practices are considered and distinguished from competition/antitrust law. **Mr. Yeater** mentioned California's Cartwright Act as an unfair competition law, which is different from antitrust law. From an economic point of view, he would distinguish these unfair trading practices to the extent that they are meant to privilege one competitor over another, but do not arise from the exercise of market power. An example of an unfair trading practice would be if a hot dog stand burned down its competitor across the street solely for his or her own benefit, while a hot dog monopolist would fall into the antitrust world. He pointed out that the lines get trickier between unfair trading practices and antitrust law if being a hot dog monopolist allowed the monopolist to do something that would destroy competition. **Mr. Smith** added that if the hot dog stand advertises that it sells kosher hot dogs when in fact it does not, this would constitute deceptive trade practice. The focus here is whether there are substantial harms to consumers that cannot be avoided by the consumers, and that do not have any offsetting benefits to consumers or to competition. Additionally, **Mr. Direnfeld** said that privacy and data security are critical due diligence aspects of any acquisition since the merging party will inherit the data security practices as well as the liabilities of the acquired firm. On the privacy side, he stressed the importance of obtaining consumer consent for the actual practice a firm is engaged in. In carrying out due diligence, the acquiring firm must also consider the privacy policy of the firm it is purchasing, and obtain user consent for data collection and use that diverges from the policy. ■