

Posted by AdExchanger.com on
April 16, 2010 In The Debate



Targeting Real-Time Targeting: Privacy Groups File Overreaching Suit with the FTC Against Real-Time Behavioral Advertising

By: Ed Zimmerman, Mark Kessler, and Matthew Savare
Lowenstein Sandler PC
www.lowenstein.com



April 16, 2010



Targeting Real-Time Targeting: Privacy Groups File Overreaching Suit with the FTC Against Real-Time Behavioral Advertising

By: Ed Zimmerman, Mark Kessler, and
Matthew Savare

Lowenstein Sandler PC
www.lowenstein.com

April 16, 2010

Let's say you're surfing the web, planning your next vacation with the family. You visit several travel sites, book your plane tickets and hotel, and rent a car. You also read some reviews and blogs about your destination, the local restaurants, and nightlife. You then Tweet about it and go to Facebook where you reconnect with one of your friends who lives in the area you're visiting. From the searches you've run, it's clear that you're going to the French countryside and you're interested in activities for the family, with a winery visit or two.

After playing around on the social networking sites, you decide to do more research for your trip. Given the way the Internet now works, you expect – actually, you know definitively – that you're going to be served some ads to help pay for all this free information you're getting. And now comes the fundamental question: would you rather get served an ad about the best local dining, a great idea for a day trip near your destination, or ads for a wonder drug that's totally inapplicable to you?

It seems too obvious to even ask the question, but recently, several privacy groups filed a legal action seeking to ensure that we continue to receive those wonder drug ads, technological advances be damned! These self-appointed privacy advocates seek to stop – or at least greatly curtail – the natural evolution from irrelevant online ads that are pushed at you (and millions of other

"Overzealous privacy advocates have been striving for years to shutdown advances in online advertising though, ironically, these same groups would be outraged were web content to become materially less free because consumers would have to pay for their content in cash – talk about financial harm to consumers!"

uninterested consumers) to smarter ads that are contextualized and served to you based on your preferences, interests, and needs.

The Latest Attack on Online Advertising

On April 8, 2010, three privacy groups jointly filed a complaint with the Federal Trade Commission ("FTC") alleging that certain online profiling and targeting practices – including real-time auctions of individual ad impressions – constitute unfair and deceptive business practices. In their complaint, the Center for Digital Democracy, the US Public Interest Research Group, and the World Privacy Forum request that the FTC investigate a number of behavioral advertising and related companies, enjoin them from certain types of behavioral advertising, award consumers compensatory damages, and require any real-time tracking and bidding system to take greater steps to protect the privacy and economic welfare of US consumers.

About the Authors:

[Ed Zimmerman](#) Chairs the Tech Group at Lowenstein Sandler, a nationally-recognized law firm that has closed hundreds of venture deals in the last several years, teaches Venture Capital & Angel Investing to MBA Candidates at Columbia Business School, actively angel invests, and chairs [First Growth Venture Network](#). [Mark Kessler](#) runs IP for the Tech Group at Lowenstein Sandler and co-chairs the firm's IP Litigation Group. Prior to that he was Chief IP, Technology & Sourcing Lawyer worldwide for JPMorganChase. He too angel invests actively. [Matt Savare](#) specializes in privacy, IP, and media at the Tech Group at Lowenstein and is a frequent author and lecturer on the subject.

Contact them at: ezimmerman@lowenstein.com; mkessler@lowenstein.com; and msavare@lowenstein.com or on the web at www.lowenstein.com

Lowenstein Sandler makes no representation or warranty, express or implied, as to the completeness or accuracy of this article and assumes no responsibility to update this article based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. Readers should consult legal counsel of their own choosing to discuss how these matters may relate to their individual circumstances.



The sweepingly broad complaint attacks numerous aspects of online advertising ranging from ad auctions to cloud computing. It is the latest in a decade-old string of legal challenges to behavioral advertising, but this time with an emphasis on the industry's push towards optimizing real-time bidding using real-time conversion data.

The Complaint & Oscar Wilde

The complaint focuses primarily on recent technological developments that have enabled online advertisers to more quickly, efficiently, and precisely target ads to individual users. The complaint also provides a veritable who's who list of hot companies in the sector. At a time when many investors and potential customers/partners/acquirers are trying to ascertain which companies are the leaders in behavioral targeting and tracking, one wonders whether the complaint isn't a roadmap spotlighting the best of breed companies in the field, raising the interesting question (stolen a bit from Oscar Wilde): If you are doing behavioral targeting, is it better to have been named in the complaint or to have been overlooked?

In terms of substance, the complaint targets real-time bidding ("RTB"), which permits advertisers and publishers to buy and sell individual display ad impressions in near real-time with the use of various targeting parameters, including geographic location, behavioral data, and information concerning the context of the ad in the page. For the advertising industry, RTB represents a seismic shift (and improvement) from the world of reserved bidding where buyers of online ads bid on future publisher placements and hope that the publisher or ad network will deliver their targeting parameters correctly.

Similar to the reasoning privacy advocates used when they complained to the FTC in 2007, this complaint repeatedly claims that the "stealth" aggregation, combination, and use of consumers' online viewing habits threaten users' privacy. However, the privacy groups do not set forth one concrete example or articulate – even in a general sense – how behavioral advertising impacts users' privacy. Instead they rely on nebulous allegations of undefined threats to autonomy and privacy.

The complaint also sets forth several additional issues that had not been previously raised to the FTC. For example, the groups strangely allege that housing the data in a "cloud" heightens security risks. This seems like a purely Luddite perspective – does housing data in one server

really provide greater data protection than spreading data across numerous servers? Not surprisingly, the groups don't supply any support for their assertion.

The complaint also emphasizes that more companies are combining online behavioral data with data residing in databases (like those of Nielsen and Experian) of the physical world. They allege that an advertiser's compilation, generation, and sale of more information on a given user compromise that user's privacy. They also highlight the fact that the ad exchange system that originated in the online world has migrated to the mobile space, making targeted advertising nearly ubiquitous, as if to say that it breaks some natural law prohibiting the matching of offline, online, and mobile data. We understand that compiling increasing quantities of data means that the holders of that data know more about you, but is that really a detriment to the consumer? How many of us rate movies on Netflix or songs on Pandora with the understanding (or hope) that the engines will more accurately understand what we like in order to make more compelling suggestions?

One of the authors recently lamented that he was served an ad by a music service. He didn't mind receiving the ad; he had not subscribed for premium service, and therefore he understood the bargain he had made. He did, however, mind that the ad indicated that the server believed him to be far older than he actually is (given the advertised product). This left him wondering whether his musical preferences gleaned by that service from scores of hours and dozens of ratings were too unhip (answer: probably). He took some comfort in thinking that the site lacked a great targeting engine (maybe it should begin working with one of the companies highlighted in the complaint!). If the targeting had, in fact, depressed him because it forced him to come to terms with the fact that his musical taste was stuck in 1983, the FTC's standards wouldn't recognize that as harm of the type the law was designed to prevent; even the complainants acknowledge that "emotional harm" doesn't count, as they articulate the standard for the FTC to find "consumer injury:"

The injury must be "substantial." Typically, this involves monetary harm, but may also include "unwarranted health and safety risks." Emotional harm and other "more subjective types of harm" generally do not make a practice unfair. Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit

that the sales practice also produces.” Thus the FTC will not find a practice unfair “unless it is injurious in its net effects.” Finally, “the injury must be one which consumers could not reasonably have avoided.”

In the most far reaching of their claims, the groups argue that the “open marketplace” that has developed to buy and sell behavioral ad data has created a financial windfall for publishers, ad agencies, and marketers that “capitalize” on consumer data. The groups contend that this unauthorized use of data causes consumers financial loss and losses to their privacy and autonomy. However, the complaint does not specify or even attempt to explain the nature of this alleged financial loss. Put simply, the ad industry’s ability to profit from the use of consumer data does not mean that consumers are financially harmed. As noted below, the exact opposite is true.

Similarly, the complaint asserts that consumers are not adequately compensated for the use of their data. This type of claim begs several important questions. For example, how – if at all – do the groups value the enormous amount of ad-supported, free content and services made available to consumers on a daily basis? Aren’t the hundreds of millions of online users already receiving consideration for their information?

Ultimately, the groups ask the FTC to do the following:

1. Compel companies involved in real-time online tracking and auction bidding to employ an “opt-in” regime, as opposed to the standard “opt-out” process;
2. Require that these companies amend their privacy policies and business practices to acknowledge that tracking and real-time auctioning involve personally-identifiable information;
3. Require that consumers receive “fair financial compensation” for the use of their data;
4. Prepare a report that informs consumers about the privacy risks and consumer protection issues involved with the real-time tracking, data profiling, and auctioning, including sections devoted to financial and health marketing and data involving 13-17 year olds; and
5. Address the potential that companies may “redline” information to certain consumers (*i.e.*, withhold editorial content to consumers based on an assessment of their economic value derived from data obtained by tracking and profiling them).

The Implications to the Advertising and Data Industries

Despite the breadth of the complaint, many of its allegations were raised to the FTC years ago. Based on those objections from 2007, the FTC, in February 2009, issued a report titled “Self-Regulatory Principles for Online Behavioral Advertising.” In July 2009, a group of the largest media and marketing trade associations, including the Association of National Advertisers, the Direct Marketing Association, and the Council of Better Business Bureaus, responded to the FTC report with its own report of the same name.

Basing its report largely on the FTC report, the consortium set forth the following seven principles for companies to follow when utilizing behavioral advertising.

1. Transparency – Third parties and service providers are to provide “clear, meaningful, and prominent notice on their own websites that describe their behavioral advertising data collection and use practices.” This is a significant change for many companies, which tend to bury these disclosures in their privacy policies. More prominent disclosures would minimize the risk that the FTC would hold the practice to be deceptive or unfair.

In January 2010, in an effort to simplify and standardize the disclosure process, the advertising industry agreed on a standard icon — a white “i” surrounded by a circle on a blue background — that companies using behavioral advertising should add to their online ads to inform consumers how their data is being collected and used. The icon, which companies plan to add to their online ads by mid-summer, would be accompanied by a phrase such as “Why did I get this ad?” When consumers click on the icon or the phrase, they will be redirected to a page that explains how the advertiser used their online history and demographic information to send them targeted ads.

2. Consumer Control – Third parties should allow consumers to choose whether their data is collected and used for behavioral advertising. Service providers should not collect and use data for those purposes without first obtaining the consumer’s consent, which, once granted, should be made easy to withdraw. Again, that kind of process tends to negate any implication of unfairness or deception.

3. Data Security – Entities should use “appropriate” physical, electronic, and

administrative safeguards to protect consumer data, and should retain data only as long as necessary to fulfill a legitimate business need or as required by law. In addition, service providers, among other things, are to anonymize, alter, or randomize any consumer personally-identifiable information or unique identifiers to prevent it from being reconstructed.

4. Material Changes to Existing Behavioral Advertising Policies and Practices – Before applying any material change to their data collection and use policies with respect to behavioral advertising, entities are to obtain a consumer’s consent.

5. Sensitive Data – Entities should not use behavioral advertising directed to children they have actual knowledge are under thirteen, except as permitted by the Children’s Online Privacy Protection Act. In addition, entities should not collect personal information from children they know to be under thirteen or from sites directed to children. Regarding other forms of “sensitive data,” entities should not collect and use Social Security Numbers, financial account numbers, drug prescriptions, or medical records for behavioral advertising without the consumer’s consent.

6. Accountability – The industry report notes that its principles are self-regulatory in nature, and apply to the more than 5,000 companies that belong to any of the sponsoring organizations. It also stipulates that monitoring, reporting, and compliance programs need to be put into place to process complaints, ensure transparency, and promote compliance.

7. Education – The report encourages entities to participate in educational and outreach programs to instruct individuals and businesses about behavioral advertising.

Current Law & Where We Go Next

Although we believe that the complaint truly misses the mark, it does rightfully point out that behavioral advertising and tracking companies should focus on providing clear and prominent disclosures to their customers. This principle was highlighted last year when the FTC filed a complaint against Sears Holdings Management Corporation (“SHMC”) for unfair and deceptive business practices relating to SHMC’s operation of the sears.com and kmart.com websites. In connection with a marketing initiative, users of those sites were invited to join the “My SHC Community,” which contained a program that

collected information on nearly all of their online activity. However, SHMC had not prominently disclosed this tracking functionality at the time users joined. Instead, SHMC made the disclosure in the middle of an end user license agreement.

In a ruling that departed from the legal precedent that full disclosure does not constitute an unfair or deceptive business practice, the FTC deemed SHMC’s otherwise complete disclosure to be insufficient in light of consumers’ expectations and the amount and detail of information SHMC was collecting. SHMC ultimately consented to an order from the FTC requiring that prior to a consumer downloading or installing any tracking application, SHMC make clear and prominent advance disclosure of how and what they track – separate and apart from any privacy policy or terms of use – and that the consumer consent to the downloading of the tracking application.

Wrap Up

Targeting is not an innovation -- sellers have targeted potential customers since the practices of buying consumer goods and services first arose. The complainants seem upset that we’ve just gotten increasingly good at it. When targeting is practiced responsibly, it provides an enhanced user experience without any meaningful damage to consumers. Overzealous privacy advocates have been striving for years to shutdown advances in online advertising though, ironically, these same groups would be outraged were web content to become materially less free because consumers would have to pay for their content in cash – talk about financial harm to consumers!

Even if the April 8th complaint never reaches the stage of formal FTC rulemaking, the commission will likely continue to bring individual enforcement actions related to behavioral advertising and similar practices, without attempting a wholesale ban on targeting. In that case, the SHMC consent agreement and future proceedings would establish the compliance framework within which companies would need to operate in order to avoid FTC action. Individual enforcement actions focused on specific misconduct make sense. In light of the FTC’s existing guidelines and industry’s self-regulatory regime, the April 8th complaint’s broad indictment of online technological advances, which most targeters are employing responsibly, is simply unwarranted.