The Layered FTC Approach to Online Behavioral Advertising

Info 205 – Information Law and Policy
Michael Lissner • 2 April 2009

Since the creation and proliferation of the Internet, online advertising and online electronic commerce (known as e-commerce) have thrived.[1] Indeed, it would probably not be going too far to claim that the success of today's Internet could in part be attributed to their success, as many of the core features of the Internet rest in many ways upon the shoulders of these giants.[2] Since the creation and invention of the first online advertisement, the types and prevalence of many of the advertisements we see online have become both more varied and more sophisticated. While the first ad was a simple banner advertisement for a third party company,[3] as the Internet has grown in popularity, advertisements have grown in complexity, with many parties involved, often in less than obvious ways. As a result of these changes, in 1998, the Federal Trade Commission (FTC) published Fair Information Practices for the Web,[4] and in early 2009, it published a staff report speaking directly to the issues of online advertising.[5]

---

1 In 2008, revenue for online advertising continued to climb, and was up more than 10% from 2007, with revenue at $23B. See Jones, K.C. *Online Ad Revenues Break Records In 2008*, March 30, 2008, accessed online at http://www.informationweek.com/news/internet/ ebusiness/showArticle.jhtml?articleID=216401797

2 See http://www.historyoftheinternet.net/history_of_internet_advertising.html.

3 Reid, Robert H., Architects of the Web, John Wiley & Sons, Inc., 1997, at 282.

4 *Online Privacy: A Report to Congress*, accesssible online at www.ftc.gov/reports/privacy3/priv-23a.pdf

5 *Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting and Technology*, accessible online at: http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

Together, these two documents form a regulatory framework for those companies that wish to advertise online, however, since it does not appear that the Behavioral Principles were drafted with the Fair Information Principles firmly in mind, the ways that the two documents regulate are not always in agreement. From a consumer's perspective, this is not necessarily a bad thing, as, where one document does not regulate, the other can serve as a safety net, but from an industry perspective, such layered regulation can be convoluted and burdensome.

This burden is best exemplified by third party advertising, which is at the core of the Behavioral Advertising document, and which requires careful analysis before it can be used. But before we analyze the application of the principles to third party advertising, we should begin by explaining the many types of advertising that are laid out in the Behavioral Advertising Principles. There are three central types that are described: Contextual, First Party, and Third Party,[6] which will be explained in turn. Generally speaking, advertisers create *Contextual Advertising* by analyzing the content or use of a website in order to generate and display an advertisement that has relevance to that website. A simple example of this are the advertisements that are shown on the results page of most search engines, where a search for "flowers" likely yields an advertisement for flower distributors, or perhaps local florists. Examples of *First Party Advertising* are common on sites such as Netflix and Amazon, where recommendation systems analyze your use of the site to recommend products you may desire. This is distinct from contextual advertising because the advertisements shown are only for the site you are currently browsing, whereas contextual advertisements could be –

6 Ibid at 26.

and often are – for products or services of third parties. The third type of advertisements are third party advertisements. In these, there are generally three parties involved in the transaction. While you browse the web site of one party, another party – the online advertiser, also known as the third party – uses a number of factors about you and your online history[7] to show you ads for yet another party.

In discussing the applicability of the Online Behavioral Principles for contextual and first party advertisements, the FTC took a liberal approach, declaring that their creation entails a minimum security risk while providing a maximum level of transparency. This is because from the consumer perspective, it is not hard to understand where such advertisements come from, nor is there a great risk of data loss or interception. This makes industry compliance fairly straightforward, since as a result only the 1998 Fair Information Principles apply.

As mentioned above, however, where things become more complicated is with regards to third party advertisement arrangements. To accomplish this kind of advertising, organizations generally use third party web cookies, which deserve explanation as well. Web cookies are small files that can generally be silently placed on a user's computer as they browse the web, and which can serve to uniquely identify and track individual users as they browse from one web site to another.[8] Such methods of advertising bring with them a number

7 Since these advertisers have no concept *you*, here we should technically speak of your browser and its history, but we turn our attention to this matter in time.

8 Most cookies of this sort, for example, contain a simple string of characters that serve as your identity, much like a license plate does on an automobile. According to RFC 2109, browsers should support at least 300 cookies, no more than 20 from a given site, and no more than 4096 bytes each. This means that for compliant browsers, at maximum a site could set twenty cookies containing a total of approximately 27,000 characters.

of privacy concerns, and the Behavioral Advertising Practices call for the following four regulations: (1) Transparency and Consumer Control, (2) Reasonable Security, and Limited Data Retention (3) Affirmative Express Consent for Material Changes to Existing Privacy Policies, and (4) Affirmative Express Consent (or Prohibition Against) Using Sensitive Data for Behavioral Advertising.[9] While each of these principles lays out important protections for users, from an industry perspective, they can be challenging in practice. Further, since this and the Fair Information Practices document are layered in their application, in addition to these principles, the Fair Information Principles lay out at least another two regulations that must be followed: (1) Access/Participation, and (2) Enforcement/Redress.[10]

To follow all of these principles across these documents, an organization utilizing third party advertising must follow a fairly regimented process that attempts to maximize user control and understanding while staying within the writ of the law. Such a regimen would likely begin by "provid[ing] a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose."[11] Ideally, such a statement would be provided before any information is gathered from the user, which would entail suppressing third party advertisements at a site until after a user has

9 *Online Behavioral Advertising* at 46-47.

10 *Fair Information Practices* at 7. Technically, there are a total of five principles that can be drawn from this text, however many of them overlap with the *Behavioral Advertising Principles,* and so we shall not address them in depth here.

11 *Behavioral Advertising* at 46.

agreed to its terms. While this appears to be good policy on paper, as Commissioner Harbour states in her concurring statement, "Disclosures about information collection, use, and control are not meaningful if they are buried deep within an opaque privacy policy that only a lawyer can understand."[12] Unfortunately though, that is likely how such a statement would be made, since so many statements of this type are now required. One alternative to this approach is to build consent and awareness functionality into the browser itself. There is a Firefox extension that accomplishes just this, displaying a warning whenever information is being requested or sent to a third party advertiser.[13] With cooperation of the advertising organizations, such functionality could easily be extended to include transparent and obvious consent agreements.

Assuming however, that a user understands such an agreement, is presented with it, and agrees to it, the next step along the third party advertising regulatory-compliance-pathway is to determine whether sensitive information is used in the scope of the advertising. Here, the Behavioral Advertising Principles analyze what is considered personally identifiable information (PII) and non-personally identifiable information (non-PII). As a result of a number of industry scandals and academic reports over the years,[14] the FTC took a

12 Concurring Statement of Commissioner Pamela Jones Harbour, at 4. Accessible online at www.ftc.gov/os/2009/02/P085400behavadharbour.pdf

13 See http://www.ghostery.com/ or https://addons.mozilla.org/en-US/firefox/addon/9609.

14 For more information, see Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, New York Times, Aug. 9, 2006, available online at http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&scp=1&sq=aol%20queries&st=cse&oref=slogin; Ellen Nakashima, *AOL Takes Down Site With Users' Search Data*, Washington Post , Aug. 8, 2006, available at http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080701150.html; Bruce Schneier, *Why "Anonymous" Data Sometimes Isn't*, Wired, Dec. 13, 2007, available at http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213

firm line on this matter, identifying that the distinction is not always clear. As such, advertisers must carefully analyze whether personal information about a user could be combined with other information to uniquely identify the user. If this is the case, then the information is considered PII, and, as indicated above, "Affirmative Express Consent (or Prohibition Against) Using Sensitive Data for Behavioral Advertising" must be gathered from the user. At this point, industry may again be haunted by Commissioner Harbour's warning not to bury that consent "deep within an opaque privacy policy."

Next, with the above analyses and consents successfully completed, the path to third-party advertising has not yet reached an end. The final step that must be completed is to analyze the 1998 Fair Information Principles, which in addition to overlapping in many ways with the items above, also call for "1) Access / Participation, and (2) Enforcement / Redress."[15] To complete the first of these two steps, an online advertiser must ensure that users are able "to view the data in an entity's files...and to contest that data's accuracy and completeness."[16] Currently, this is not possible. To comply with the Fair Information Practices however, this information needs to be provided in an open and transparent manner.

For the final point, in what is a complicated, but mostly workable set of regulations, the industry needs to have a mechanism in place to enforce all of the above principles. The industry has thus far created the Network Advertising Initiative (NAI),[17] which is an initial approach to enforcement, but it is limited by a number of problems. First, its enforcement

15 *Fair Information Practices* at 7.
16 Ibid at 9.
17 See http://www.networkadvertising.org.

power is limited by the quantity of its member organizations – if an advertiser is not a member, they are not regulated by this body[18]. Second, the NAI does not complete third party evaluations of its member organizations, as is recommended by the Fair Information Practices, leaving the results of its own evaluations in question. Third, any non-compliances of organizations have not been publicly published thus far, although promises have been made to do so in an annual report beginning in 2009.[19] Finally, it does not seem clear that the evaluations of the member organizations are done on a random or surprise basis, thus allowing the organizations to prepare for the evaluation, and possibly game the system.

An additional number of problems arise from the scenarios described above. First is the security of the information that is being gathered by the third party advertisers. Although the FTC is at pains to describe how a number of pieces of seemingly non-PII can be combined to create PII, they do not address the fact that while one online advertiser may collect my first name only, another may collect my last name only. Although each advertiser may have concluded that alone the information was not PII,[20] because much of this information is collected over insecure connections there is little to prevent these disparate pieces of information from being combined by a malicious person listening in. Since individually, the information was not deemed to be sensitive, it is possible that it would not be protected by the individual advertisers as such. Once these pieces of information have been combined, it is trivial to continue gathering information about that person based on their web use.

18 Currently the NAI has 28 member organizations.
19 See http://www.networkadvertising.org/managing/enforcement.asp.
20 Although it certainly *could* be considered PII.

A second problem that arises from the scenario described above is its consistent use of cookies as containers for data. The NAI has indeed created a simple and effective opt out tool, however for those users most concerned about their privacy, it fails because it requires a cookie to be placed on their computer. Many of the same people that would seek such an opt out mechanism, are the same people that would delete all cookies from their browser whenever they close the program. Because the NAI system relies on cookies to function, the opt out choice does not have persistence., and in addition, because cookies are placed onto and deleted from a user's computer in an invisible way, users are hard pressed to know if the opt out cookie has been deleted, and that they should take action based on that fact.

A third and final problem that is not addressed by the above scenarios is a series of actions between two users on a shared computer. Because of the blanket exemption for first party advertisements, ads meant for one user could easily be shown to a latter user, as in the case of third party advertisements, described above. It is interesting that the FTC did not anticipate this problem with regards to first party advertisements, but was well aware of it with regards to third.