2011

# Regulatory Efforts and Best Practices for the Online Behavioral Advertising Industry

Kraig Koch
*Southern Illinois University Carbondale*, kraig.koch@gmail.com

# REGULATORY EFFORTS AND BEST PRACTICES FOR THE ONLINE BEHAVIORAL ADVERTISING INDUSTRY

by

Kraig Koch

B.A., Eastern Illinois University, 2008

A Research Paper
Submitted in Partial Fulfillment of the Requirements for the
Master of Science.

Department of Mass Communication and Media Arts
in the Graduate School
Southern Illinois University Carbondale
May, 20011

RESEARCH PAPER APPROVAL

# REGULATORY EFFORTS AND BEST PRACTICES FOR THE ONLINE BEHAVIORAL ADVERTISING INDUSTRY

By

Kraig A. Koch

A Research Paper Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Science

in the field of Mass Communication and Media Arts

Approved by:

William Freivogel, Chair

Graduate School
Southern Illinois University Carbondale
April 8, 2011

## Introduction

The year may not be 1984, but concerns of Big Brother-style surveillance have not ceased. One such concern stems from a topic that has received a great deal of recent attention from consumers, media, government and industry officials alike. The topic is online behavioral advertising, which the Federal Trade Commission (FTC) defines as "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests" (2007, December 20). Online behavioral advertising has become one of, if not the, key component of marketing in the digital age, and the topic has peaked the interests and efforts of the advertising community, while garnering equal concern and criticism from privacy rights and advocacy groups.

In June 2010, *The Wall Street Journal* published the results of an investigative study analyzing the tracking methods employed by the 50-most visited U.S. websites. The results were documented on the paper's website and presented as an interactive multimedia graphic detailing the number of tracking devices for individual websites and presenting the privacy policies outlined by the respective sites.

Based on the study, *The Wall Street Journal* published an ongoing series titled "What They Know." It covered industry, government and legal developments related to online behavioral advertising as well as opinions and feedback on the topic. According to an informal readers poll conducted as part of the "What They Know" series, nearly 60% of respondents indicated that they were "Very alarmed" by advertisers and companies tracking their behavior across the Web (*Wall Street Journal*, 2011).

With such ongoing attention given to this hot button issue, it is worth taking account of the developments surrounding online behavioral advertising in recent years. This

paper will detail the technology used in online behavioral advertising and survey the landscape of voices and opinions that have grown up around its use. Court cases, government regulation and industry practices will all be examined in an effort to produce a set of best practices to be considered for future advancements in online behavioral advertising. Finally, the paper will offer suggestions for further advancing self-regulation among the advertising industry as a way of reserving government regulation as a last resort.

## What is Online Behavioral Advertising?

Most websites regularly offer content free of charge. The user does not pay a subscription or fee, so the content is, instead, paid for by advertising. These sites are known to advertisers as "publishers," and make certain portions of their page space available to display ads.

According to the Center for Democracy and Technology, publisher sites sell the space on their pages to "marketers, ad agencies, or online ad networks that place advertisements into the space" (2008, July 31). In addition to purchasing ad space, these intermediaries may also make arrangements with a website to collect information about the site's visitors, allowing them to track the visitors' behavior and, therefore cater the advertisements they display. In the context of these agreements, "a consumer's computer connects to one or more ad networks to communicate data about the consumer's visit and receive advertising on the site" (2008, July 31).

The ad networks act as a sort of middleman between publishers and advertisers, collecting information about visitors on the publisher sites on the one hand and collecting information about advertisers on the other. Based on a visitor's behavior, the ad

networks pull from the advertisements available in their network and then display the ones they believe will be most relevant to the individual in question.

The two most widely used methods ad networks employ to place advertisements are "contextual" advertising and "behavioral" advertising. Unlike behavioral advertising, contextual ads do not take into account the behavior or actions of an individual user or site visitor. Instead, contextual advertising is based on the content of a website. For example, a website about music news might display an ad for tickets to an upcoming concert.

In contrast, behavioral advertising, as the name suggests, is based entirely on the actions and behavior of an individual, placing ads in relation to a consumer's interests, as they are determined over a period of time. Ads do not have to relate to the content of the page on which they appear. Instead, the ad network may notice that a user has made searches relating to music before visiting a news website about current events. While no music news exists on the current events news page, an ad for concert tickets might still appear based on the user's previous search behavior. The Center for Democracy and Technology explains, "a traditional behavioral ad network assembles profiles of individual consumers by tracking users' activities on publisher sites within their network. When the consumer visits a site where the ad network has purchased ad space, the ad network collects data about that visit while serving an advertisement based on the consumer's profile" (2008, July 31).

The act of tracking user behavior to generate relevant ads happens in two distinct ways. The first and most basic way is through "first-party" or "intra-site" collection. This refers to a single website's use of an individual's personal information to generate

tailored content based on previous search patterns and does not include the presence of an outside ad network. The collection of the individual's data most often takes place through the use of cookies, "a small piece of text that is saved on a computer and retrieved when the user revisits the site" (Lilke, 2009, p. 11). A unique cookie ID is deposited the first time a user visits a site. The cookie then tracks the user's information, including how long the individual stays on a particular page and what items the individual views. All the information collected about the individual is attributed to that user's unique ID and stored in a database. According to Lilke, "when the individual returns to the site, the user's browser automatically sends the individual's cookie back to the site. From here, the site looks up the cookie ID in its database and serves the user product recommendations and ads based on previous behaviors" (2009, p. 11).

In contrast to first-party advertising, behavioral tracking also occurs through "third-party" advertising. Rather than collecting information from a single site, third-party advertising tracks behavior across multiple sites and includes the presence of an outside, or "third-party" ad network. In this scenario, the ad network acts as a third party by collecting the data tracked by first-party sites within its network. The first-party sites collect user data in the fashion described above and then sell that information to the third-party ad network. When this is the case, the third-party ad network can compile a broader picture of the individual user and generate ads based on that user's general behavior across a number of sites, rather than the user's specific behavior from an individual site. For example, a first-party site may notice that a user has been looking at information for Toyota Corollas and believe the user is interested in buying that specific car. A third-party ad network, on the other hand, can see through its participating sites

that the same user also looked at Nissan Maximas on another site and Ford Tauruses on yet another. Therefore, based on the user's general behavior, the third-party ad network can then tell that the user is likely in the market for a new sedan, while the first-party site only knows the user has been looking at specific cars and may think he is in the market for a only one brand or model.

Third-party advertising and tracking has been the cause of many consumer concerns and complaints. While consumers can reasonably infer that an individual website has access to their behavior while on the site, it is not as obvious that additional parties might also have access to their information. In the following section, two legal case studies are provided as examples of concerns raised by consumers over such third-party tracking and advertising. These accounts will help provide real world examples of how tracking occurs and why consumers are so deeply bothered by the thought of outside parties accessing their personal information.

## Legal Case Studies

In a November 6, 2007 press release, Facebook announced, "44 websites are using Facebook Beacon to allow users to share information from other websites for distribution to their friends on Facebook." The program, designed to combine the social networking efforts of Facebook and the 44 affiliate sites, allowed users' actions from the outside websites to be published to their individual Facebook profiles and news feeds. In the same press release, Facebook noted, "Beacon is a core element of the Facebook Ads system for connecting businesses with users and targeting advertising to the audiences they want" (2007, November 6). Both Facebook and the businesses involved intended to use the Beacon program to enhance their behavioral advertising efforts.

In theory, the Beacon program sounded harmless enough. In fact, it seemed in line with what Facebook was already doing, in that it allowed users to share personal information with other users in their network. Where Facebook failed in launching the new program, was in its disclosure of privacy standards and participation requests for Beacon. From the period of November 6, 2007, when the program launched, to roughly a month later, on December 5, 2007, default settings for the Beacon program were designed as an "opt out" platform. In other words, unless Facebook users indicated they did not want to participate in the Beacon program, they were automatically enrolled.

The result of these nontransparent settings was a class action lawsuit filed against Facebook and Facebook Beacon's 44 affiliate sites in the Northern District of California on August, 12, 2008. According to the complaint:

> Facebook and the Facebook Beacon Activated Affiliates acted both independently and jointly in that they knowingly authorized, directed, ratified, approved, acquiesced, or participated by accessing and disclosing the personal information ("PI") and/or personal identifying information ("PPI") derived from the activity of the Facebook member which had accessed the website of Facebook Beacon Activated Affiliate, without authority or consent of the Facebook member (Lane v. Facebook, Inc., 2008).

In short, Facebook and the affiliated sites published private information about Facebook users without the knowledge or consent of those users. In a particularly telling example, Facebook user Sean Lane purchased a ring from Overstock.com as a present to his wife. As soon as the transaction was completed, its details (including the 51 percent discount Lane received) were published to the user's Facebook wall and news feed. As a result,

Lane's friends, co-workers, acquaintances and *wife* saw that he had purchased the ring (Mullin, 2010, April 14).

The class action suit concluded that in order to change the default privacy settings of their accounts at the time of Beacon's launch, users like Lane would have to, "read interpret and select nine separate tabs displaying privacy options." Put another way, "the Facebook user would be obligated to read approximately 4 pages and 2,283 words in order to permit access only to their selected friends" (Lane v. Facebook, Inc., 2008). In the current example, Lane would not only have had to find the time to sneak away long enough to select and purchase a gift for his wife, but also to find the additional time to read a privacy statement the length of an instruction manual and then change his privacy settings accordingly, all in order to keep the gift a secret.

The class action complaint filed against Facebook Beacon cited more than just the program's "opt out" setting as a problem. One such problem was that information about individuals using Facebook Beacon's affiliated sites was transmitted to Facebook, regardless of whether or not those individuals were Facebook members. Unlike Facebook users who had the option of reading through privacy settings, "non-Facebook persons who utilized the Facebook Beacon Activated Affiliate websites were not told that their transaction, and indeed, every transaction they engaged in on the website was being communicated to a third party (Facebook) with whom they had no relationship whatsoever" (Lane v. Facebook, Inc., 2008).

Even in the case of Facebook users, individuals were not notified of their information being transmitted to a third party until after the information had been sent. According to the complaint, attempts to gain users' consent were, "inadequate, uninformed,

misleading, untimely, and deceptive" (Lane v. Facebook, Inc., 2008). The *inadequacy* of the attempts to gain consent stemmed from the fact that, when the attempts were present at all, they occurred in the form of pop-up windows, appearing for roughly 10 seconds or less. The attempts were *uninformed* in that they did not explain or specify the details of "how, which, or through what means" the user's information was being transmitted from the affiliate site to Facebook. Attempts were *misleading* because their nature implied that users had some control over the exchange of information when, in reality, such control was not an option. The *untimely* nature of the attempts was due to the fact that information had already been transmitted by the time users were made aware of what was happening. Finally the attempts to gain user consent were *deceptive* because, in most instances, the sharing of user information between Facebook and the affiliated sites was contrary to the privacy policies of Facebook and the affiliate sites alike.

Nearly a month after Beacon's release, a statement was issued by Facebook founder Mark Zuckerberg admitting that company had erred in its release of the program. Speaking on behalf of Facebook, Zuckerberg explained, "we've made a lot of mistakes building this feature, but we've made even more with how we've handled them. We simply did a bad job with this release and I apologize for it" (2007, December 5). Zuckerberg went on to further explain Facebook's original intentions behind the Beacon program, including the fact that the goal was to provide people with a way to easily share information across sites with friends. In his explanation, Zuckerberg noted that the problem with Facebook's efforts was their lack of transparency, which resulted from their desire to make the platform as lightweight as possible. The lightweight nature of the

platform was supposed to avoid making the act of sharing information too cumbersome, but instead, it simply made the sharing that took place deceptive.

On September 17, 2009, the class action suit against Facebook and the Beacon affiliates came to an end when the plaintiffs filed a settlement agreement. The agreement called for a settlement fund of $9.5 million, from which up to $3 million was to be used for administrative costs and attorneys' fees. Also from the fund, the 19 representative plaintiffs received monetary sums based on the amount of money they contributed during the duration of the case. With what was left of the $9.5 million, Facebook was ordered to use to establish a nonprofit Privacy Foundation "to fund projects and initiatives that promote the cause of online privacy, safety, and security" (Lane v. Facebook, Inc., 2008). The settlement was approved by Judge Richard Seeborg of the U.S. District Court for the Northern District of California on March 17, 2010.

Just months after the lawsuit against Facebook Beacon was filed, a class action suit was filed against the online advertising company NebuAd and at least six NebuAd Activated ISP Affiliates (NAISPs) on November 10, 2008. At the time, NebuAd's business model was built on the development of behavioral advertising through partnerships with ISPs that allowed NebuAd access to their customers' web surfing habits. The goal, as with Facebook Beacon and other online behavioral advertising companies, was to provide individual web users with targeted, relevant advertising.

There was, however, a significant difference between NebuAd and Facebook's Beacon program. While Beacon relied on the use of cookies to track and share user behavior, NebuAd relied on a tactic called "deep packet inspection." In a *Washington*

*Post* article, Rob Pegoraro provided a practical analogy to describe the difference between the two tactics:

> Tracking via cookies is the rough equivalent of a supermarket clerk noting that you spend a lot of time in Aisle 9 checking out cereal but never duck into Aisle 2 for frozen dinners. Deep packet inspection, by contrast, is more like the clerk following you to see which boxes of cereal you eyeballed – and doing so at every store you visit, even those run by other companies (2008).

While Facebook and the Beacon affiliates tracked and shared the general behavior of web users on select, participating sites, NebuAd signed on with ISPs to track every move Internet users made while surfing the web and then provided advertising based on those specific actions.

Similar to the Facebook Beacon case, the complaint against NebuAd and the NAISPs alleged:

> NebuAd and the NAISPs acted both independently and jointly, in that they knowingly authorized, directed, ratified, approved acquiesced, or participated by accessing and disclosing sensitive information ("SI"), personal identifying information ("PII"), personal information ("PI"), and non-personal identifying information ("Non-PII") derived from the intentional interception of the NAISP subscriber's online transmissions, without authority or consent of the NAISP subscriber (Valentine v. NebuAd, Inc., 2008).

According to the complaint, the actions performed through the joint venture between NebuAd and the NAISPs were not based on a normal course of business, but instead, were intended to monetize subscribers' data for advertisement purposes. In a normal

course of business, ISPs have a right to inspect a subscriber's datastream for reasons like viruses, spam, securing the network or policing bandwidth, but using deep packet inspection to produce advertising content does not fall within those rights.

Also similar to the actions of Facebook's Beacon program was NebuAd's default "opt out" setting. If NebuAd had a contract with a user's ISP, the user was automatically enrolled in the NebuAd service. According to the complaint against NebuAd, there were no cases in which users were given adequate or informed notice of the true nature of the service. In instances where some type of notice of NebuAd's services was given, the notice was "insufficient, misleading, and inadequate" (Valentine v. NebuAd, Inc., 2008). Even in cases where users were provided with an "opt out" function, their data was still collected and the only change made was to the provision of advertisements during their web experience. In the same way that Facebook Beacon collected information about non-Facebook users, NebuAd still collected information about users that had chosen not to receive the company's advertisements.

In an act suggesting the company knew it could no longer operate in its intended form, a document was filed in the class action suit on May 17, 2009 explaining that NebuAd would be closing its services. According to the document, NebuAd claimed it would "cease to exist as on ongoing concern" and that it was assigning all assets to its creditors. In the document, NebuAd further asserted, "from a company that once employed over 60 people, NebuAd now operates with a skeleton staff, and shortly, that too will disappear. At the time the document was filed, a news story from *Ars Technica* explained that the company had intended to attempt a news business model, "but the money wasn't there to continue, it appears, and the company is gone" (Anderson, 2009, May 19).

Concerns similar to those raised by the plaintiffs in the above cases are common among consumers and a large number of privacy groups and organizations, such as the Center for Digital Democracy, Consumer Federation of America, Electronic Frontier Foundation and U.S. Public Interest Research Group. As a result, legislators and government officials have been seeking solutions to ease these concerns and protect the interest of Internet users. The following section examines some of the recent efforts made by the U.S. government to regulate the online advertising industry and develop useful solutions for protecting online privacy.

## Government Regulation

In 2010, two separate pieces of legislation were introduced to address the online privacy rights of American consumers. In July, U. S. Rep. Bobby L. Rush, chairman of the Subcommittee on Commerce, Trade, and Consumer Protection, introduced a bill titled "The Best Practices Act of 2010." Drafted after a series of joint hearings with the Subcommittee on Communications, Internet, and Technology, which looked into the issue of consumer privacy, Rush's bill sought to achieve a balance between privacy rights and industry incentives. In a press release, Rush's staff concluded the bill "establishes a flexible framework of basic rights for consumers while also outlining obligations for companies based on fair information principles" (Jenkins & Gadlin, July 19, 2010). Following are some of the key provisions included in the proposed legislation:

- Ensure that consumers have meaningful choices about the collection, use, and disclosure of their personal information.

- Require companies that collect personal information to disclose their practices with respect to the collection, use disclosure, merging, and retention of personal information, and explain consumers' options regarding those practices.
- Require companies to provide disclosures of their practices in concise, meaningful, timely, and easy-to-understand notices, and direct the Federal Trade Commission to establish flexible and reasonable standards and requirements for such notices.
- Require companies to obtain "opt-in" consent to disclose information to a third party. In the bill, the term, "third party" would be defined based on consumers' reasonable expectations rather than corporate structure.
- Waive the "opt-in" consent requirement, for companies choosing to participate in a universal opt-out program operated by self-regulatory bodies and monitored by FTC.
- Require companies to have reasonable procedures to assure the accuracy of the personal information they collect. The bill would also require the companies to provide consumers with reasonable access to, and the ability to correct or amend, certain information.
- Require companies to have reasonable procedures to secure information and to retain personal information only as long as is necessary to fulfill a legitimate business or law enforcement need (Jenkins & Gadlin, July 19, 2010).

Rush's bill did not come to a vote during the 2010 Congressional session, but Rush announced in October that he had gained the support of three industry leaders – eBay, Intel and Microsoft. In a letter to the representative, the companies announced, "We

support the bill's overall framework, which is built upon the Fair Information Practices regime. We appreciate that the Best Practices Act is technology neutral and gives flexibility to the Federal Trade Commission to adapt to the changes in technology" (Jenkins & Gadlin, October, 7, 2010). The companies also expressed their approval of the bill's provision to allow businesses the opportunity to enter into a robust self-regulatory choice program. Acting on the end-of-year momentum, Rush re-introduced the legislation in February 2011 and continues to search for additional support for the bill.

Before Rush's Best Practices Act, Rep. Rick Boucher proposed his own legislation in the form of a "discussion" draft on May 4, 2010. Boucher's proposal would have mandated the length of time consumer information could be retained online and, similar to the Rush bill, required that websites gain consumers' consent before sharing their data for marketing purposes. Unlike Rush's Best Practices Act, however, the Boucher proposal garnered harsh criticism from consumer groups and conservatives alike. Consumers argued the bill was not strong enough on limiting the time information could be stored, while conservative groups argued the bill went too far. In a statement released by the Progress and Freedom Foundation, the organization claimed:

> By mandating a hodgepodge of restrictive regulatory defaults, policymakers could unintentionally devastate the 'free' Internet as we know it. Because the digital economy is fueled by advertising and data collection, a privacy industrial policy for the Internet would diminish consumer choice in ad-supported content and services, raise prices, quash digital innovation, and hurt online speech platforms enjoyed by Internet users worldwide" (Kravitz, 2010).

Boucher's bill, like Rush's, never came to fruition during the 2010 Congressional session and the complaints surrounding the bill illustrated the caution and balance such regulation would require. Boucher went on to lose in the November 2010 election and, consequently, his privacy efforts ended with his unsuccessful campaign.

Shortly after the 2010 elections, one of the most notable government efforts to secure online privacy rights came on December 1, 2010 when the FTC released a staff report recommending specific practices to insure the protection of online consumers. In addition to addressing concerns about educating consumers and fears surrounding practices like deep packet inspection, the report set forth the recommendation of a "Do Not Track" mechanism that could be installed in all Internet browsers. The mechanism was the FTC's attempt at a blanket approach to addressing consumer protection and was developed based on the popular Do Not Call registry that currently governs the telemarketing industry.

According to the report, "Such a mechanism would ensure that consumers would not have to exercise choices on a company-by-company or industry-by-industry basis, and that such choices would be persistent" (FTC, 2010). The Do Not Track tool would be established either by legislation or, as the report explained, by "robust, enforceable self-regulation" by advertisers and Web companies. Once established, the mechanism would most likely exist as a persistent cookie on users' browsers that communicates with websites to establish that a user does not want to be tracked or receive targeted advertising (Kang, 2010).

While coming up with its Do Not Track recommendation, the commission noted that it sought to balance consumer concerns for privacy and business interests

regarding targeted advertising. The FTC explained, "in developing the proposed framework, staff was cognizant of the need to protect consumer privacy interests effectively, while also encouraging the development of innovative new products and services that consumers want" (Federal Trade Commission, 2010). Such awareness of the balancing act required by regulation efforts suggested that the FTC was more sensitive to the needs of both consumers and advertisers than Rep. Boucher was in his own proposal earlier that year.

If the FTC's proposed Do Not Track mechanism is eventually adopted it would affect more than just the interests of consumers and advertisers. Internet software providers would be deeply impacted by the proposal, as it would be the responsibility of companies that design Internet browsers to develop and maintain the Do Not Track tool. Microsoft and Mozilla have each expressed support for the FTC proposal since the staff report was released, with Microsoft going as far as developing and releasing a version of the Do Not Track tool in its most recent version of Internet Explorer. While Mozilla has not yet released its own version, it announced in January that it would include a do-not-track feature in its upcoming version of the Firefox browser (Wingfield & Angwin, 2011, March 15). At this point, Google and Apple are the only large providers of Internet browsers that have not yet announced their support.

Finally, the most recent move by the government to endorse consumer privacy came on March 16, 2011 when the Obama administration expressed its desire for Congress to pass a "privacy bill of rights" that would protect Americans from intrusive data gathering. In a written testimony before the Senate Commerce Committee, Assistant Commerce Secretary Lawrence Strickling said, "The administration urges Congress to

enact a ‘consumer privacy bill of rights’ to provide baseline consumer data privacy protections” (Engleman, 2011, March 16). Strickling explained that the legislation should give the FTC authority to enforce privacy protections and take action against noncompliant advertisers. Such outspoken involvement from the current administration is a change from the previous hands-off approach previous administrations took towards the Internet and clearly demonstrates the administration’s concern for consumers as it reassesses the federal government’s role in regulating online tracking. Strickling’s statements will most likely produce additional support for the re-introduction of Rep. Rush’s legislation as well as provide momentum to privacy legislation that is currently being drafted by Sen. John Kerry.

While the government continues to develop its strategies for protecting consumers, the advertising industry has been hard at work producing its own solutions for regulating Internet tracking. The following section examines these solutions and outlines the recent steps the industry has taken in developing its own self-regulatory programs.

## Industry Self-Regulation

In efforts to avoid government regulation, the advertising industry has come together to work collectively at developing a system of self-regulation. The industry’s efforts came to fruition in July 2009 when the American Association of Advertising Agencies, the Association of National Advertisers, the Council of Better Business Bureaus, the Direct Marketing Association and the Interactive Advertising Bureau collectively released their “Self Regulatory Principles for Online Behavioral Advertising.” The industry leaders developed the principles based on tenets the FTC

had released earlier the same year and designed them to address consumer concerns about the use of personal information while protecting their own interest in advancing innovations within the advertising community. The effort consisted of the following seven self-regulatory principles:

1. **The Education Principle** calls for organizations to participate in efforts to educate individuals and businesses about online behavioral advertising and the Principles.
2. **The Transparency Principle** calls for clearer and easily accessible disclosures to consumers about data collection and use practices associated with online behavioral advertising. It would result in new, enhanced notice on the page where data is collected through links embedded in or around advertisements, or on the Web page itself.
3. **The Consumer Control Principle** provides consumers with an expanded ability to choose whether data is collected and used for online behavioral advertising purposes. This choice will be available through a link from the notice provided on the Web page where data is collected. The Consumer Control Principle requires "service providers" … to obtain the consent of users before engaging in online behavioral advertising, and take steps to de-identify the data used for such purposes.
4. **The Data Security Principle** calls for organizations to provide appropriate security for, and limited retention of data, collected and used for online behavioral advertising purposes.

5. **The Material Changes Principle** calls for obtaining consumer consent before a Material Change is made to an entity's Online Behavioral Advertising data collection and use policies unless that change will result in less collection or use of data.
6. **The Sensitive Data Principle** recognizes that data collected from children and used for online behavioral advertising merits heightened protection, and requires parental consent for behavioral advertising to consumers known to be under 13 on child-directed Web sites. This Principle also provides heightened protections to certain health and financial data when attributable to a specific individual.
7. **The Accountability Principle** calls for development of programs to further advance these Principles, including programs to monitor and report instances of uncorrected non-compliance with these Principles to appropriate government agencies. The CBBB and DMA have been asked and agreed to work cooperatively to establish accountability mechanisms under the Principles (Digital Advertising Alliance, 2009).

In October 2010, a little more than a year after the release of the principles, the participating organizations, along with a handful of additional industry groups, announced the creation of a coalition offering a "Self-Regulatory Program for Online Behavioral Advertising." The coalition, named the Digital Advertising Alliance, opened a registration platform through their website wwww.aboutads.info allowing any advertiser to sign up and become a part of the self-policing program.

The Digital Advertising Alliance program requires participants to include an icon in the right-hand corner of ads that allows Internet users to click and receive information about the ad and who is serving it. After clicking on the icon, users are able to follow links enabling them to opt out of being tracked by the advertiser and third-party data partners. The annual fee for participating in the program is $5,000 for first-party companies and $10,000 for third parties (Lee, 2010, October 4).

In a display of commitment to the program, the Digital Advertising Alliance enlisted the support of the Council of Better Business Bureaus (CBBB) to administer its efforts. While the CBBB was listed as the enforcement arm of the program since the time of its inception, the council announced in March 2011 that it would be stepping up enforcement in order to make the efforts official. In an interview with *Ad Age*, Eugenie Barton, the individual charged with heading up the enforcement efforts, explained, "for everybody who states they are in compliance, we will be checking to see if they are in compliance with the principles. And if they're not, we'll be talking to them about what steps they are taking to be in compliance, and what they're timeline is" (Lee, 2011, March 4).

According to Barton, if there is a dispute about a company's compliance, the company will be monitored to determine whether or not they are displaying proper notices and offering functional opt-out links. If, eventually, a company fails to comply with the principles, they will be referred to the "appropriate agency." In most cases, according to Barton, the agency will be the FTC.

The advertising industry's efforts, along with the proposals of legislators and the U.S. government, all represent an acknowledgement of the fact that something should be done to regulate the use of online behavioral advertising. The final section of this research

paper summarizes the some of the key takeaways of these efforts and offers a set of suggestions for moving forward with regulatory efforts and behavioral advertising practices in the future.

## Suggestions for Future Practices

As the Facebook and NebuAd lawsuits both show, one of the main issues to consider in relation to online behavioral advertising is transparency. Consumers are clearly alarmed by the fact that third parties are tracking their online behavior, and hiding this fact only heightens their sense of concern. Facebook and NebuAd both erred in deceptively collecting information about Internet users without their consent, and their behavior should serve as a warning sign to other advertisers as they move forward with their own efforts in the future.

It is a well-known fact that user information is collected by first-party tracking on individual websites. However, in situations where third-party tracking occurs, websites and advertising companies should be upfront with users about what information is being collected or shared. Unlike the failed Facebook Beacon program, Facebook's newer Connect platform has seen broad acceptance from its users. Connect, much like Beacon, allows Facebook users to share information about what they are doing on the Web with other users in their Facebook community. The primary difference between the two programs has been Facebook's willingness to disclose information to their users. While Beacon shared information without adequate notice, Connect requests a user's permission before sharing information between Facebook and third-party websites. As Josh Catone put it at the time of Connect's release, "by introducing user controlled privacy settings from the start and allowing any site to tap into Facebook's user base via Connect,

Facebook has created the version of Beacon that they should have launched last fall" (2008, July 24). Indeed, sharing information across platforms is not what concerns Internet users. It is when their information is shared without knowledge or consent that users become alarmed.

In order to ease the alarm of consumers while simultaneously protecting the interests of the advertising industry, a set of regulatory practices is desirable. Such regulation, however, poses a central question to the concerns surrounding online behavioral advertising. Should government or industry control the regulatory efforts? The question, unfortunately, does not have any easy answers. At this point, the government has not formally passed any proper regulatory program and the self-regulating program created by the advertising industry is still in its infancy. As such, neither effort can be adequately evaluated or accurately compared to the other and the argument for one option is potentially as viable as the next.

With that said, it is still necessary to develop a strategy for regulating behavioral advertising in order to protect the interests of all concerned parties. Having researched both sides of the debate and weighing the options of each, this author believes that the industry should be given a chance at self-regulation before the government intervenes. As evidenced by the Facebook Connect example, the industry is clearly capable of reworking its structure to adequately address the concerns of consumers while further developing the technology behind behavioral advertising. Through self-regulation, the industry could continue to advance its technology without fear of punishment or retribution, while simultaneously considering consumer concerns and government suggestions to maintain transparency and accountability.

A primary industry concern regarding possible regulation is the fact that the FTC's suggestions along with the efforts of legislators and the administration generally favor an opt-in approach to behavioral advertising. This strategy, of course, would thoroughly protect consumers, but it would do so at the risk of stifling innovation among the advertising industry. If all behavioral advertising is transitioned to an opt-in strategy, there is a very real possibility that the general consumer population could simply choose not to participate. Such an act would be detrimental to the previous work of the advertising community, and it is therefore worth affording the industry the chance to alter its strategy in order to preserve the value of its work while observing the rights of consumers and considering the concerns of the government.

Indeed, the Digital Advertising Alliance's "Self Regulatory Principles for Online Behavioral Advertising" show that the industry has taken government concerns into consideration by basing the principles on tenets outlined by the FTC. Tellingly, the principles, published more than a year before the FTC's official suggestion of a Do Not Track Tool, seemed to foreshadow such a mechanism, promoting some of the exact issues the tool seeks to address, such as transparency, consumer control and accountability. The similarities among efforts depict the industry's willingness to include the government's suggestions in the formation of their self-policing efforts and show that it may be possible for the two bodies to work harmoniously, rather than in opposition.

The inclusion of the CBBB as an enforcement arm, and the use of the FTC as a disciplinary body highlight the industry's attempts to include the government in its efforts and display the Digital Advertising Alliance's willingness to work collectively in the execution of its "Self-Regulatory Program for Online Behavioral Advertising." In fact,

the program embodies exactly what Rep. Boucher's bill describes when he refers to "a universal opt-out program operated by self-regulatory bodies and monitored by the FTC" (Jenkins & Gadlin, July 19, 2010). The program allows consumers to opt out of third-party advertisements and refers companies not in compliance with program standards to the FTC. It is worth letting such a program prove itself, before imposing further restraints on the industry.

The program, in its current form, represents a desirable compromise between government and industry by combining their efforts rather than giving one party final say over the other. A further compromise could be the incorporation of the FTC's Do Not Track proposal in the "Self-Regulatory Program for Online Behavioral Advertising." While the program now offers consumers the ability to opt out of advertisements from a particular network, the inclusion of a Do Not Track tool would allow particularly concerned consumers to opt out of tracking by all advertisers. This would further enhance the transparency of the industry as well as strengthen their cooperation with the government's efforts. It would also highlight some of the strongest efforts of both parties by including one the of the government's most highly praised suggestions with the industry's best efforts to date.

The implementation of a Do Not Track tool in the existing Digital Advertising Alliance program would essentially please consumers, government and the advertising industry. Consumers, for example, would be provided with upfront, transparent information and the option of opting out of third party tracking. The government would see the enforcement of its best regulatory suggestion and be given the authority to discipline companies not in compliance with regulation requirements. Finally, the

advertising industry would maintain initial autonomy over its behavior and be able to continue developing and applying innovative new technologies without the limiting presence of strict rules and guidelines. If, after a trial period, the self-regulatory efforts of the advertising industry prove ineffective, with companies routinely violating guidelines and consumers expressing similar levels of concern, it will be time to reexamine regulatory efforts and consider imposing a set of laws and government statutes to oversee behavioral advertising industry. Until that time, industry and government should continue to work cooperatively in their efforts as they attempt to guard consumers and protect the interests of a still new industry practice.

# REFERENCES

American Association of Advertising, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, & Interactive Advertising Bureu. (2009). *Self-regulatory principles for online behavioral advertising*. Retrieved from http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf (2011, March 22).

Anderson, N. (2009, May 19). NebuAd shuts up shop, web users rejoice. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/news/2009/05/nebuad-shuts-up-shop-web-users-rejoice.ars (2011, March 22).

Angwin, J., & McGinty, T. (2010, July 30). Sites feed personal details to new tracking industry. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html (2011, March 22).

Center for Democracy and Technology. (2008, July 31). A briefing on public policy issues affecting civil liberties online from The Center For Democracy and Technology. [Web log comment]. Retrieved from http://www.mail-archive.com/cdt-announcements@cdt.org/msg00527.html (2011, March 22).

Digital Advertising Alliance. (2009). *Self-regulatory principles overview*. Retrieved from http://www.aboutads.info/principles (2011, March 22).

Engleman, E. (2011, March 16). Obama calls for privacy bill of rights for online consumers. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2011-03-16/obama-calls-for-privacy-bill-of-rights-for-online-consumers-1-.html (2011, March 22).

Facebook. (2007, November 6). Leading websites offer Facebook Beacon for social distribution. [Press release]. Retrieved from http://www.sys-con.com/node/456546 (2011, March 22).

Federal Trade Commission. (2010). *A preliminary FTC staff report on protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers*. Retrieved from http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (2011, March 22).

Federal Trade Commission. (2007, December 20). Online behavioral advertising: Moving the discussion forward to possible self-regulatory principles. Retrieved from http://www.ftc.gov/os/2007/12/P859900stmt.pdf (2011, March 22).

Jenkins, S., & Gadlin, S. (2010, July 19). Subcommittee chairman Bobby L. Rush fights for consumer privacy and protection of personal information introduces the Best Practices Act of 2010. [Press Release]. Retrieved from http://www.house.gov/list/press/il01_rush/pr_100719_best_practices_act.shtml (2011, March 22).

Jenkins, S., & Gadlin, S. (2010, October 7). Rush welcomes support of tech industry leaders eBay, Intel and Microsoft for their support of the Best Practices Act of 2010. [Press Release]. Retrieved from http://www.house.gov/apps/list/press/il01_rush/pr_101007_best_practices.shtml (2011, March 22).

Kang, C. (2010, December 1). FTC recommends 'Do Not Track' program in Internet privacy report. *Washington Post*. Retrieved from

http://voices.washingtonpost.com/posttech/2010/12/ftc_suggests_do_not_track_more.html (2011, March 22).

Kravitz, D. (2010, May 4). Groups call 'privacy' legislation Orwellian. *Wired*. Retrieved from http://www.wired.com/threatlevel/2010/05/online-privacy-proposal/ (2011, March 22)

Lane v. Facebook, Inc., Case 5:08-cv-03845-RS (N.D. California 2008).

Lee, E. (2010, October 4). Hoping to maintain self-regulation, trade groups charge advertisers and networks for privacy system. *Ad Age*. Retrieved from http://adage.com/article/digital/advertiser-groups-band-online-track-list/146240/ (2011, March 22).

Lee, E. (2011, March 4). Industry to begin enforcing compliance on behavioral advertising principles. *Ad Age*. Retrieved from http://adage.com/article/digital/behavioral-advertising-principles-enforced/149228/ (2011, March 22).

Lilke, J. (2009, Fall). *The acceptance of online behavioral advertising: A study of the perceptions of young adults*. Retrieved from http://www.slideshare.net/jeaninelilke/the-acceptance-of-online-behavioral-advertising-a-study-of-the-perceptions-of-young-adults (2011, March 22).

Mullin, S. (2010, April 14). Efficiency v. privacy: Is online behavioral advertising capable of self-regulatoin? [Web log comment]. Retrieved from http://www.coveringyourads.com/2010/04/articles/advertising-law/efficiency-v-privacy-is-online-behavioral-advertising-capable-of-selfregulation/ (2011, March 22).

Valentine v. NebuAd, Inc., Case 5:08-cv-5113-RS (N.D. California 2008).

Pegoraro, R. (2008, August 1). Internet providers' new tool raises deep privacy concerns. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2008/08/20/AR2008082003259_2.html?hpid=news-col-blogs&sid=ST2008082003266&s_pos= (2011, March 22).

*Wall Street Journal*. (2011). [Graph illustration of *Wall Street Journal* tracking survey]. *How concerned are you about advertisers and companies tracking your behavior across the Web?* Retrieved from http://online.wsj.com/community/groups/media-marketing-267/topics/how-concerned-you-about-advertisers (2011, March 22).

Wingfield, N., & Angwin, J. (2011, March 15). Microsoft adds do-not-track tool to browser. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052748703363904576200981919667762.html (2011, March 22).

Zuckerberg, M. (2007, December 5). Thoughts on Beacon. [Web log comment]. Retrieved from http://blog.facebook.com/blog.php?post=7584397130 (2011, March 22)

# VITA

Graduate School
Southern Illinois University

Kraig A. Koch Date of Birth: May 9, 1986

8 Spruce Drive, Belleville, IL 62221

kraig.koch@gmail.com

Eastern Illinois University
Bachelor of Arts, English, May 2008

Research Paper Title:
Regulatory Efforts and Best Practices for the Online Behavioral Advertising Industry

Major Professor: William Freivogel