Self Regulatory Principles for Online Behavioral Advertising

Implementation Guide

October 2010

Self Regulatory Principles for Online Behavioral Advertising Implementation Guide

– What Everyone Needs To Know –

Leading marketing and advertising industry associations have established a comprehensive, self-regulatory program and implemented consumer-friendly principles and enforcement standards regarding online behavioral advertising.

Defining Online Behavioral Advertising

Online behavioral advertising ('OBA') is defined as the practice of collecting "data from a particular computer or device regarding Web viewing behaviors over time and across non-Affiliate Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors." The purpose of OBA is to deliver relevant advertising to specific computers or devices in ways that enrich the consumer online experience.

As defined in the *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles"), OBA does not include:

- The activities of First Parties (Web site publishers / operators) that are limited to their own or affiliated sites.
- Ad delivery (i.e., delivery of online advertisements or advertising-related services using Ad Reporting data and not based on user preferences inferred from information collected over time and across non-affiliated Web sites);
- Ad reporting (i.e., the collection or use of information for statistical reporting, Web analytics/analysis and advertising metrics); or
- Contextual advertising (i.e., advertising based on the content of the Web page being visited, a consumer's current visit to a Web page, or a search query).

About the Principles

The industry-wide effort to develop consumer-friendly standards for OBA activities across the Internet was led by a coalition of the nation's largest media and marketing trade associations, including the American Association of Advertising Agencies (AAAA), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), and the Interactive Advertising Bureau (IAB), and supported by the Council of Better Business Bureaus (BBB). This unprecedented collaboration responds the Federal Trade Commission's call to the advertising and media industry to develop self-regulatory principles and practices for OBA.

In July 2009, the Associations jointly released the *Self-Regulatory Principles for Online Behavioral Advertising* (the "Principles"), which are intended to apply broadly to the diverse set of actors that work interdependently to deliver relevant advertising intended to enrich the consumer online experience.

The Principles call for:

- **Education** for consumers and businesses about online behavioral advertising and the Principles.
- **Transparency** about data collection and use practices associated with OBA, providing consumers with clear, meaningful and prominent notice through multiple mechanisms.
- **Consumer Control** over whether data is collected and used or transferred for OBA purposes, provided through easy-to-use consumer choice mechanisms.
- Appropriate **Data Security** for, and limited retention of, data collected and used for OBA purposes.
- Obtaining consumer consent before a **Material Change** is made to an entity's OBA data collection and use policies unless that change will result in less collection or use of data.
- Limitations on the collection of **Sensitive Data** for OBA purposes.
- **Accountability** for entities collecting and using data for OBA purposes, including mechanisms for enforcement of the Principles.

Implementing the Principles

Since July 2009, industry-wide collaboration has continued on the development and launch of a self-regulatory program for OBA ("Program") that will implement the Principles, promoting enhanced transparency and choice and fostering compliance and accountability across the marketing and advertising community.

The Program includes several important components:

- **Advertising Option Icon**: The program promotes the use of an icon and accompanying language, to be displayed in or near online advertisements or on Web pages where data is collected and used for behavioral advertising. Advertising Option Icon indicates that the advertising is covered by the self-regulatory program, and by clicking on it consumers will be able to link to a clear disclosure statement regarding the data collection and use practices associated with the ad as well as an easy-to-use opt-out mechanism.

- **www.AboutAds.info**: Companies collecting or using information for behavioral advertising are encouraged to visit www.AboutAds.info to acquire and begin displaying the Advertising Option Icon, signaling their utilization of behavioral advertising and adherence to the *Principles*. Interested companies engaged in behavioral advertising can also register to participate in the easy-to-use consumer opt-out mechanism on the www.AboutAds.info site.

- **Consumer Choice Mechanism**: This easy-to-use choice option will give consumers the ability to conveniently opt-out of some or all participating companies' online behavioral ads, if they choose. Entities may now register at www.aboutads.info to participate in an industry-wide choice mechanism.

- **Accountability and Enforcement**: Both the CBBB and the DMA will play roles in ensuring compliance and enforcement of the Program. All DMA members – as a condition of membership – are required to comply with program's provisions.

The CBBB and DMA will utilize a monitoring technology platform to foster accountability among participating companies with respect to the Transparency and Control requirements of the Principles, as well as manage consumer complaint resolution.

- **Educational Campaign**: An educational campaign will be undertaken to build awareness around the Program for both the business community and consumers.

How Does This Affect My Organization?

The Principles cover three major types of entities that – working interdependently – deliver relevant advertising to specific computers or devices in ways that enrich the consumer online experience:

- "First Parties": such as Web site publishers / operators;
- "Third Parties": such as advertising networks and data companies (including ad exchanges and data aggregators) and in some cases advertisers; and
- Service Providers": such as any internet access provider, search engine, Web tool bar, browser, or other service that enables the provider to have access to all or substantially all URLs accessed by its users, that in the course of its activities as such a provider, collects and uses such user data for OBA.

This Implementation Guide also includes sections that address the responsibilities of each type of entity.

It is possible that a single company or organization may operate in more than one of these three categories, depending on what activity is being undertaken at a particular time. For this reason, it is important to consider requirements that may apply to your business across all three categories.

Questions?

This Implementation Guide includes a detailed set of Frequently Asked Questions and answers regarding the entire scope of this industry-wide program. Additional information is also available online at www.AboutAds.info.

Self Regulatory Principles for Online Behavioral Advertising Implementation Guide

– "First Party" Responsibilities –

What is a "First Party"?

The *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles") apply broadly to the diverse entities that engage in online behavioral advertising ("OBA"), governing three major types of entities – First Parties, Third Parties and Service Providers – that work interdependently to deliver relevant advertising to specific computers or devices in ways that enrich the consumer online experience.

Under these *Principles*, a First Party is defined as "the entity that is the owner of the Web site or has Control over the Web site with which the consumer interacts and its Affiliates." In short, a first party is a Web site publisher or operator.

In order to fully understand the responsibilities of First Parties and the environment in which you are operating, you should also read the "What Everyone Needs to Know" section of this Implementation Guide.

How Do the Principles Apply to First Parties?

You have identified yourself as a First Party, which means that you operate Web sites and/or exercise control over other affiliated sites. As an example, you may publish an online magazine or operate an online retail site.

[**NOTE**: If your company engages in OBA on a non-affiliated Web site, then you may also be a Third Party and you should also comply with the sections of the *Principles* and this Implementation Guide directed to "Third Parties" engaged in those activities.]

The *Principles* do not apply to the data collection and use practices you employ on your own site – for your own purposes – or on other sites over which you exercise direct control for your own or an affiliated site's purposes.

If Third Parties, such as advertising networks, collect or use OBA data on your site, the *Principles* assign responsibilities for consumer transparency and control concerning OBA practices to those Third Parties (i.e., the entity collecting the data for OBA purposes is responsible for complying with this aspect of the *Principles*). However, Third Parties engaged in OBA activities on your site will in many instances require your agreement, and sometimes your direct cooperation, in order to comply. In addition, if Third Parties operating on your site do not provide enhanced notice as required by the *Principles*, then you should provide the notice.

To ensure compliance with the following requirements, it may be preferable for both First and Third Parties to provide notice that makes consumers aware that OBA is occurring on the web site and provide consumers with a means to exercise choice regarding the collection and use of their data for OBA purposes. In addition, First Parties should obtain consumer consent before materially changing their OBA data collection and use policies.

Below is a more detailed explanation of each of these requirements.

1. Providing Consumer Transparency

As a First Party operating a Web site on which Third Parties collect and use data for OBA purposes, you share responsibility for ensuring that a clear, meaningful and prominent link appears on any page on your Web site where OBA data is collected or used. This "enhanced notice link" should direct consumers to the proper disclosure notice required by the *Principles.*

Third Parties engaging in OBA activities on your site are encouraged to provide the enhanced notice link "in" or "around" the OBA advertisement or in another prominent location agreed to by you.

If any Third Party does not provide enhanced notice on any page of your site where it is collecting or using OBA data, then you should display a clear, meaningful and prominent enhanced notice link that directs consumers to a disclosure on your own Web site that:

- Links to the www.AboutAds.info website, where Third Parties engaging in OBA activities on your site have registered and are listed; or
- lists the Third Parties engaging in OBA activities at your site, including links to their own disclosures.

Any enhanced notice link provided by you should be distinct from the link to your own privacy policy.

If this disclosure is in your Web site privacy statement, your enhanced notice link should go directly to the relevant section of the statement where the disclosure is located.

Where a Third Party includes an appropriate link to its notice from a location in or around an advertisement or other permitted place on your Web page, you have no further disclosure requirements under the *Principles*. However, to ensure compliance with the requirements it may be preferable for both First and Third Parties to provide the enhanced notice.

Finally, your Web site should also indicate adherence to the *Principles*.

2. Changing OBA Data Collection / Use Policies

You should obtain consumer consent before making any material changes to your OBA data collection or use policies and practices. A material change might be a decision to use or share previously collected OBA data in a new way. A change that results in less collection or use of OBA data would not be considered material for purposes of the *Principles*. Consent requires an individual's action in response to a clear, meaningful and prominent notice.

Questions?

This Implementation Guide includes a detailed set of Frequently Asked Questions and answers regarding the entire scope of this industry-wide program. Additional information

is also available online at www.AboutAds.info. First parties might find the following FAQs of particular interest:

- Why did the leading marketing and advertising trade associations develop the self-regulatory *Principles* for online behavioral advertising?
- What is the Advertising Option Icon? What does it mean?
- What is www.AboutAds.info ? Where can I find it? How does it work?
- I am Web publisher and OBA activity occurs on my Web site. What do the Principles indicate that I should do?
- I am a Web publisher. If I use data collected across my family of affiliated Web sites for OBA purposes, do the *Principles* say I should do anything?
- Do the *Principles* impose specific data security standards?

Self Regulatory Principles for Online Behavioral Advertising Implementation Guide

– "Third Party" Responsibilities –

What is a "Third Party"?

The *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles") apply broadly to the diverse entities that engage in online behavioral advertising ("OBA"), governing three major types of entities – First Parties, Third Parties and Service Providers – that work interdependently to deliver relevant advertising to specific computers or devices in ways that enrich the consumer online experience.

Under these *Principles,* a Third Party is defined as "an entity that engages in OBA on a non-affiliate's Web site." In short, Third Parties are advertising networks and data companies (including ad exchanges and data aggregators) and, in some cases, advertisers.

In order to fully understand the responsibilities of Third Parties and the environment in which you are operating, you should also read the "What Everyone Needs to Know" section of this Implementation Guide.

How Do the *Principles* Apply to Third Parties?

You have identified yourself as a Third Party, which means that you engage in online behavioral advertising ("OBA") on a non-affiliate's Web site. This guidance for Third Parties is directed primarily to **advertising networks and data companies** that collect Web viewing data across multiple unaffiliated sites and use such data to serve online interest-based advertising.

An **advertiser** (i.e., a company whose product or service is being promoted in an advertisement) may also be a Third Party if it engages in data collection and use for online interest-based advertising. However, if the advertiser uses an ad network or other entity to collect data for interest-based advertising purposes and that entity does not provide such data to the advertiser for its independent use, the advertiser is not a Third Party and not subject to the *Principles* in that capacity.

[**NOTE**: If your company also operates Web sites and/or exercise control over other affiliated sites, then you may also be a First Party and you should also comply with the sections of the *Principles* and this Implementation Guide directed to "First Parties" engaged in those activities.]

As a Third Party that operates across multiple unaffiliated sites, you should do the following to comply with the *Principles*:

1. Provide a clear, meaningful and prominent notice on your Web site disclosing your OBA practices;
2. Provide a clear, meaningful and prominent link (i.e., the "enhanced notice link") to the information in your Web Site notice. This can be accomplished either by linking directly from the advertisements you place (i.e., notice in or near the ad),

or from other places on the Web page where you collect or use data for OBA purposes (likely accomplished through collaboration with a First Party);
3. Provide easy-to-use ways for consumers to choose whether data is collected and used for OBA purposes or is transferred to another, unaffiliated entity for OBA purposes;
4. Provide appropriate security for, including limiting the retention of, the data you collect and use for OBA purposes;
5. Obtain consumer consent before materially changing your OBA data collection and use policies; and
6. Limit the collection of certain sensitive information for OBA purposes.

Below is a more detailed explanation of each of these obligations.

1. Ensuring Transparency

The *Principles* assign responsibility for consumer transparency and control concerning OBA practices to Third Parties (i.e., the entity collecting the data for OBA purposes is responsible for complying with this aspect of the *Principles*).

You should provide notice of your data collection practices on your own Web site. This notice should be clear, meaningful and prominent, and should describe the following:

- The types of data collected online, including any personally identifiable information collected for OBA purposes;
- The uses of such data, including whether it will be transferred to another, unaffiliated entity for OBA purposes;
- An easy-to-use way for consumers to exercise choice with respect to the collection and use of data for OBA purposes or transfer of such data to other, unaffiliated entities for OBA purposes; and
- The fact that you adhere to the *Principles.*

In addition to the notice on your Web site, you should also provide "enhanced notice" to consumers whenever you are collecting or using data for OBA purposes on a non-affiliated Web site. This enhanced notice should take the form of a clear, meaningful and prominent link (the "enhanced notice link") to the information in your Web site notice. The link may be provided either by you or by the operator of the non-affiliated Web site ("First Party") on which you are collecting or using data for OBA purposes.

If you provide the enhanced notice link:

- You can place a link "in" an advertisement by locating it within the content of the advertisement, eg. an overlay;
- You can place a link "around" an advertisement by locating it within an area around the ad that you control; or
- With agreement from the (First Party) Web site operator, you can place a link "in another place" on the Web page where the OBA data is collected, as long as it is clear, meaningful and prominent.

If the (First Party) Web site operator provides the enhanced notice link on its site, it should place the link on the Web page(s) where the data is collected or used for OBA purposes. The link should connect directly to a disclosure statement on the Web site itself that:

- Links to the www.AboutAds.info site if you are registered and listed on it; or
- individually lists you as a Third Party and provides a link to the information in your Web site notice.

The (First Party) Web site operator's provision of the enhanced notice link to the industry Web page will be particularly useful for Third Parties that are collecting data for OBA purposes on pages where they are not serving OBA advertisements.

Any enhanced notice link provided by the Web site operator should be distinct from the link to its own privacy policy.

In all cases, where the enhanced notice link takes the user to disclosure language about Third Party OBA practices in a general privacy policy, then the link should go directly to the relevant section of the privacy policy where the disclosure is located and not just generally to the privacy policy. Providing notice hidden in lengthy terms and conditions does not satisfy the requirement to provide clear, meaningful and prominent notice.

2. Providing Choice

You should provide consumers with the ability to exercise choice with respect to the collection and use of data for OBA purposes, and the sharing of this data with other unaffiliated entities. An example of a mechanism that would satisfy the choice requirement is one that allows a user to stop the collection and use of data for OBA purposes.

In all cases, the choice mechanism should be easy to use.

You should provide consumers with a choice mechanism in at least one of three locations:

- In the notice on your Web Site regarding OBA practices linked to by an "enhanced notice link" placed "in" or "around" the advertisement or elsewhere on the page with agreement from the Web site operator;
- From your listing on www.AboutAds.info that provides a choice mechanism. This approach will be particularly useful for entities that do not place a link to a notice in or around the advertisement, or that are collecting data for OBA purposes on pages where they are not serving advertisements, or in situations where multiple Third Parties are collecting and using data from a single advertisement; or
- In instances where you are individually listed in the (First Party) Web site operator's disclosure on the Web page where OBA data is collected, your choice mechanism should be available in the notice information on your Web site linked to from the Web site operator's listing.

3. Maintaining Data Security

You should maintain appropriate physical, electronic and administrative safeguards to protect the data collected and used for OBA purposes.

You should retain data that is collected and used for OBA only as long as necessary to fulfill a legitimate business need, or as required by law.

4. Changing Data Collection / Use Policies

You should obtain consumer consent before making any material changes to your OBA data collection or use policies and practices. A material change might be a decision to use or share previously collected OBA data in a new way. A change that results in less collection or use of data would not be considered material for purposes of the *Principles*. Consent requires an individual's action in response to a clear, meaningful and prominent notice.

5. Refraining from the Collection of Sensitive Information

You should not collect "personal information," as defined in the Children's Online Privacy Protection Act (COPPA), from children that you have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for OBA purposes, or engage in OBA directed to children that you have actual knowledge are under the age of 13 except as compliant with the COPPA.

In addition, you should obtain consent before collecting financial account numbers, Social Security numbers, pharmaceutical prescriptions or medical records related to a specific individual for OBA purposes. Consent requires an individual's action in response to a clear, meaningful and prominent notice.

Questions?

This Implementation Guide includes a detailed set of Frequently Asked Questions and answers regarding the entire scope of this industry-wide program. Additional information is also available online at www.AboutAds.info. Third Parties might find the following FAQs of particular interest:

- Why did the leading marketing and advertising trade associations develop the self-regulatory Principles for online behavioral advertising?
- What is the Advertising Option Icon? What does it mean?
- What is www.AboutAds.info? How does it work?
- I am engaged in collecting and using data for OBA purposes across multiple, non-affiliated Web sites. What do the Principles indicate that I should do?
- Do the Principles provide requirements for Third Parties to provide consumers with choice?
- If an entity is collecting OBA data from a Web page, but not serving advertisements based on that data, is it required to comply with the Principles?
- Do the Principles impose specific data security standards?

Self Regulatory Principles for Online Behavioral Advertising Implementation Guide

– "Service Provider" Responsibilities –

What is a "Service Provider"?

The *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles") apply broadly to the diverse entities that engage in online behavioral advertising ("OBA"), governing three major types of entities – First Parties, Third Parties and Service Providers – that work interdependently to deliver relevant advertising to specific computers or devices in ways that enrich the consumer online experience.

Under these *Principles*, a Service Provider is defined as "an entity that collects and uses data from all or substantially all URLs traversed by a web browser across Web sites for OBA purposes in the course of the entity's activities as a provider of Internet access service, a toolbar, an Internet browser, or comparable desktop application or client software and not for its other applications and activities." In short, Service Providers may provide Internet access, search capabilities, Web tool bars, Internet browsers, desktop applications, software or other similar services.

In order to fully understand the responsibilities of Service Providers and the environment in which you are operating, you should also read the "What Everyone Needs to Know" section of this Implementation Guide.

How Do the *Principles* Apply to Service Providers?

You have identified yourself as a Service Provider, which means that the service you provide enables you to have access to all or substantially all URLs accessed by your users and that in the course of your activities as such a provider, you collect and use such user data for OBA purposes. As an example, you may provide Internet access service or desktop application software such as browsers or Web tool bars.

[NOTE: If your company also acts as a Web site operator (a "First Party" under the *Principles*) and hosts online behavioral advertising on its Web site, or if it also engages in OBA on non-affiliated Web sites by means of a relationship with an advertising network or data company (a "Third Party"), the *Principles* may impose additional requirements on your activities. You should also review the sections of the *Principles* and this Implementation Guide directed to those types of entities.]

In your capacity as a Service Provider, you should do the following to comply with the *Principles*:

1. Provide a clear, meaningful and prominent notice on your Web site disclosing your OBA practices;
2. Obtain consumer consent for collecting and using data for OBA purposes and provide an easy-to-use method to withdraw such consent;
3. Provide appropriate security for, including limiting the retention of, the data you collect and use for OBA purposes and take appropriate steps to help preserve the de-identified status of data collected and used for OBA;

4. Obtain consumer consent before materially changing your OBA data collection and use policies; and
5. Limit the collection of certain sensitive information for OBA purposes.

Below is a detailed explanation of each of these requirements.

1. Ensuring Transparency

You should provide notice of your data collection practices on your own Web site. This notice should be clear, meaningful and prominent and should describe the following:

- The types of data collected online, including any personally identifiable information collected for OBA purposes;
- The uses of such data, including whether it will be transferred to another, unaffiliated entity for OBA purposes;
- An easy-to-use way for consumers to exercise choice with respect to the collection and use of data for OBA purposes or transfer of such data to other, unaffiliated entities for OBA purposes; and
- The fact that you adhere to the *Principles.*

2. Obtaining Consent, Providing Choice

The *Principles* require that you obtain a consumer's consent **prior to** collecting and using data for OBA purposes. Under the *Principles*, the term "consent" means an individual's action in response to a clear, meaningful, prominent notice regarding the collection and use of data for OBA purposes. The consent requirement applies to you only when engaging in OBA activities in your capacity as a Service Provider (i.e., if you are also engaging in OBA activities as a First Party or Third Party, different requirements apply when you are acting in those capacities).

Once you have obtained consent to collect and use data for OBA purposes, you should provide consumers with an easy-to-use choice mechanism to withdraw their consent for the collection and use of that data for OBA purposes.

3. Maintaining Data Security

You should maintain appropriate physical, electronic and administrative safeguards to protect the data collected and used for OBA purposes.

You should retain data that is collected and used for OBA only as long as necessary to fulfill a legitimate business need, or as required by law.

The *Principles* identify the following four additional steps that you should take regarding data collection and use when you are engaged in OBA:

- Alter, randomize or make anonymous (e.g., through "hashing" or substantial redaction) any personally-identifiable information or unique identifiers in order to prevent your data from being reconstructed into its original form in the ordinary course of business;

- Disclose the circumstances in which data that is collected and used for OBA is subject to the above process;
- Take reasonable steps to protect the non-identifiable nature of your data if it is distributed to unaffiliated entities by not disclosing the algorithm or other mechanism you utilize for randomizing or making it anonymous. In addition, obtain written assurance that such entities will not attempt to re-construct your anonymous data and will only use or share it for an agreed purpose, such as OBA, that was specified to consumers during the process to obtain their initial consent. This assurance is considered met if another entity, by contract, does not have the right to use your data for its own purposes; and
- Take reasonable steps to ensure that any unaffiliated entity that receives your anonymous data will itself ensure that further unaffiliated entities to which your data is disclosed also agree to the restrictions and conditions you are imposing. This requirement is also considered met if such unaffiliated entities, by contract, do not have the right to use your data for their own purposes.

4. Changing Data Collection / Use Policies

You should obtain consumer consent before making any material changes to your OBA data collection or use policies and practices. A material change might be a decision to use or share previously collected OBA data in a new way. A change that results in less collection or use of data would not be considered material for purposes of the *Principles*. Consent requires an individual's action in response to a clear, meaningful and prominent notice.

5. Refraining from the Collection of Sensitive Information

You should not collect "personal information," as defined in the Children's Online Privacy Protection Act (COPPA), from children that you have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for OBA purposes; or engage in OBA directed to children that you have actual knowledge are under the age of 13.

In addition, you should obtain consent before collecting financial account numbers, Social Security numbers, pharmaceutical prescriptions or medical records related to a specific individual. Consent requires an individual's action in response to a clear, meaningful and prominent notice.

Questions?

This Implementation Guide includes a detailed set of Frequently Asked Questions and answers regarding the entire scope of this industry-wide program. Additional information is also available online at www.AboutAds.info. Service Providers might find the following FAQs of particular interest:

- Why did the leading marketing and advertising trade associations develop the self-regulatory Principles for online behavioral advertising?
- What is www.AboutAds.info ? How does it work?
- The services that I provide enable me to have access to all or substantially all URLs accessed by my users and, in the course of my activities, I collect and use

such user data for OBA purposes. What do the Principles indicate that I should do?

- If an entity is collecting OBA data from a Web page, but not serving advertisements based on that data, is it required to comply with the Principles?
- Do the Principles impose specific data security standards?

Self Regulatory Principles for Online Behavioral Advertising Implementation Guide

– Frequently Asked Questions –

What is online behavioral advertising ("OBA")?

OBA is defined in the *Self-Regulatory Principles for Online Behavioral Advertising ("Principles")* as the "collection of data from a particular computer or device regarding Web viewing behaviors over time and across non-affiliated Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors."

Not all online advertising is considered OBA.

Do the *Principles* cover all online advertising?

No. The *Principles* cover only those activities that are defined as OBA.

As defined in the *Principles*, OBA does not include:

a. Activities of First Parties (Web site publishers / operators) that are limited to their own sites or affiliated sites over which they exercise direct control.

b. Contextual advertising, which is advertising based on the content of the Web page being visited, a consumer's current visit to a Web page, or a search query.

c. Ad reporting, the collection or use of information for statistical reporting, Web analytics/analysis and advertising metrics.

d. Ad delivery, the distribution or delivery of online advertisements or advertising-related services using Ad Reporting data and not based on user preferences inferred from information collected over time and across non-affiliated Web sites.

Why did the leading marketing and advertising trade associations develop the *Self-Regulatory Principles for Online Behavioral Advertising*?

Leading marketing and advertising industry associations initiated a comprehensive, self-regulatory effort to develop and implement consumer-friendly principles and enforcement standards regarding OBA.

This collaborative, industry-wide effort was supported by the American Association of Advertising Agencies (AAAA), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), the Interactive Advertising Bureau (IAB), and included the participation of the Council of Better Business Bureaus (CBBB), in response to the Federal Trade Commission's call to the advertising and media industry to develop self-regulatory principles and practices for OBA.

In July 2009, the Associations jointly released the *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles"), which are intended to apply broadly to the diverse set of actors that work interdependently to deliver relevant advertising intended to enrich the consumer online experience. The *Principles* call for:

- **Education** for consumers and businesses about online behavioral advertising and the Principles.
- **Transparency** about data collection and use practices associated with OBA, providing consumers with clear, meaningful and prominent notice through multiple mechanisms.
- **Consumer Control** over whether data is collected and used or transferred for OBA purposes, provided through easy-to-use consumer choice mechanisms.
- Appropriate **Data Security** for, and limited retention of, data collected and used for OBA purposes.
- Obtaining consumer consent before a **Material Change** is made to an entity's OBA data collection and use policies unless that change will result in less collection or use of data.
- Limitations on the collection of **Sensitive Data** collected and used for OBA.
- **Accountability** for entities collecting and using data for OBA purposes, including mechanisms for enforcement of the Principles.

To learn more about the background of this self-regulatory initiative, please read the section on "What Everyone Needs to Know."

How do I know if the activities of my organization are covered by the *Principles*?

The *Principles* apply only to those entities engaged in OBA. Not all online advertising is considered OBA.

While the *Principles* are intended to apply broadly across a wide range of marketing and media entities, they focus on the three major types of entities that – working interdependently – deliver relevant advertising to specific computers or devices in ways that enrich the consumer online experience:

- "**First Parties**": such as Web site publishers / operators;
- "**Third Parties**": such as advertising networks and data companies (including ad exchanges and data aggregators) and in some cases advertisers; and
- "**Service Providers**": such as any internet access provider, search engine, Web tool bar, browser, or other service that enables the provider to have access to all or substantially all URLs accessed by its users, that in the

course of its activities as such a provider, collects and uses such user data for OBA.

An entity's actions are governed by the respective *Principles* related to the particular role or roles it fulfills in collecting and using data for OBA purposes. For example, an entity can be a First Party through its provision of content or retail products on its Web site; can be a Third Party through serving advertisements on multiple unaffiliated Web sites as an ad network or data company or in some cases an advertiser; and can serve as a Service Provider by providing services such as an Internet access Service Provider; offering desktop application software such as a toolbar where by virtue of such services the entity has access to all or substantially all URLs accessed by their users, and that in the course of such services collect and use such data for OBA. Each function would be separately subject to the relevant provisions of the *Principles*.

Please read the sections for First Parties, Third Parties and Service Providers in this Implementation Guide to learn more about the specific responsibilities and requirements for each type of entity under the *Principles*.

What is the Advertising Option Icon? What does it mean?

The Advertising Option Icon is a specific mark created by the participating trade associations that, together with approved wording, can be used by First Parties, Third Parties and Service Providers engaged in OBA to signify their adherence to the *Principles.*

Third Parties serving behavioral advertising will use this icon in or around advertisements, or on the Web pages where data is collected and used for behavioral advertising. The icon will link to a clear disclosure statement regarding the data collection and use practices associated with that ad and an easy to use consumer choice option. Web pages where OBA data is collected can also use the Advertising Option Icon, or another clear, meaningful and prominent notice, to link to the disclosures and choice options provided by the principles.

The Advertising Option Icon and approved wording can be accessed at www.AboutAds.com.

What is www.AboutAds.info ? How does it work?

Leading marketing and advertising industry associations have joined to create this one-stop Web site, where consumers can gain detailed knowledge about online behavioral advertising and conveniently opt-out of some or all participating companies' online behavioral ads, if they choose. Entities engaged in the collection and use of data for OBA purposes can also register to participate in the choice mechanism and acquire the Advertising Option Icon on the site.

Many companies engaged in OBA, or on whose pages OBA data is collected or OBA ads are served, will link to this Web site.

Consumers using the Web site can choose to stop receiving OBA from a specific company listed to the page, or from all the participating companies.

The Web site can be found at www.Aboutads.info.

I am Web publisher and OBA activity occurs on my Web site. What do the Principles indicate that I should do?

In this capacity, you are acting as a First Party. Please read the section on First Party Responsibilities in this Implementation Guide closely and comply with all of the requirements discussed there**.**

In short, to ensure compliance with the Principles it may be preferable for both First and Third Parties to provide notice that makes consumers aware that OBA is occurring on the web site and provide consumers with a means to exercise choice regarding the collection and use of their data for OBA purposes. In addition, First Parties should obtain consumer consent before materially changing their OBA data collection and use policies.

I am a Web publisher. If I use data collected across my family of affiliated Web sites for OBA purposes, do the *Principles* say I should do anything?

In this capacity, you are acting as a First Party. Please read the section on First Party Responsibilities in this Implementation Guide closely and comply with all of the requirements discussed there**.**

In short, the *Principles* do not apply to the activities of First Parties (i.e., Web site publishers / operators) when Web viewing data is collected and used from your own site or across affiliated sites over which you exercise control. However, if you collect or allow others to collect OBA data from your Web site for advertising on non-affiliated Web sites, then you should in cooperation with Third Parties share in the work of complying with the *Principles* for those activities.

I am engaged in collecting and using data for OBA purposes across multiple, non-affiliated Web sites. What do the Principles indicate that I should do?

In this capacity, you are acting as a Third Party. Third Parties may include Advertising networks, data companies (including ad exchanges and data aggregators) and in some cases advertisers are examples.

Please read the section on Third Party Responsibilities in this Implementation Guide closely and comply with all of the requirements discussed there**.**

The services that I provide enable me to have access to all or substantially all URLs accessed by my users and, in the course of my activities, I collect and use such user data for OBA purposes. What do the Principles indicate that I should do?

In this capacity, you are acting as a Service Provider. Service Providers may provide Internet access, search capabilities, Web tool bars, Internet browsers, desktop applications, software or other similar services.

Please read the section on Service Provider Responsibilities in this Implementation Guide closely and comply with all of the requirements discussed there**.**

Do the *Principles* provide requirements for Third Parties to provide consumers with choice?

Yes, the *Principles* state that a Third Party should provide consumers with the ability to exercise choice with respect to the collection and use of data for OBA purposes, and the transfer of data to unaffiliated entities for OBA purposes. Please read the section on Third Party Responsibilities in this Implementation Guide closely and comply with all of the requirements discussed there**.**

If an entity is collecting OBA data from a Web page, but not serving advertisements based on that data, is it required to comply with the *Principles*?

Yes. The *Principles* define OBA as the practice of collecting data from a particular computer or device regarding Web viewing behaviors over time and across multiple, unaffiliated Web sites. Even if that data is not currently being used for the purpose of targeting the delivery of advertisements, the practice should be disclosed in accordance with the *Principles* and the remainder of the requirements still apply.

Do the *Principles* impose specific data security standards?

Yes. The *Principles* require all entities to maintain appropriate physical, electronic and administrative safeguards to protect the data collected and used for OBA purposes. The *Principles* also require all entities to retain data that is collected and used for OBA only as long as necessary to fulfill a legitimate business need, or as required by law.

The *Principles* also set forth steps that a Service Provider should take to de-identify OBA data they collect and use for OBA, disclose the de-identification process, help preserve the de-identified status of interest-based online data that is shared with unaffiliated entities, to safeguard the data and to be held accountable for the use of such data. Please read the section on Service Provider Responsibilities in this Implementation Guide closely and comply with all of the requirements discussed there**.**

Do the *Principles* limit the collection of Sensitive Data?

Yes. The *Principles* place the following limitations on the collection of Sensitive Data:

- Entities should not collect "personal information", as defined in the Children's Online Privacy Protection Act ("COPPA"), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for OBA, or engage in OBA directed to children they have actual knowledge are under the age of 13 except as compliant with COPPA.

- Entities should not collect and use financial account numbers, Social Security numbers, pharmaceutical prescriptions or medical records about a specific individual for OBA without Consent.

Do the *Principles* provide for accountability and enforcement mechanisms?

Yes. Both the CBBB and the DMA will play roles in ensuring compliance and enforcement of the Program. All DMA members – as a condition of membership – are required to comply with program's provisions. The CBBB and DMA will utilize a monitoring technology platform to foster accountability among participating companies with respect to the Transparency and Control requirements of the Principles, as well as manage consumer complaint resolution.