Online Behavioral Advertising: Trends and Developments

D. Reed Freeman, Julie O'Neill and Nicholas Datlowe, Morrison & Foerster LLP

Online behavioral advertising programs, which target consumers based on their interests and preferences, have recently faced enhanced scrutiny from consumer advocates and regulators. This article explores the evolving legal and self-regulatory landscape of online behavioral advertising, and outlines key practical considerations for companies.

Online behavioral advertising (OBA) is one of the hottest topics in technology and privacy law today. Consumer advocates and journalists have brought attention to the practice, and have argued that consumers should be more informed and have more control over the data used for OBA. Regulators and legislators have presented various proposed approaches designed to achieve this goal. However, at the time of going to press, these amount solely to recommendations from the Federal Trade Commission (FTC) and bills pending in Congress.

Meanwhile, the advertising industry has developed a self-regulatory regime that is designed to meet the concerns expressed by regulators and legislators. In addition, several browser manufacturers have adopted browser-based tools to directly empower consumers.

This body of "soft law" is only now starting to take form, and it is expected not only to grow in volume and complexity, but also to remain fluid for some time. To make informed decisions on how to structure advertising programs, companies should understand the current regulatory, self-regulatory and legislative trends and developments in this area. This article explores:

- The US regulatory framework, including two reports released by the FTC:
  - a report that sets out advisory principles for self-regulation; and
  - a report that provides a preliminary indication on how the FTC believes consumer privacy should be protected going forward (see *FTC Self-regulatory Principles* and *FTC Preliminary Privacy Report*).
- Industry initiatives to create principles and guidelines (see *Self-regulatory Background and Developments*).
- Technology designed to empower consumers, specifically, browser implementation of do-not-track functionality (see *Browser-based Tools*).
- Proposed US legislation aimed at regulating OBA practices (see *Proposed US Legislation*).
- EU regulatory developments (see *EU Developments*).
- Key practical considerations for industry participants (see *Practical Tips*).

WHAT IS ONLINE BEHAVIORAL ADVERTISING?

For regulatory purposes, the FTC offered in a February 2009 staff report the most concise definition of OBA:

online behavioral advertising means the tracking of a consumer's online activities over time – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests.

(FTC, *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising*, at 46 (Feb. 2009) (emphasis in original) (OBA Report).)

In the US, at least for now, OBA generally does not include:

- "First party" advertising, where no data is shared with third parties.
- Contextual advertising, where an advertisement is based on a single visit to a web page or single search query.
- First-party data collection and analysis for website optimization (analytics).

For website publishers and advertising networks, OBA promises a higher return from the delivery of advertising tailored to the specific consumer viewing the website. Consumers benefit from advertisement delivery focused on their interests and preferences. However, privacy advocates have expressed concern that consumers are not informed about the information collected on their browsing habits, and that consumers should have easy to use and persistent control over data collected about them for OBA purposes by website publishers and their service providers.

FTC SELF-REGULATORY PRINCIPLES

For over a decade, regulators and industry representatives have taken turns at creating OBA guidelines. The OBA regulatory framework began to take shape in February 2009 when the FTC staff released the OBA Report. The OBA Report marked the culmination of the FTC's review of the privacy issues associated with OBA in the preceding decade. It also reflected previous

enforcement actions brought by the FTC under Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices (*15 U.S.C. § 45(a)*) (see *Box, FTC Enforcement Actions*).

The Self-Regulatory Principles (FTC Principles) in the OBA Report are only advisory and do not have the force of law. Nevertheless, and in somewhat contradictory fashion, the OBA Report states that, where appropriate, the FTC will initiate investigations into potentially unfair or deceptive practices. It seems the FTC Principles will be a road map for these enforcement activities. At the same time, in the OBA Report the FTC demonstrated frustration with the OBA industry and urged it to adopt more meaningful and effective self-regulation.

Scope of the FTC Principles

The FTC Principles cover any information collected for OBA purposes that "reasonably could be associated with a particular consumer or with a particular computer or device." This broad definition was significant because it broke the traditional dividing line between:

- Personally-identifiable information.
- Anonymous data that is not, in isolation, personally identifiable, but which can become identified with a particular person. For example, click-stream data that, through reasonable efforts, could be combined with a consumer's website registration information.

The FTC repeated this point in its December 2010 preliminary privacy report (see *FTC Preliminary Privacy Report*).

Exclusions from OBA

The definition of OBA in the FTC Principles expressly does not extend to advertising that would otherwise meet the definition of OBA if it is in the form of a "first-party" relationship. A first-party relationship refers to single-site or single-domain tracking used by a website operator to personalize its site's (or sites') content and advertising. It remains unclear whether the exception extends to "retargeting," where a single site advertises its products and services on other sites using a service provider, based on consumers' activities on the first-party site.

The FTC Principles also exclude "contextual advertising," which is the delivery of advertisements based on a "consumer's current visit to a single web page or a single search query, without the collection and retention of data about a consumer's online activities over time."

Four Central Principles

The four central FTC Principles in the OBA Report cover:

- Transparency and consumer control (see *Transparency and Consumer Control*).
- Data security and data retention (see *Data Security and Retention*).
- Opt-in consent for the use of sensitive data (see *Opt-in Consent for Sensitive Data*).
- Opt-in consent for retroactive changes (see *Opt-in Consent for Retroactive Changes*).

Transparency and Consumer Control

The FTC Principles call for every website where information is collected for OBA purposes to provide "a clear, concise, consumer-friendly, and prominent statement" disclosing the collection practices and explaining that consumers have a choice concerning the collection and use of their information. They also call for a means for consumers to exercise their choice that is:

- Clear.
- Easy to use.
- Accessible.

This principle is consistent with the outcomes of the FTC's enforcement actions (see *Box, FTC Enforcement Actions*).

Concerned that privacy policies have become long and difficult to understand, and therefore an ineffective method of communicating information to consumers, the FTC urged companies to develop new ways to provide consumers with effective notice and choice outside of their privacy policies. This high disclosure standard marked a departure from the then-current industry standard of providing notice and choice solely within a privacy policy.

Some companies responded promptly by, for example, implementing links to "About Our Ads" and other similarly titled sections on their home pages. A coalition of industry trade associations also started an advertising icon program that is beginning to find widespread adoption (see *DAA Program Components*).

Data Security and Retention

The FTC Principles state that companies should provide reasonable security for data collected for OBA purposes consistent with FTC guidance. The level and type of security is flexible, based on a reasonability standard tailored to the:

- Sensitivity of the collected data.
- Nature of the company's business.
- Types of risks the company faces.
- Reasonable protections available.

Data should also be retained only as long as necessary to fulfill a legitimate business or law enforcement need.

Opt-in Consent for Sensitive Data

The FTC Principles provide that companies should obtain affirmative express consent before collecting sensitive data for OBA purposes. This is commonly referred to as opt-in consent. As a general principle, the difference between opt-in (express) consent and opt-out (implied) consent is a matter of the default. Opt-in consent refers to consent expressed through some sort of affirmative action, such as ticking a box that says "I Agree." Opt-out consent generally refers to a mechanism by which the OBA uses are explained and will take effect unless a consumer takes an affirmative action, such as ticking a box that says "Opt Out."

While the OBA Report does not provide an exhaustive definition of "sensitive" data, which the FTC believes requires opt-in consent for OBA use, it indicated that the following categories qualify:

- Financial and health information.
- Information about children.
- Precise geographic location information.
- Social Security numbers.

The FTC called on industry members and other stakeholders to develop standards around the definition and use of sensitive data. It also proposed consideration of whether certain categories of data are so sensitive that they should never be used for OBA.

Opt-in Consent for Retroactive Changes

According to the FTC Principles, companies should obtain affected individuals' affirmative express consent before using their previously collected information in a way that is materially different from the uses permitted under the privacy policy in place when the information was collected. Material prospective changes to privacy policies are subject to a more flexible approach that could include prominent notice and opt-out choice.

FTC PRELIMINARY PRIVACY REPORT

In December 2010, the FTC released a long-awaited preliminary staff report on privacy, "Protecting Consumer Privacy in an Era of Rapid Change" (Preliminary Privacy Report). The FTC expects to release a final report later this year.

The Preliminary Privacy Report outlines an exhaustive, broadly applicable framework for how "online and offline commercial entities that collect, maintain, share, or otherwise use consumer data" should protect the privacy of this data. The staff explained that this broad approach is supported by the fading of the traditional distinction between personally identifiable information and anonymous identifiable information resulting from changes in technology that make it possible to identify consumers from anonymous data.

Application to OBA

Important parts of the Preliminary Privacy Report are directly relevant to OBA. In particular, one of the report's overarching themes is the need for simplified consumer choice relating to information collection, use and disclosure.

The Preliminary Privacy Report proposes that choice should be implied for "commonly accepted" data uses and disclosures because, when a company uses or discloses data in a way that is commonly accepted and therefore expected by a consumer, it can reasonably infer consent. In the FTC's view, this category of obvious uses and disclosures is narrow, but probably includes first-party marketing. A company would be required to obtain a consumer's consent for all other uses and disclosures, including sharing data with a third party for its own marketing or other purposes.

The Preliminary Privacy Report also states that the consumers' choices should be clearly and concisely described and offered when the consumers are making a decision about their data. Consistent with the FTC Principles, this means that the disclosures should be made outside of the privacy policy and in a manner that is easy for consumers to see, understand and use.

The Preliminary Privacy Report states that stricter requirements should apply to sensitive data and sensitive classes of consumers, such as children. However, it does not otherwise specify whether or when an opt-in versus opt-out consent is required. The FTC has requested public comments on this and related issues, including how to define "sensitive information."

Do-not-track Mechanisms

The Preliminary Privacy Report takes the position that the most practical way to offer choice in the context of OBA is through a universal do-not-track mechanism.

According to the FTC staff, this would most likely involve the placement of a persistent setting, similar to a cookie, on consumers' browsers, signaling their choices about online tracking. The FTC believes it does not have the legal authority to develop and implement a do-not-track requirement, indicating that it must be accomplished through either legislation or private sector efforts. But, as part of the Preliminary Privacy Report, the staff sought public comments related to the proposal.

Notably, two of the five FTC Commissioners, while concurring with the Preliminary Privacy Report, expressed reservations with respect to a do-not-track mechanism. Commissioner Kovacic stated that the do-not-track proposal was premature, as the FTC first needed to present more evidence that consumer expectations of privacy are largely going unmet.

Commissioner Rosch stated that several questions need to be answered before the FTC should endorse any particular do-not-track mechanism. He expressed support for a do-not-track mechanism if it is technically feasible, but stated consumers should have to opt in to this mechanism, similar to entering their telephone numbers on the FTC's national Do-Not-Call Registry.

FTC Speeches and Testimony

Since the release of the Preliminary Privacy Report, FTC officials have repeatedly emphasized the benefits to consumers of a universal do-not-track mechanism.

One day after the Preliminary Privacy Report was released, David Vladeck, director of the FTC's Bureau of Consumer Protection, testified before the Subcommittee on Commerce, Trade and Consumer Protection of the House Committee on Energy and Commerce. He highlighted a do-not-track mechanism as an important component of the FTC's efforts to simplify consumers' control over the collection and use of their personal information. He explained that an appropriate do-not-track mechanism would be uniform, easy to use and widely adopted. This would relieve the consumers' burden of visiting multiple sites and trying to figure out how various opt-outs work. In addition, it should apply to all third-party tracking methods, so new technologies would

be unable to override a consumer's choices. Director Vladeck stressed that the FTC has not ruled out a self-regulatory regime, as long as there is a law enforcement agency that can enforce it.

In the following months, Director Vladeck and other FTC officials repeated the themes of improved transparency and consumer choice in various public appearances. However, as the adoption of a self-regulatory framework gained momentum (see *Self-regulatory Background and Developments*), the FTC appears to have softened its position. In written testimony presented to a Senate Subcommittee on May 19, 2011, the FTC stated that "recent industry efforts to improve consumer control are promising, but they are still in the early stage and their effectiveness remains to be seen."

SELF-REGULATORY BACKGROUND AND DEVELOPMENTS

The self-regulatory approach to OBA began in 1999 when the Network Advertising Initiative (NAI), an association of network advertisers, developed self-regulatory guidelines that required OBA vendors to, among other things:

- Disclose their OBA practices in their privacy policies.
- Make best efforts to have the OBA practices disclosed in their publisher clients' privacy policies.
- Offer an easy-to-use opt-out link.

The NAI periodically updated its guidelines, and the FTC initially endorsed them. However, as the use of OBA expanded, the FTC began to adopt a different approach. This approach was designed to increase the likelihood that consumers would understand the OBA uses of their data and more easily find and use a persistent opt-out mechanism, if they so choose. These themes resonate in the FTC Principles (see *FTC Self-regulatory Principles*) and in the Preliminary Privacy Report (see *FTC Preliminary Privacy Report*).

In July 2009, just five months after the release of the FTC Principles, the Digital Advertising Alliance (DAA), a coalition of media and marketing associations, released its own set of principles titled "Self-Regulatory Principles for Online Behavioral Advertising" (Industry Principles).

The Industry Principles largely mirror the FTC Principles, calling for:

- Education for both consumers and businesses about OBA and the Industry Principles.
- Transparency about data collection and use practices associated with OBA, by 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 opt-out mechanisms.
- Security for, and limited retention of, data collected and used for OBA.
- Consumer consent for material changes to OBA data practices.
- Limitations on the collection and use of sensitive data for OBA.
- Accountability for entities collecting and using data for OBA, including mechanisms for enforcement of the Industry Principles.

While the FTC commended the release of the Industry Principles, it continued to warn that the principles need to be adopted on a widespread level, and that the industry needed must move quickly to avoid government intervention.

In response, on October 4, 2010, the DAA announced the implementation of the Industry Principles into practice through a program titled "The Self-Regulatory Program for Online Behavioral Advertising" (DAA Program). Both the Direct Marketing Association (DMA) and the Interactive Advertising Bureau (IAB) also incorporated the Industry Principles into their respective codes of conduct. Members of the IAB must comply with the Industry Principles by August 29, 2011.

Scope of the DAA Program

The DAA Program covers the various entities that interact to deliver OBA. These entities include website publishers and advertising service providers (such as advertising networks and agencies) that collect and use online behavioral data to deliver advertisements.

The DAA Program places compliance obligations on publishers. A publisher can place the DAA Program icon (see *Advertising Option Icon*) on its website and link consumers who click on it to a notice containing the disclosures required by the DAA Program. A publisher can also comply through its advertising network, agency or other service provider, for example, by contractually requiring that the relevant third party participate in the DAA Program.

DAA Program Components

The DAA Program includes the following five major components:

- Participants must display an icon and accompanying language to inform consumers about data collection and use practices.
- A single, industry-developed website that allows consumers to opt out of OBA practices of companies participating in the DAA Program.
- A website dedicated to informing consumers about OBA and the DAA Program.
- Mechanisms for accountability and enforcement of the DAA Program.
- Campaigns for greater consumer education about OBA.

Advertising Option Icon

DAA Program participants must use an icon and accompanying language, displayed in or near online advertisements or on webpages where data is collected and used for OBA. The icon indicates that the advertisement is targeted and constitutes behavioral advertising. The fee to license the icon is $5,000 annually, but there is no fee for publishers with annual revenues from OBA of less than $2 million.

A consumer who clicks on the icon is brought to an explanation of the data collection and use practices associated with the advertising and an easy-to-use mechanism that allows the consumer to opt out. The opt-out page is dynamic. It lists each of the advertising service providers that is collecting information for OBA purposes and allows the consumer to opt out of collecting by service providers individually or collectively. By moving notice and choice outside of the privacy policy into a more conspicuous position, the icon and its click-through information and choice mechanisms represent a shift in industry practice consistent with the FTC Principles.

Second Consumer Choice Mechanism

Once the icon becomes widespread, consumers will also be able to visit a single, industry-developed website to opt out of some or all participating companies' OBA.

Dedicated Website

The DAA created a website, http://us.aboutads.info, to provide both consumers and businesses with information about OBA and the DAA Program, as well as to familiarize consumers with the icon.

Mechanisms for Accountability and Enforcement

Beginning later this year, the Council of Better Business Bureaus (CBBB) and the DMA intend to begin monitoring and enforcing DAA Program compliance. In addition, the CBBB plans to identify companies that are engaged in OBA but are not following the DAA Program. These organizations will also manage the resolution of consumer complaints about the OBA practices of participating companies.

Educational Campaigns

The DAA's trade associations will conduct educational campaigns targeted to both consumers and businesses. These will include webinars and other practical guidance for interested businesses on how to understand, implement and comply with DAA Program requirements.

DAA Program Adoption

The DAA hopes that widespread industry adoption of the DAA Program will prove to the FTC and legislators that self-regulation is sufficient and therefore legislative and regulatory intervention is unnecessary.

Participation in the program is voluntary, except for members of the DMA and the IAB. These mandatory participation requirements are significant because once a company makes a representation about its commitment to privacy, such as its participation in the DAA Program, its failure to honor that representation can be the basis of an FTC enforcement action on a deception theory.

However, the FTC's continued support for a do-not-track mechanism shows that it is not convinced that the DAA program, in and of itself, meets the criteria for an effective anti-tracking mechanism. Congress may also possibly step in and provide the FTC with rulemaking authority to require a do-not-track mechanism (see *Proposed US Legislation*).

BROWSER-BASED TOOLS

Following the FTC staff's support for a do-not-track mechanism in the Preliminary Privacy Report, the four major internet browser developers began to introduce their own set of browser-based tools to implement do-not-track functionality. This functionality is in addition to existing features that some of these companies already offer consumers to manage their preferences and opt out of targeted advertising.

Internet Explorer

Internet Explorer 9, the latest version of Microsoft's browser, was the first major browser released with do-not-track functionality. The primary anti-tracking feature is called Tracking Protection Lists (TPLs). Internet Explorer 9 automatically creates a personalized TPL based on sites a consumer visits. Any third-party site that tracks a consumer across ten or more pages (by default) is automatically added to the list. Consumers may also create their own TPLs or download them from third parties such as TRUSTe. The personalized TPL must be activated by the consumer, but downloading or creating a different TPL turns on the protection automatically.

Once installed or enabled, the TPL will stop any page the consumer visits from automatically sending consumer data to sites on the TPL. The personalized TPL is updated based on browsing habits, and Internet Explorer 9 periodically checks for updates to third-party lists. Because TPLs can be modified by consumers, they may tailor their lists to their preferences and more than one list may be active at a time. However, if there are conflicting instructions in active TPLs, Internet Explorer 9 will obey the instruction that allows transmission of the consumer data.

Microsoft also included Mozilla's header-based anti-tracking system (see *Firefox*). It is activated automatically whenever a consumer enables a TPL.

Firefox

Mozilla released a do-not-track feature for its Firefox 4 browser in March 2011. The feature is inactive by default, and the consumer must turn on the feature by checking a box marked "Tell web sites I do not want to be tracked" in Firefox's Options window. After the feature is enabled, when the browser sends or receives data it includes a notification in the form of a header that requests that the loaded page (as well as the site's advertisers and other content providers) does not track the consumer. However, compliance with the request is voluntary.

While this header-based utility is the most innovative and potentially most flexible industry solution currently available, it raises several questions for advertising industry participants and consumers. Chief among these questions is just what the header means:

- Does the header mean that the consumer has expressed a preference not to be tracked by third-party advertising service providers employed by advertisers and publishers?

- Does it mean no tracking across domains?
- Does it mean no tracking for advertising purposes by anyone, including first parties?
- Does it mean that the consumer has expressed a preference not to be tracked at all, by anyone, for any purpose?

Most advertisers, publishers and advertising service providers appear to be in the process of evaluating this mechanism. As of June 1, 2011, at least three advertising networks (Blue Kai, Chitika and AdInsight) and at least one publisher (the AP) have agreed to follow it. Use of the header is not part of the DAA Program and is therefore not subject to DAA monitoring or enforcement, or FTC enforcement for failure to comply with the DAA Program after having represented compliance. It is also not clear yet whether the FTC would have an unfairness cause of action against an advertising server provider who is not a DAA member for failing to comply with the header.

Safari

Apple has publicly announced that it intends to release its Safari 5.1 browser with OS X 10.7 (Lion) in July 2011. This new version of Safari will support the browser-based header system for tracking protection. As Safari's default setting does not accept third-party cookies, this functionality is in addition to the substantial tracking restrictions already in place.

Chrome

Google has not implemented any true anti-tracking feature in its Chrome browser. Instead, Chrome offers an add-on, a small program that runs within a browser, called "Keep My Opt-Outs." The typical expression of a consumer's opt-out choice is an opt-out cookie. However, the consumers who opt out of online tracking also tend to delete cookies. The add-on retains opt-out cookies when other cookies are deleted.

Google's reluctance to adopt a browser header mechanism (see *Firefox*) or a TPL (see *Internet Explorer*) is based on its belief that no consensus exists about what tracking is or how to provide it in a way that respects consumers' current privacy controls. Notably, the World Wide Web Consortium conference in April 2011 on Tracking and Targeting focused heavily on these questions, and revealed that no consensus exists.

PROPOSED US LEGISLATION

Proposed federal and state legislation has addressed OBA directly, and also indirectly as part of an overarching focus on privacy or focused directly on the regulation of OBA.

Federal Privacy Legislation

Multiple bills have been introduced in the current Congress that address privacy holistically. These include:

- The Commercial Privacy Bill of Rights Act of 2011 in the Senate (S. 799).
- The Consumer Privacy Protection Act of 2011 in the House (H.R. 1528).

Because the scope of each bill is broad, each faces an uphill battle to passage. However, both bills seek to provide consumers with more transparency and more choice with respect to OBA.

Federal Do-not-track Legislation

So far in the current Congress, three bills have been introduced that directly target online tracking:

- **Do-Not-Track Online Act of 2011 (S. 913).** Introduced in early May 2011 by Sen. John D. (Jay) Rockefeller IV (D-W. Va.), chairman of the Committee on Commerce, Science and Transportation, the Do-Not-Track Online Act of 2011 (S. 913) would require the FTC to adopt and enforce a trade regulation rule by creating a mechanism for consumers to express their preference not to be tracked online or on mobile devices, and it would require companies to honor that preference. Companies would be permitted to continue to collect the information necessary to function and be effective, though they would have to destroy or to make anonymous that information when it was no longer needed. The bill does not specify how a do-not-track mechanism would be structured.
- **Do Not Track Me Online Act (H.R. 654).** Introduced in February 2011 by Rep. Jackie Speier (D-Cal.), the Do Not Track Me Online Act (H.R. 654) would direct the FTC to set up rules for an opt-out mechanism to allow consumers to easily prohibit the collection or use of their online activities and information. Some data collection and use would be allowed, such as to provide a requested product or service or for basic business functions.
- **Do Not Track Kids Act of 2011 (H.R. 1895).** Introduced on May 13, 2011 by Reps. Edward J. Markey (D-Mass.) and Joe Barton (R-Tex.), the Do Not Track Kids Act of 2011 (H.R. 1895) would amend the Children's Online Privacy Protection Act of 1998 (COPPA) to prohibit the use of personal information to deliver OBA to children or minors by any operator:
  - of a website, online service, online application or mobile application that is directed to children or minors; or
  - that has actual knowledge that it collects personal information from children or minors.

The narrow scope of these bills, together with the support of the do-not-track mechanism derived from the success of the Do-Not-Call Registry, makes them more compelling candidates for action this term.

EU DEVELOPMENTS

While the US legislative landscape is in its early stages, the EU has modified its established privacy framework in the form of an amendment to several existing directives aimed at cookies and other information written to consumers' computers. Depending on how the EU's enabling legislation is implemented in the EU member states, this amendment has the potential to have a substantial impact on OBA practices.

In November 2009, the European Parliament passed Directive 2009/136/EC (Directive), amending (among other things) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

For OBA purposes, the key part of this EU-wide enabling legislation addresses information stored on users' "terminal equipment." Specifically, the Directive, sometimes known as the "Cookie Directive," requires that member states ensure the storing of information, or accessing of previously stored information, in the "terminal equipment" of a user is only allowed if the user "has given his or her consent, having been provided with clear and comprehensive information . . . about the purposes of the processing" (*Official Journal of the European Union*, No. 337 "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009," at 30 (Dec. 12, 2009)).

There are exceptions for technical storage or access that is for the sole purpose of carrying out an electronic communication or "strictly necessary" to provide an explicitly requested service.

Member states had to transpose this Directive into national legislation by May 26, 2011. However, at the time of going to press, only Denmark, Estonia, Finland and the United Kingdom have done so. About 11 other member states are at various stages in their legislative process.

There are three key uncertain issues associated with the implementation of the Directive into national legislation:

- What information is "strictly necessary," to provide an explicitly requested service and therefore outside the scope of the Directive.
- Whether consent must always be express (opt-in), or whether it may be implied, at least in some cases.
- Whether Recital 66 to the Directive, which provides that where technically possible and effective, the user's consent may be expressed by the appropriate settings of a browser setting or other application, will make its way into national law.

The delay in implementation by most jurisdictions suggests these issues are meriting close scrutiny. Similarly, for those jurisdictions that have implemented legislation, official guidance, such as from the UK's Information Commissioner's Office, and the scope of future enforcement actions may go some way toward addressing these open areas.

PRACTICAL TIPS

As the OBA landscape continues to develop, all industry participants, including advertisers, service providers and website publishers, must stay engaged, flexible and attentive to developments and new risks.

There are likely to be ever increasing demands for transparency, choice and widespread best practices relating to information security and data collection. Companies that follow these trends, and adapt to meet demands as they emerge, will be best positioned for long-term success. This is because they will have demonstrated a progressive attitude toward their customers and will also be less likely to have their brands tarnished by regulatory or private enforcement.

Specifically, all parties involved with OBA, including advertisers, publishers and advertising service providers, should:

- Evaluate their existing public representations and compare them to their actual practices. FTC enforcement actions have emphasized that companies must:
  - abide by their promised conduct;
  - avoid material omissions regarding their practices; and
  - respect the control mechanisms offered to consumers.
- Stay engaged and up to date with the latest developments. For example, the FTC's Final Privacy Report, which is expected later this year, may provide additional detail on what the FTC considers "sensitive data."

Website publishers should also:

- Review their privacy policies. In addition to making sure these policies are accurate and complete, publishers should consider including clear instructions on how to control browser preferences for cookies.
- Periodically audit their websites. Often publishers are unaware that their sites are calling servers and therefore cookies are being placed by third-party companies. These activities may be the result of old relationships or test campaigns. If a site does not need to call third-party servers, the publisher should delete the Javascript for web beacons making the calls.
- If their websites collect information for OBA, consider:
  - requiring that the advertising service providers who display OBA advertisements on their sites are members of the DAA, and that they display the icon in or around all OBA advertisements; or
  - licensing the DAA icon directly and displaying it on their pages.

Advertisers should also:

- Require that all service providers they use to display OBA advertisements are, at least, members of the DAA program and that these service providers display the DAA icon in or around all of their advertisements.
- Be engaged with their advertising service providers regarding their use of the header data made available by Firefox, Internet Explorer 9 and Safari. The significance of the header will become clearer over time, and as it does, the failure to respect it will likewise become more risky.
- Be careful with the scope of the data they and their advertising service providers use for OBA purposes. At this stage, the use of health characteristics, exact geographic location, financial information or information regarding children should be carefully vetted before being used in an OBA campaign.

FTC ENFORCEMENT ACTIONS

The FTC Principles are based in large part on the FTC's own enforcement actions. Key enforcement actions relate to either:

- Insufficient disclosure of online information collection practices (see *Actions relating to Transparency and Consumer Control*).
- Neglecting to obtain opt-in consent for material changes applied retroactively (see *Actions relating to Opt-in Consent for Retroactive Changes*).

Actions relating to Transparency and Consumer Control

The FTC Principle of transparency and consumer control (see *Transparency and Consumer Control*) stems from multiple FTC actions focusing on companies' failures to sufficiently disclose the fact, scope or purpose of their online information collection practices. These cases were brought on a deception theory cause of action.

Before the FTC Principles

In 2004, the FTC brought an action against Advertising.com, alleging that it represented that its product was an online security program but failed adequately to disclose that the product collected IP addresses and browsing activity in order to deliver targeted pop-up advertisements. The FTC brought a similar claim in 2006 against Odysseus Marketing, Inc., which marketed its product as an online anonymity program, but allegedly failed to clearly disclose that it collected data about customers' activity to send targeted pop-ups and other advertisements.

In both cases, the FTC found that disclosure in an End User License Agreement (EULA) was insufficient to cure the deception.

After the FTC Principles

The FTC has continued this line of enforcement activity since releasing the FTC Principles.

In June 2009, it announced that it had settled charges with Sears Holdings Corp. The company had allegedly paid consumers to download software that it said would confidentially track their browsing. The FTC claimed that the software monitored all online activity and had access to desktop documents and that disclosure in the EULA, or even in the unavoidable install process, was insufficient.

Similarly, in December 2010, the FTC announced a settlement with EchoMetrix, a company that sold software that enabled parents to monitor their children's online activities. The company allegedly failed to adequately disclose that it sold information that it collected from children through this software to third-party marketers.

In March 2011, the FTC announced its first OBA case against a network advertiser, Chitika, Inc., which acts as an intermediary between website publishers and advertisers. The FTC settled charges alleging that Chitika had tracked consumers' online activities even after they had opted out of tracking. The opt-out lasted for only 10 days (reports indicated that this was the result of a programming error), violating the company's claims about its opt-out mechanism. The proposed consent order imposes injunctive relief, including the requirements that:

- Every targeted ad delivered by Chitika include a link to a clear opt-out mechanism that allows a consumer to opt out for at least five years.
- Chitika alert consumers who previously tried to opt out that their attempt was not effective and that they should opt out again to avoid targeted advertisements.
- Chitika destroy all identifiable consumer information that it collected when the defective opt-out was in place.

Actions relating to Opt-in Consent for Retroactive Changes

The FTC Principle requiring opt-in consent for material changes applied retroactively (see *Opt-in Consent for Retroactive Changes*) is also based on FTC enforcement actions.

In 2004, the FTC alleged that Gateway Learning Corp. sold consumer data in a way that violated its privacy policy and then modified its policy and applied new language to data previously collected (*In re Gateway Learning Corp., No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004)*). The FTC's consent agreement with Gateway requires opt-in consent for material changes to its privacy policy.

More recently, the FTC announced a proposed settlement with Google, Inc. The FTC alleged that Google disclosed information concerning its Gmail service users' in a manner for which it had not obtained prior consent, in violation of its privacy policy. The proposed order would require Google to obtain users' opt-in consent before sharing their information with third parties if the sharing is contrary to any privacy promises made when the users' information was collected.

