

media  
contacts

**INSIGHT**

# NAVIGATING ONLINE CONSUMER PRIVACY

June 2011



**HAVAS**  
DIGITAL

## LEAD CONTRIBUTORS

---



**ADAM KASPER**

Director of Digital Investments  
Media Contacts USA  
[adam.kasper@havasdigital.com](mailto:adam.kasper@havasdigital.com)



**TOM PENQUE**

Managing Director  
Media Contacts Boston  
[tom.penque@havasdigital.com](mailto:tom.penque@havasdigital.com)



**ANDREW ALTERSOHN**

Regional Manager  
Havas Digital North America  
[andrew.altersohn@havasdigital.com](mailto:andrew.altersohn@havasdigital.com)



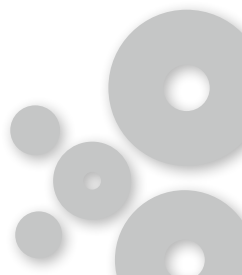
**MARK EGAN**

Director of New Business  
Havas Digital Global  
[mark.egan@havasdigital.com](mailto:mark.egan@havasdigital.com)



**MEGAN MOKRI**

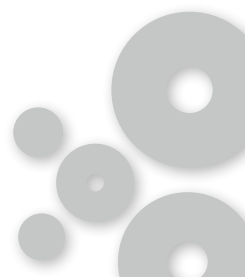
Director of Agency Relations  
Evidon  
[mmokri@evidon.com](mailto:mmokri@evidon.com)



## CONTENTS

---

Introduction .....	3
What Data are Being Collected? .....	5
Response from the Industry, Self-Regulation from the DAA .....	6
Response from the US Government .....	8
The FTC's Framework .....	9
Similar Movements in Europe .....	11
The Impact on the Industry Everywhere .....	12
What Marketers Need to Do: Short Term .....	14
Compliance Monitoring .....	18
Taking Action .....	18
The Longer Term View .....	21
Conclusion .....	23
Glossary .....	24
Sources .....	27
Contacts details .....	28



## INTRODUCTION

---

**Consumers live in a world where information about their behavior, habits, and activities is collected, analyzed, used, and shared.** While the practice of marketers using consumer data is nothing new –banks and credit card companies have been doing it for decades– the issue is amplified in the digital world where data and information are used (in near real time) to deliver better services, increase marketing relevance, and improve the effectiveness of advertising spend. In most instances, the use of data is not visible to or readily known by the user, as it is delivered through cookies or snippets of code, but still, most Americans appear deeply concerned about Internet privacy. According to a telephone poll of 1,019 adults conducted in December 2010 by the Gallup Organization and *USA Today*, 67% of respondents would prevent advertisers from showing them ads based on websites they have visited. However, these same consumers need to know what such a decision could mean. If they limit access to their data, their experience on many websites and search engines would change significantly, limiting the customization and personalization consumers have grown accustomed to while hampering some marketer's ability to serve up meaningful content, well-targeted offers, and clear brand value.

“67% of respondents would prevent advertisers from showing them ads based on websites they have visited. However, these same consumers need to know what such a decision could mean”

Consumer privacy in the digital age is not a new issue. As far back as 1973, the **United States Federal Trade Commission (FTC)** introduced its Fair Information Practice Principles (FIPPs) for the electronic marketplace. With the burgeoning adoption of the Internet, in 1995 the FTC specifically started addressing online privacy issues through recommendations for maintaining privacy-friendly, consumer-oriented data collection practices, with the key digital privacy challenge being enforcement. The marketing industry has created, in various forms, a fair number of sound best practices regarding privacy, but within the industry many questions remain on how these policies should be policed and enforced.

As digital media produces larger and more advanced sets of audience data and information, the FTC and its European counterparts, along with consumer and industry privacy advocates, have become ever more concerned with how to ensure the fair use of the data that is generated from digital brand activities. The FTC advocates greater education and protection of consumers online, urging users be provided with greater



transparency and a simpler choice as it relates to the information and data collected. Currently, the practices are not enforceable by law, and adherence to these principles is primarily enforced through self-regulation. However, the FTC is threatening increased government oversight and enforcement, should these self-regulation efforts prove to be ineffective.



From the current situation, an important questions arise: **“What can marketers do to put consumers more at ease about they type of data being collected, while still delivering relevant messages and content?”** This paper strives to bring some clarity to this question by laying out the current marketplace situation, identifying the role of marketers in the privacy ecosystem and identifying immediate and long-term strategies for agencies, advertisers, aggregators and publishers to ensure compliance and give consumers a say in how the data they gerenate is used.

## WHAT DATA ARE BEING COLLECTED?

---

Consumer data used to target digital advertising are **primarily derived from three sources:**

- **Actual behavior:** Occurs when a user visits the website or other owned media property of a marketer and receives online ad in future browsing sessions based on this visit.
- **Inferred interest:** Targeting based on a consumer's browsing behavior in similar or related content (e.g. a marketer delivering a luxury car ad to someone who recently visited the BMW 5-series section on Edmunds.com)
- **Predicted response:** Utilizes multiple and sophisticated data sets to create models that predict actions the audience might take.

“In 2012 eMarketer predicts spend on behaviorally targeted advertising will rise to \$1.7 billion, a 25.9% increase from 2011”

Because of the potential for precise targeting with reduced advertising waste combined with improved consumer relevance, **online behavioral advertising (OBA)** typically outperforms other media types, delivering the highest return on investment compared to other approaches to display advertising. As a result, it spawned a new segment of advertising formats, tools, and business offerings that advocates a data-driven model of online marketing, where data can be valued independently of the media. In full disclosure, Havas Digital and its Media Contacts subsidiary have always been a data-driven agency, taking great strides to protect consumers' Personal Identifiable Information (PII) and delivering maximum results by enhancing the consumer experience without risk to a clients' brand or reputation.

## RESPONSE FROM THE INDUSTRY, SELF-REGULATION FROM THE DAA

In reaction to potential legislation restricting use of data marketing to consumers, a group of marketing and advertising industry associations formed the **Digital Advertising Alliance (DAA)** to define, implement, and oversee self-regulation of OBA practices. The DAA is made up of the American Association of Advertising Agencies (AAAA), American Advertising Federation (AAF), Association of National Advertisers (ANA), Council of Better Business Bureaus (CBBB), the Direct Marketing Association (DMA), Network Advertising Initiative (NAI), and the Interactive Advertising Bureau (IAB). The DAA, along with a mix of publishers, advertisers, and agencies, created and issued the "Self-Regulatory Principles for Online Behavioral Advertising."

Issued in July 2009, these principles focus on the appropriate approach to take with OBA to address the FTC's concerns around education, policies, disclosure, transparency, and control. They cover the collection of data online, how that data are being used to predict user behavior to deliver advertising, and the approaches to take with regards to the use of first party cookies (i.e., those a marketer places on its website for its own purposes) vs. that of third party cookies (i.e., those cookies or tags placed on a marketer's website to be used by a partner).



### Digital Advertising Alliance (DAA):

American Association of Advertising Agencies (AAAA)

American Advertising Federation (AAF)

Association of National Advertisers (ANA)

Council of Better Business Bureaus (CBBB)

Direct Marketing Association (DMA)

Network Advertising Initiative (NAI)

Interactive Advertising Bureau (IAB)

**There are seven DAA principles:**

- 1. Education:** participate in efforts to educate consumers and businesses about OBA.
- 2. Transparency:** deploy mechanisms for clearly disclosing and informing consumers about data collection and usage.
- 3. Consumer Control:** provide mechanisms so consumers have the ability to choose whether or not data are collected about them.
- 4. Data Security:** provide reasonable security for data collected and used.
- 5. Material Changes:** obtain consent before applying any changes to OBA data collection and usage.
- 6. Sensitive Data:** apply heightened protection of certain consumer data (e.g., children's data, financial numbers, medical information, etc.)
- 7. Accountability:** implement policies and procedures to adhere to the principles.

Other industry groups have formed around this issue as well. The **National Advertising Review Council (NARC)** is a self-regulated industry group that was formed to monitor compliance efforts. If advertisers are deemed non-compliant with the DAA principles, they risk further investigation by the NARC. Most recently the Web Analytics Association (WAA) also published its own guiding principles regarding the ethics of using personal information related to enhancing advertising.

## RESPONSE FROM THE US GOVERNMENT

---

While the industry has made advances in improving transparency, control, and accountability, US, government agencies –along with a number of representatives in Congress– have expressed concerns that **the industry’s efforts have been too slow and have failed to provide adequate and meaningful protection for consumers**. The industry has also been criticized for its inability to enforce existing policies and there is a growing momentum around online privacy legislation.

In December 2010, the US Commerce Department called for a privacy **Bill of Rights for online consumers**, as well as the establishment of an office within the department to strengthen privacy policies in the United States. Shortly thereafter, the FTC issued a preliminary report titled “Protecting Consumer Privacy in an Era of Rapid Change.” In this report, the FTC contends that though many companies use privacy policies to explain their practices, they have become “long and legalistic disclosures that consumers usually don’t read and don’t understand. In recent months there has been greater Congressional interest in protecting consumer privacy. Most notable has been the online privacy bill backed by Senators John Kerry and John McCain.” Additionally, the FTC believes that under the current approach, consumers bear too much of the burden in protecting their privacy.

The Kerry-McCain bill underscores growing bipartisan support for this topic. Their proposed bill is in line with current self-regulations and also includes opt-out standards for OBA. It does not, however, include any provision for Do Not Track, instead focusing on the use of information collected, rather than the collection of data themselves (with requirements stipulated only for sensitive data). The bill does give the FTC the authority to write rules for data gathering.

Senators Kerry and McCain are not the only ones in Congress to propose such measures. Rep. Jackie Speier introduced the “Do Not Track Me Online Act of 2011” in February. His effort came on the heels of Rep. Bobby L. Rush who reintroduced his own privacy bill from the previous Congressional session. Also floating in the House is a bill from Rep. Cliff Stearns that focuses on providing consumers with notice of what information is being collected and how, leaving it largely to the companies themselves to self-regulate for compliance.

The White House, given its recent recommendation that Congress enact legislation with regards to online privacy, supports these efforts.



## THE FTC'S FRAMEWORK

---

In its report, *Protecting Consumer Privacy in an Era of Rapid Change*, the FTC defined **three principles** that businesses should follow to reduce the burden on consumers and ensure basic privacy protections:

1. **Privacy by design**
2. **Simplified consumer choice**
3. **Greater transparency**

### PRINCIPLE 1: PRIVACY BY DESIGN

The first principle recommends that companies adopt a “privacy-by-design” approach by **building privacy protections into their everyday business practices**. Such protections include reasonable security for consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy. This would also entail the implementation and enforcement of procedurally sound privacy practices throughout their organization, including assigning personnel to oversee privacy issues, training employees, and conducting privacy reviews for new products and services.

### PRINCIPLE 2: SIMPLIFIED CHOICE

The second principle states that **consumers should be given a choice about whether they want data about them to be collected and shared**. To ensure this, companies will need to describe consumer choices clearly and concisely, and offer easy-to-use choice mechanisms for opt-in or opt-out.

It should be noted that offering choice is not required for certain commonly accepted practices. This includes data collection and usage for: product and service fulfillment; internal operations to improve customer service or the user experience; fraud prevention; legal compliance; and first-party marketing (e.g., recommendations based on consumer’s prior behavior on that website). Outside of these instances, informed and meaningful consumer choice is required.

Mechanisms that provide choice will need to be displayed clearly on the page where consumers input personal information or at the point of sale. Sensitive information (e.g., that about children, financial and medical information, or precise geo-location data) would warrant special protection and require affirmation of consent.

In those instances where a consumer's online behavioral activity is being collected and/or tracked for the purpose of delivering targeted advertisements, the FTC recommends a legislative "Do Not Track" mechanism, similar to the national Do Not Call list for telemarketing, which would allow consumers to opt-out of the collection of information about their Internet behavior for targeted ads.

### PRINCIPLE 3: GREATER TRANSPARENCY

The FTC recommends other measures to improve the transparency of information and related practices. The report recommends **allowing consumers "reasonable access" to the data that companies maintain about them**, particularly for non-consumer facing entities such as data brokers. Finally the FTC proposes that stakeholders undertake a broad effort to educate consumers about commercial data practices and the choices available to them.

However, the FTC's online privacy report left a number of transparency issues open for additional comment, including the feasibility of standardizing notices, the approach for providing user access to data/profiles, whether consent is an "opt-in" or "opt-out" function, and the impact these issues have on affiliate marketing. The current DAA model focuses on an opt-out approach vs. opt-in. During the coming months, the FTC may endorse more stringent rules that require an opt-in approach. Though business should support increased transparency of their data practices, the way forward for the industry is still an open issue.

Though the scope of these principles encompasses OBA, they apply to a broader area of data capture and usage. In addition, those responsible for compliance go beyond marketers and businesses to include government policymakers as well.

Specifically, the framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or device. It encompasses both offline and online entities that collect data, as well as those that directly and indirectly interact with consumers. It is also not limited to only those who collect personally identifiable information (PII). These principles are intended to cover both PII and non-PII information since the distinction between the two is blurred by technology that allows the data to be combined to potentially re-identify consumers.

## SIMILAR MOVEMENTS IN EUROPE

---

Like the FTC, the European Union is advancing measures to ensure that Web users have greater transparency around cookie data being captured and a better understanding of how this data is being used, whether it is to store passwords or target them with relevant marketing messaging. On May 25, 2011, an amendment to the EU's **Privacy and Electronic Communications Framework and Directive** will come into effect. It requires European businesses and other organizations to obtain explicit consent from web users being tracked via cookies.

The EU's directive states that accessing or storing information for services explicitly requested by the user (e.g., making an e-commerce transaction) would be exempt from the need for consent. However, the mechanism of how the user is deemed to have given consent is not explicit in the directive. In the UK, the Government supports the EU directive but acknowledges the importance of the Internet economy saying: "We need to make sure these changes do not make using the Internet more difficult."

To date, in the UK the **Information Commissioner's Office (ICO)** has said that website operators can deliver cookies so long as the relevant information is outlined to users in their privacy policy. The government has rejected the notion of a strict opt-in system, worried that it may damage innovation. It has sought instead to grant the ICO leeway to interpret the new directive. While the ICO has stated that guidelines to businesses will not be made available before the directive comes into force on May 25, ICO is expected to follow the government's stance as it has done on previous occasions and require marketers to be compliant with the industry self-regulatory approach.

As seen stateside, the **IAB Europe is working with its EU partners** across the industry to implement a pan-European self-regulatory framework to enhance transparency and consumer control. This will involve a contextual notice or "icon" and control tool, similar to what is currently being deployed in the US. This approach has the support of the European Commission.

“Website operators can deliver cookies so long as the relevant information is outlined to users in their privacy policy”

## THE IMPACT ON THE INDUSTRY EVERYWHERE

---

At face value, **giving consumers the right to opt-out of online tracking should be an easy solution** to address a number of privacy concerns raised by the FTC. Given the way privacy policies and opt-out procedures have typically been buried in legal-rich disclosures, the current approach and process needs to be simplified.

The FTC's guidelines, along with pressure from other government agencies and consumer and privacy groups, will continue to shift a greater portion of the privacy burden to businesses. This will require organizations to improve policies, procedures, and disclosures –as well as ensure they stay in compliance with the FTC's framework.

Media Contacts recommends that brands **go further** than meeting the minimum requirements as it will only improve consumer trust and brand loyalty. If history is any indication, the industry, specifically in relation to OBA, risks a fate similar to that of Gator Corp. Gator Corp. was a company that embedded tracking –commonly called spyware– in free downloadable apps and then sold advertising outside of the browser in the form of pop-up and pop-under ad units. Gator was singled out by the FTC and made an example of for these types of deceptive practices in 2003. This action enabled industry associations to gain traction against similar practices, effectively shutting down this area of the online marketing industry.

“Media Contacts recommends that brands go further than meeting the minimum requirements as it will only improve consumer trust and brand loyalty”

Meanwhile, broad consumer adoption of “opt-out” mechanisms, such as a national Do Not Track server or a browser-based cookie-blocking application (e.g., Microsoft's Internet Explorer 9, Mozilla's Firefox, and Apple's Safari), will most certainly impact and change the dynamics of digital advertising options and the ability to track performance. Behavioral targeting tactics could be limited both in approach as well as scale. This could take shape in a reduced scope for certain behavioral targeting tactics.

Without the ability to leverage audience data for OBA ads, brand websites and social communities will be hindered in providing targeted marketing content to the user; without data, the experience will be difficult to tailor to a consumer's activity and perceived interest may be completely indiscernible.

For some doomsayers, **this is the death knell of e-commerce**. If users potentially have to give consent every time they interact with a website that stores anonymous data, it could create a comparatively negative experience that will turn users away from browsing and purchasing online. A mass-rejection of cookies could also mean publishers will be constrained in personalizing content and marketers will no longer be able to target or track their online campaigns, leading to inefficiency and a lack of visibility for advertisers. It may also mean that protecting vulnerable audiences such as children will be made more difficult as cookies are one of the traditional means of identifying individuals online.

**Media Contacts believes this overstates the likely impact, but we do support improved user control and transparency.** We believe that this is best achieved through self-regulation that is clear, distinct, and enforceable. We are liaising closely with the IAB to ensure we are at the forefront of reacting to regulatory changes and to support our clients in implementing those requirements.

Media Contacts supports efforts to provide users with greater transparency and choice around data collection. We also fully support the "Self-Regulatory Principles for Online Behavioral Advertising," developed by the DAA.

## WHAT MARKETERS NEED TO DO: SHORT TERM

---

The issues associated with privacy and control over user data will continue to evolve. As outlined below there are a number of steps that marketers can take to ensure compliance.

### AUDIT YOUR CURRENT PRIVACY POLICY STATEMENT AND PROCEDURES

At a minimum, **every business must have a link on its website to the privacy/disclosure policy statement**. The statement itself should be written in a way that is straightforward and easy to understand. Since the privacy statement is the outward embodiment of the organization's data usage practices, it is important to make sure that the statement is in line with the organization's privacy and data collection processes and procedures.

As it relates to specific content, the privacy policy statement should include:

- **Disclosure of the practice of using third parties and data collection for marketing purposes.** If user-profiling tools are used (e.g., cookies, tags, log files, etc.), these tactics should be identified in the statement. Additionally, the statement should be specific with regards to whom data is being shared with and not framed in a less transparent manner (e.g., "We may/might share our data with...")
- **Link to an opt-out tracking service(s) for third party sources** (e.g., NAI)
- **Link to an external source for users to learn more about advertising and data collection** (e.g., AboutAds.info)
- **Link to an opt-out for the company's local/first-party tracking providers** (e.g., Google Analytics, Omniture, etc.)
- **Disclosure on policies and procedures regarding safeguarding and securing data/information**
- **Process of making changes to privacy statement**
- **Disclosure regarding compliance with the Children's Online Privacy Protection Act COPPA and other sensitive data** (e.g., financial, health, etc.)

Links to the privacy policy statement should be placed on the homepage, as well as on any page that captures personal information. Such a review and audit should be performed in conjunction with a company's CTO and legal staff/counsel.



## MONITOR AND MANAGE ALL THE PIXELS AND TAGS ON YOUR WEBSITE

Organizations need to know **what data is currently accessible to third parties** through its website. One area of exposure is old or outdated tracking pixels. Over time, tags may be forgotten and/or lie dormant, however, that does not mean that they are not accessible by the third parties they point to.

To manage this issue, companies should perform a comprehensive audit of all website tracking. Current tags should be documented and old tags should be removed. Every pixel needs to be documented with its location, the information on what data is passed through it, the date implemented, and what it is used for/vendor association. From there, the organization should implement an approval process for website instrumentation so pixels aren't randomly implemented. As part of the audit, the organization should ensure compliance with the established Privacy Policy and implement updates. In many cases Media Contacts recommends tag management solutions, such as TagMan, built off of container tags as a way to more efficiently manage this process.

Beyond an audit, **publishers and advertisers alike need to focus on the ongoing management of tag needs.** Actively monitoring and controlling tags is the only way to ensure compliance with a consumer-centric approach to data and privacy. Businesses should consider a universal container tag management system to monitor, install, and disable tags centrally as needed for the organization's Web and media teams.

## IMPLEMENT OBA COMPLIANCE

In addition to defining self-regulatory practices and procedures, the DAA developed a **scalable, consistent way for companies to track and demonstrate compliance.** To fulfill compliance requirements, marketers will need to provide the following to consumers on all campaigns and owned websites where OBA is being gathered or used:

- Clear notification of when a user is being served an ad that is behaviorally targeted to them and the option to learn more about OBA.
- Clear notification of when a user is being tracked on a web page for subsequent ad targeting (e.g., pages on which data is collected for later retargeting)
- A way to control and opt-out of future behaviorally targeted ads.



The DAA has certified a few technology providers, such as Evidon (formerly Better Advertising Project), DoubleVerify, and TRUSTe, to offer a turnkey solution for implementing OBA compliance. All these solutions utilize the "Advertising Option Icon." This icon is integrated into the advertising creative and serves to notify the consumer that the ad they are being

served is behaviorally targeted to them. On websites, the icon is integrated into the footer of any pages collecting behavioral data and serves a similar purpose of notice in the ad.

Media Contacts has tested a number of these solutions for clients; below is a top-line summary of what these firms offer.



DAA Approved Vendor	Yes	Yes	Yes
Ad Choice Icon, Interstitial, Proof of Compliance	Yes	Yes	Yes
Implementation	Pixel placed within creative by agency	Pixel placed within creative by agency	Pixel placed within creative by agency
Reporting: AdChoice Icon, Impressions, Clicks, CTR	Yes	Yes	Yes
Reporting: Opt-Out Rate	No	Yes	Yes
Currently Working to Top Agencies	Yes	Yes	Yes
Chosen Platform for DAA Monitoring System	No	Yes	No

These solutions provide disclosure through an ad interstitial that educates users about OBA, and provide an opt-out of behavioral targeting. The icon and interstitial approach should also be used within a brand's website where data is collected for behavioral advertising such as retargeting. The solutions also provide proof of compliance for the advertiser.

It should be noted that in addition to offering compliance monitoring to advertisers, Evidon is also the sole provider of the DAA's monitoring system, which is overseen by the DMA and the BBB. This system –which is separate from the platform enabling the icon in ads– is helping the DAA track companies' compliance with the self-regulatory program. This accountability program monitors the marketplace externally for data that suggests non-compliance and reviews consumer and competitive reports of non-compliance. While the objective is to see all companies participating in the program, the accountability mechanisms can refer uncorrected non-compliance to the FTC.

As marketers assess their options with regards to factors such as a provider's technical approach, implementation requirements, and publisher adoption need to be taken into account before selecting the appropriate solution.

Currently advertisers are bearing the cost of such a service, which is generally below a \$.05 Cost Per Thousand (CPM). The programs described above focus at the point of when a user is served an OBA ad through methods or data utilized by a third party. These providers also offer solutions to address compliance for first-party or site-side situations –at those points where a user’s information is being captured and leveraged on an advertiser’s website. Though there is a cost for these services, they provide a solution for advertisers to take control of the issue and become compliant with the self-regulatory guidelines. Many advertisers are considering these types of solutions campaign-wide (with or without OBA) to demonstrate complete transparency as to when data are and are not being used. Because of the additional cost many marketers will only deploy these solutions for the OBA portions of their campaigns.

**Some online publishers are also taking a proactive stance**, implementing their own icons to manage first-party cookies, data collection and OBA within their sites/network. Yahoo! and MSN include an “Ad Choices” icon, to provide consumers with similar information and choices as the third party served icons. Google offers the same on its display network and now offers the ability for consumers to agree or disagree with the relevancy of a result within its search result pages, Facebook also offers the ability for consumers to rate ads and provide feedback. These efforts take consumer control a step further and underscore the industry’s need to provide choice and transparency.

The screenshot shows a browser window with the Yahoo! Privacy page. At the top, there are navigation links for 'New User? Register', 'Sign In', and 'Help'. A search bar is present with the text 'Trending: Tyson tattoo' and a 'Web Search' button. Below the search bar is a large blue 'AdChoices' icon. The main content is divided into two sections: 'FOR CONSUMERS' and 'FOR ADVERTISERS AND PUBLISHERS'. The 'FOR CONSUMERS' section includes text about how ads are targeted and provides links for 'Who placed this ad?', 'Where can I learn more about how Yahoo! selects ads?', and 'What choices do I have about interest-based advertising from Yahoo!?'. The 'FOR ADVERTISERS AND PUBLISHERS' section includes text about Yahoo!'s advertising solutions and provides links for 'Yahoo! Advertising Solutions' and 'Yahoo! Publisher Network'. A footer contains copyright information: 'Copyright © 2010 Yahoo! Inc. All Rights Reserved. Privacy | Legal'.

## COMPLIANCE MONITORING

---

Beyond implementing proactive and compliant solutions for consumer transparency, advertisers should also **assess the relationship they have with publishers**. Having open lines of communication with sites, properties, and aggregators can help limit under-delivery, billing and reporting discrepancies, and other inventory management issues that may arise as they take steps to establish compliance monitoring.

## TAKING ACTION

---

The self-regulatory program impacts companies that use or gather third party online behavioral advertising. This can include advertisers, networks, site owners, data aggregators, and others. To demonstrate compliance with the industry's **Self Regulatory Program for Online Behavioral Advertising**, companies can take the following steps:

### AGENCIES

1. Create an agency point-of-view that summarizes its self-regulatory program, how advertisers can comply, as well as the strengths and an analysis of the available compliance providers.
2. Evaluate how clients are using online behavioral advertising in media buys, as well as what clients are utilizing retargeting tactics. Behavioral media buys will require notice in the ad, while retargeting will require notice on the site.
3. Be proactive about discussing the issue with clients; create a compliance plan and timeline.
4. Ensure all network and data partners are participating in the self-regulatory program.

### ADVERTISERS

1. Obtain a license for the Advertising Option Icon on the DAA website, [www.aboutads.info](http://www.aboutads.info)
2. Ensure the icon and notice are displayed on all of your ads that collect or use third party online behavioral data and allow consumers to opt-out of data use by these third party providers.

3. Review data collection on your own site, particularly data collection for retargeting campaigns, which are considered third party OBA and, therefore, require site-based notice and choice.
4. Review your company's privacy policy to make sure it includes accurate information on your use and collection of online data.
5. Provide reporting to demonstrate compliance with the *Self Regulatory Program for Online Behavioral Advertising* program developed by the DAA.

## NETWORKS, TRADING DESKS AND DEMAND-SIDE PLATFORMS

1. Obtain a license for the Advertising Option Icon on the DAA website at [www.aboutads.info](http://www.aboutads.info)
2. If your network has its own cookie space, register for the opt-out page on the DAA website at <http://www.aboutads.info/choices/>
3. Ensure the icon and notice are displayed on all ads served that collect or use third party online behavioral data (regardless of whether or not you host the creative).
4. Allow consumers to opt-out of data collection and use for OBA from the companies providing the third party behavioral data.
5. If you are collecting OBA data from publisher sites on behalf of advertising clients or for your own downstream use and cannot attach notice to an ad event on that page, ensure that each of these sites are providing site-based notice.
6. Review your company's privacy policy to make sure it includes accurate information on your use and collection of online data.
7. Provide reporting to demonstrate compliance with the *Self Regulatory Program for Online Behavioral Advertising* program developed by the DAA.

## WEB SITE OWNERS

1. If any third parties collect data for later OBA use or use OBA data on your site without delivering their own notice, obtain a license for the icon on the DAA website at [www.aboutads.info](http://www.aboutads.info)  
  
[Note that retargeting campaigns, involving first party collection of data on your site for use in third party retargeted advertisements (ads on other sites), are considered OBA and therefore require this notice.]
2. Ensure the icon and notice are displayed on all pages of your site on which OBA collection or use can occur.

3. Allow consumers to opt-out of data collection and use for OBA from your site.
4. Review your company's privacy policy to make sure it includes accurate information on your use and collection of online data.
5. Ensure the icon and notice are displayed on OBA ads that you deliver as an advertiser on third party sites, including all retargeted ads.
6. Provide reporting to demonstrate compliance with the *Self Regulatory Program for Online Behavioral Advertising* program developed by the DAA.

## THE LONGER TERM VIEW

---

The short-term recommendations above focus on helping businesses get ahead of compliance with the industry's self-regulatory principles for OBA. However, the FTC's guidelines are broader-reaching and will have a greater impact on a company's use and disclosure of audience data. As such, Media Contacts recommends **a proactive approach to the FTC measures**. There are a number of other open issues particularly around execution and how to maintain compliance. In the long term, the following approaches should be considered to address the increased scrutiny in this area for now and moving forward.

---

### STRENGTHEN ALIGNMENT BETWEEN MARKETING, TECHNOLOGY AND LEGAL COUNSEL

---

Privacy issues and related compliance are not strictly the sole responsibility of a company's marketing or media department. Though roles and groups may be siloed within an organization, functional experts across marketing, media, web management, information technology, and legal need to work in concert to understand and address the issues and needs facing the organization. This thinking also applies to social media and will only increase in importance as social media grows and changes the relationship between brands and consumers.

Though the recent focus on privacy has arisen from web-based activities, it is not necessarily an issue restricted to digital. Given the reach of the FTC's principles, these topics will also impact any offline function where information about a consumer is collected and need to be managed accordingly.

---

### KNOWING AND MONITORING ALL POLICIES AND PROCESSES AROUND CONSUMER DATA

---

Understand the policies, processes and practices of vendors who will be collecting data from consumers on the brand's behalf including ad networks, site analytics, retargeting solutions, etc. As a rule, the data practices of anyone who is allowed to pixel the client website need to be strictly evaluated. Businesses should also understand internal data retention policies (for both itself and its agencies) for all consumer data collected and stored.

---

## TAKING CONTROL OF YOUR CONSUMER RELATIONSHIPS

---

Many commentators have noted that our industry wouldn't be in the cross hairs of legislators, regulators, and the press if we had taken the conversation directly to the consumer years ago. Your company, as a brand, is leveraging data about the consumer for marketing. The consumer wants to know how that process works, what the boundaries are, and how this benefits them. All of the data suggests that when you communicate this in simple and clear terms, and offer control mechanisms, their trust in your brand actually increases. Think more broadly about ways that you extend this dialogue beyond a compliance exercise, into a more strategic set of tools that you can develop to build more trusting relationships with consumers, across platforms, devices, etc., going forward.

Additionally, companies like DoubleVerify and AdSafe offer delivery verification. Delivery verification ensures media buying guidelines are adhered to. This is particularly important to pharmaceutical and financial advertisers who operate under strict regulatory rules, as well as sites with a regional/local focus as they can better reduce waste outside of the target region. Media Contacts recommends the use of both front-end consumer transparency solutions as well as back-end verification services

## CONCLUSION

---

**Media Contacts** fully supports the industry's efforts to improve consumer protection and privacy.

At a minimum, we believe that **all advertisers should adopt the DAA's "Self-Regulatory Principles for Online Behavioral Advertising"** as well as live by the **Web Analytics Association's "Code of Ethics"**. This includes implementing OBA compliance through third-party solutions for owned and operated websites and existing digital media planning and buying as well as bidded media and ad exchanges. This should also extend to multi-device advertising and mobile. It is critical whether its web-based and cookie-derived or a mobile effort with device targeting to offer the same consumer transparency and ad delivery control.

Media Contacts believes full implementation of consumer protection needs to be **an industry-wide initiative**, not just the responsibility of advertisers. Collectively, we need to put greater emphasis on educating the public on privacy issues. Two-thirds of consumers say they would prevent advertisers from showing them ads based on websites they have visited. However, consumers need to be educated on how this would impact their web experience. The campaign the IAB ran in 2010 that focused on privacy concerns is a great first step and needs to be expanded upon by other leadership groups in the industry to create continued focus on consumer understanding and education.

The current self-regulatory practices focus on enabling a user to opt-out of seeing a targeted ad. In most cases, though the ad is not served, the collection of the data itself is still being allowed. The difference between opting-out of seeing a targeted ad vs. opting-out of being tracked is subtle, but important.

Unresolved issues like this, and countless others, will continue to elevate the focus on privacy throughout the government and will stoke society's fears that one's personal data are available to anyone who wants it. The former is exhibited by the fact that FTC's guidelines are further reaching than what the industry put forth through the DAA, and that there are a number of broader issues around consumer protection that will need to be addressed.

As an industry, we want to avoid heavy regulations. Being **proactive and transparent** in our approach and far reaching in execution as well as having an enhanced ability to control whether ads are delivered according to guidelines is the only path to harmonization between business success and the empowerment of the consumer now and in the future.



## GLOSSARY

---

### **Aboutads.com**

Leading marketing and advertising industry associations have joined to create a one-stop website, 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.

### **Ad delivery**

Ad delivery is the delivery of online advertisements or advertising-related services using ad-reporting data. Ad delivery does not include the collection and use of ad reporting data when such data are used to deliver advertisements to a computer or device based on the preferences or interests inferred from information collected over time and across non-affiliate sites because this type of collection and use is covered by the definition of online behavioral advertising.

### **Ad reporting**

Ad reporting is the logging of page views on a website(s), or the collection or use of other information about a browser, operating system, domain name, date, and time of the viewing of the Web page or advertisement, and related information for purposes including but not limited to:

- Statistical reporting in connection with the activity on a website(s);
- Web analytics and analysis; and
- Logging the number and type of advertisements served on a particular website(s).

### **Affiliate**

An affiliate is an entity that controls, is controlled by, or is under common control with, another entity.

### **Behavioral targeting**

A technique used by online publishers and advertisers to increase the effectiveness of their campaigns. Behavioral targeting uses information collected on an individual's Web browsing behavior to select which advertisements to display to that individual. Practitioners believe this helps them deliver their online advertisements to the users who are most likely to be interested. Behavioral targeting allows site owners or ad networks to display content more relevant to the interests of the individual viewing the page. On the theory

that properly targeted ads will fetch more consumer interest, the seller may ask for a premium for these over random advertising or ads based on the context of a site.

### **Consent**

Consent means an individual's action in response to a clear, meaningful, and prominent notice regarding the collection and use of data for online behavioral advertising purposes.

### **Control**

Control of an entity means that one entity 1) is under significant common ownership or operational control of the other entity; or 2) has the power to exercise a controlling influence over the management or policies of the other entity. In addition, for an entity to be under the control of another entity and, thus, be treated as a first party under these principles, the entity must adhere to online behavioral advertising policies that are not materially inconsistent with the other entity's policies.

### **COPPA**

Children's Online Privacy Protection Act of 1998. The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13. While children under 13 can legally give out personal information with their parents' permission, many websites altogether disallow underage children from using their services due to the amount of paperwork involved.

### **First party**

A first party is the entity that is the owner of the website or has control over the website with which the consumer interacts and its affiliates.

### **Frequency capping**

Frequency capping means restricting (capping) the amount of times (frequency) a specific visitor to a website is shown a particular advertisement. This restriction is applied to all websites that serve ads from the same advertising network.

### **Online behavioral advertising**

Online behavioral advertising means the collection of data from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate websites 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. Online behavioral advertising does not include the activities of first parties, ad delivery or ad reporting, 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).

**Personally identifiable information (PII)**

Personally identifiable information is information about a specific individual including name, address, telephone number, and email address, which can be tracked to a particular individual.

**Retargeting**

Behavioral retargeting (also known as behavioral remarketing, or simply, retargeting) is a form of online-targeted advertising by which online advertising is delivered to consumers based on previous Internet actions that did not in the past result in a conversion or the action intended by the site owner, which typically involves making a purchase.

**Service Provider**

An entity is a service provider to the extent that it collects and uses data from all or substantially all URLs traversed by a Web browser across websites for online behavioral advertising 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.

**Third party**

An entity is a third party to the extent that it engages in online behavioral advertising on a non-affiliate's website.

## SOURCES

---

***FTC Fair Information Practice***

Wikipedia.org, as of December 19, 2010

***FTC Industry Association Guidelines***

<http://www.ftc.gov/reports/privacy3/industry.shtm#Industry%20Association%20Guidelines%20A>

***Protecting Personal Information: A Guide for Business***

<http://www.ftc.gov/infosecurity/>

***Self-Regulatory Principles for Online Behavioral Advertising***

Developed by the American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, the Direct Marketing Association and the Interactive Advertising Bureau, July 2009

***A Call for a Federal Office to Guide Online Privacy***

by Tanzina Vega, The New York Times, December 16, 2010

***United States: FTC Proposed Framework for Protecting Consumer Privacy***

by Mary Innis and Joan L. Long, Mondaq, December 8, 2010

***FTC Staff Issues Privacy Report***

News wire released by Federal Trade Commission, December 1, 2010

***Audience Ad Targeting: Data and Privacy Issues***

eMarketer, February 2010

Interviews with individuals at TruEffect, Evidon, Double Verify and TRUSTe

## CONTACT DETAILS

---

We encourage you to contact us directly to discuss, in more details, any concerns you may have regarding this Media Contacts Insight issue. **We will be happy to assist you.**

- [adam.kasper@havasdigital.com](mailto:adam.kasper@havasdigital.com)
- [tom.penque@havasdigital.com](mailto:tom.penque@havasdigital.com)
- [andrew.altersohn@havasdigital.com](mailto:andrew.altersohn@havasdigital.com)
- [mark.egan@havasdigital.com](mailto:mark.egan@havasdigital.com)
- [mmokri@evidon.com](mailto:mmokri@evidon.com)

Or contact your **Media Contacts local office:**

### MEDIA CONTACTS USA

**ADDRESS 1** 101 Huntington Avenue,  
16th Floor. Boston MA 02199 USA.

**OFFICE PHONE** +1 617 425 4100

**FAX** +1 617 425 4101

**CONTACT** Tom Penque

**EMAIL** [tom.penque@mediacontacts.com](mailto:tom.penque@mediacontacts.com)

**ADDRESS 2** 195 Broadway, 12th Floor.  
New York, NY 10007.

**OFFICE PHONE** +1 646 587 5000

**FAX** +1 646 587 5005

**CONTACT** Andrea Millet

**EMAIL** [andrea.millet@mediacontacts.com](mailto:andrea.millet@mediacontacts.com)

**ADDRESS 3** 5301 Blue Lagoon Drive,  
Suite 850, Miami, FL 33126.

**OFFICE PHONE** +1 305 377 1907

**FAX** +1 305 377 1906

**CONTACT** Fernando Monedero

**EMAIL** [fernando.monedero@mediacontacts.com](mailto:fernando.monedero@mediacontacts.com)

**ADDRESS 4** 36 East Grand, 5th Floor.  
Chicago, IL 60611.

**OFFICE PHONE** +1 312 337 4400

**FAX** +1 312 337 3898

**CONTACT** Chris Costello

**EMAIL** [chris.costello@mediacontacts.com](mailto:chris.costello@mediacontacts.com)

media   
contacts

**HAVAS**  
**HAVAS**  
DIGITAL

[www.havasdigital.com](http://www.havasdigital.com)