



**Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580**

**COMMENTS
OF THE
INTERACTIVE ADVERTISING BUREAU
ON
ONLINE BEHAVIORAL ADVERTISING
PROPOSED PRINCIPLES**

Randall Rothenberg
President & CEO
Interactive Advertising Bureau
116 East 27th Street 7th Floor
New York, NY 10016
212/380-4717

Mike Zaneis
Vice President, Public Policy
Interactive Advertising Bureau
575 7th Street, NW Suite E9009
Washington, D.C. 20004
202/253-1466

April 11, 2008



Introduction and Summary

The Interactive Advertising Bureau (“IAB”) is pleased to submit these comments on behalf of its members.

Founded in 1996, the IAB (www.iab.net) represents over 375 leading interactive companies that actively engage in and support the sale of interactive advertising. IAB members include Yahoo!, AOL, MSN, Google, Forbes.com, New York Times Digital, CNET Networks, and others. Collectively, our members are responsible for selling over 86% of online advertising in the United States, a \$21.7 billion dollar industry, which is expected to grow to \$50.3 billion by 2011.

On behalf of its members, the IAB is dedicated to the continuing growth of the interactive advertising marketplace, of interactive’s share of total marketing spend, and of its members’ share of total marketing spend. The IAB evaluates and recommends standards and practices, fields interactive effectiveness research, and educates marketers, agencies, and media companies, as well as the wider business community, about the value of interactive advertising.

IAB opened a Washington, D.C. office last year to oversee regulatory matters, legislative affairs, and public policy initiatives that affect the interactive advertising industry. We work with Congress and the Federal administrative agencies as they consider the important issues surrounding privacy and e-commerce. We participated in the Federal Trade Commission’s November 2007 “town hall” on online behavioral advertising, and look forward to working with the FTC as it addresses such matters.

IAB welcomes the opportunity provided by the FTC to elaborate on appropriate self-regulation of the interactive advertising industry. After summarizing the benefits of interactive advertising and discussing the current regulatory approach to such advertising, the IAB comments on the FTC’s proposed online behavioral advertising privacy principles. The following points are discussed in more detail below:

- The FTC’s proposed definition of online behavioral advertising needs greater precision.
- The IAB and its members are committed to strong consumer education and meaningful transparency, and to working with the FTC to enhance consumer awareness regarding interactive advertising. The goal of such efforts should be to help further educate consumers that data collection for online advertising is a widespread, beneficial practice and that they should assume its existence whenever they experience personalization or online advertising. Such personalization can be deployed in a way that maintains benefits for consumers, is mindful of privacy concerns, and allows consumers to set that balance consistent with the value exchange they are receiving.
- Businesses collecting or using information about individual consumers for interactive advertising purposes should provide choice, where appropriate, to these individuals. The extent of choices

will undoubtedly reflect a continuum of the value exchange, with the greatest benefits coming from the most effective, broader and, in some instances, more personalized, collection and use of data. Choice in every instance of collection or use of data will interrupt important business practices with no countervailing consumer benefit.

- The data our members collect enables businesses to better serve customers with advertisements and information more closely geared to their needs and desires. “Know your customer” is a basic tenet of business. Congress and the FTC have shown their understanding of this by choosing to regulate the sharing and/or selling of information as specified by federal statutes, but not regulating the collection of customer data. Restrictions on the collection of data would have an adverse impact on business and consumers.
- The IAB supports the principle that any company that maintains information for purposes of interactive advertising should provide reasonable security for that data.
- A self-regulatory standard calling for affirmative opt-in consent is a significant change to the regulatory landscape to date that has balanced consumer protection and the benefits to consumers of free online content.

I. The Benefits of Online Behavioral Advertising

As the FTC staff recognized in requesting comments, behavioral advertising provides consumers with significant benefits in the form of cost-free access to content and services. Interactive advertising underwrites:

- Quality online content (news, business, entertainment, maps). The majority of news publishing firms have abandoned a subscription model and moved to online advertising to provide free content to millions of readers. But the online culture of “free” often outshines the reality that sustainable free content for the user has never been—and cannot be—really free. Content and service products are costly and time consuming to create and maintain, and if not subsidized by subscriptions, require alternative monetization, the chief of which at present is advertising revenue. The centrality of this value exchange cannot be understated.
- Education and information-gathering tools, including search engines, have undoubtedly democratized the availability and accessibility of educational content. Hundreds of millions of consumers perform billions of searches through search engines annually. The largest search engines on the Internet are free to users and supported almost exclusively by advertising.
- Communications and other online services (for example, e-mail, chat and telephone services; resume services and job banks; enhanced classified services; video and photo storage and sharing) depend on advertising for their revenue. There are an estimated 1 billion users of free,

ad-supported e-mail services in the world today. There are more than 112 million blogs worldwide, providing every Internet user a free outlet to voice their opinion and create useful content for others. In November 2007, 138 million Americans (over 75% of US Internet users) watched almost 9.5 billion videos online, all for free because of advertising.

- Social networking and professional networking environments. Free social networking and online-networking sites alone had more than 86.6 million users as of December 2007. (Source Nielsen Online) The sites are ad-supported.
- Online safety tools, such as anti-spam and antivirus protection.
- Competitive pricing and product comparison tools.

Interactive advertising has benefited business too, especially small business:

- Thousands of small businesses have expanded their reach through online advertising from local to regional or national. In its testimony at the November 2007 “town hall,” IAB highlighted the experience of a former contractor, and now owner and sole operator of askthebuilder.com, who more than quadrupled his earnings in his first year of offering an advertising-supported web site.
- Businesses of all sizes have achieved more efficient marketing of goods and services through targeted online advertising.
- Online advertising has created national markets out of local or regional markets. For example, items once sold in local garage sales and pawn shops are now available nationally and internationally on eBay.

This rich, diverse, and competitive marketplace is the backdrop against which the FTC should weigh legitimate concerns about the collection of information about users of the Internet for use in online behavioral advertising.

II. The Benefits of the Current Regulatory Approach to Online Behavioral Advertising

Some criticism leveled at interactive advertising is based upon the misconception that this is an area free of all regulation. Yet, interactive advertising is subject to both self-regulation and government regulation.

For IAB and its members, self-regulation that is responsive to consumer needs and protection makes business sense: it helps instill consumer confidence and improve business practices. That is why, notwithstanding the additional risk of liability shouldered by posting privacy notices describing practices

at web sites, American companies and their trade associations years ago took the lead in such practices, quickly outpacing their counterparts in other parts of the globe. Among the successful examples of effective self-regulation are guidelines and standards of organizations such as the Direct Marketing Association (“DMA”), the Network Advertising Initiative (“NAI”), TRUSTe, the AICPA’s WebTrust, and BBB*OnLine*. These organizations and programs, among others, have many years of experience in developing best practices and standards to protect consumers’ privacy online, and their efforts offer the most flexible and effective means to do so.

The self-regulatory programs administered by the National Advertising Review Council, including its Children’s Advertising Review Unit (“CARU”), oversee the content of online advertising, and provide mechanisms for securing swift changes to potentially inappropriate advertising.

IAB also has developed guidelines that foster legitimate Internet advertising and marketing, help build trust in the medium, and ensure that online commerce can continue to thrive and grow. They include lead generation best practices, ethical e-mail guidelines, and privacy principles.

Online behavioral advertising is particularly sensitive to marketplace discipline given the medium. Just as the Internet has been a powerful tool for providing content and services, it also allows a consumer swell to deliver powerful, rapid, and blunt pushback to practices that consumers do not find valuable or acceptable. The best example of this type of highly effective “consumer regulation” comes out of the recent attention garnered by Facebook’s Beacon program. When consumers thought they were not provided ample notice or choice about their personal information, they collectively raised their voices. The result was a swift response by Facebook that swung the privacy pendulum back into equilibrium. Given that the success of the interactive advertising industry depends on consumer engagement and receptiveness (particularly as new measurement models prioritize and put a price premium on specific actions), such marketplace discipline is precise, contemporaneous, and effective. Also, this discipline is more effective than a sweeping, regulatory framework disconnected from the diversity and fluidity of the industry and any demonstration of actual harm.

Consumers have benefited and continue to benefit from the flexibility and adaptability of these self-regulatory programs, which have enabled businesses to respond to technological advances and consumer expectations far more quickly than legislative and regulatory bodies.

Behavioral marketing has effectively benefited consumers and businesses in the offline world for many years. Businesses have effectively used information about consumers collected offline to target consumers regarding products or services that may be of interest to them. In the online environment, these same types of practices are being used, with arguably greater privacy protections, given that the data is collected, stored, and used anonymously. The Commission has not articulated any basis as to why the successes in offline targeting do not translate online.

In addition to robust self-regulation, the content of online advertising remains subject to federal and state advertising laws, as the FTC made clear as early as 1999 at its public workshop on “Interpretation of

Rules and Guides for Electronic Media.” Online advertisers are subject to the same laws regarding, for example, substantiation and promotions, as advertisers in other media.

Similarly, data collection practices associated with interactive advertising are subject to federal privacy laws such as the Children’s Online Privacy Protection Act (“COPPA”), the HIPAA Privacy Rule, and the Gramm-Leach-Bliley (“GLB”) Privacy Rule, as well as Section 5 of the FTC Act and state prohibitions against unfair and deceptive practices (“UDP”). One reason why the federal and state UDP laws are effective is the widespread posting of privacy notices and disclosures of web site data collection and use practices.

Further, enforcement mechanisms have historically played a key role in protecting consumers. For the past decade, the FTC has averaged several enforcement actions a year under section 5 of the FTC Act for deceptive privacy policies. In addition, it has brought more than a dozen enforcement actions under COPPA and GLB for deceptive privacy policies. State attorneys general have also brought enforcement actions.

Finally, a critical part of ensuring consumer protection has been education efforts by both industry and the FTC. Industry has long been engaged on this front and continues to stand ready to do its part. The IAB is a financial contributor and active participant in The Internet Safety Coalition (“ISC”). The ISC was formed in 2007 to address the issues surrounding Internet safety for children and teens with a unified, research-based communication strategy. We are working to develop research-based messages that most effectively resonate with kids, teens and parents around various online safety concerns. Similarly, industry programs can be bolstered by FTC engagement in education efforts similar to those currently being undertaken in the areas of identity theft, online security and online safety. Industry looks forwarding to hearing more about ways we can partner with the FTC in the area of consumer education.

Given these protections and measures, IAB questions how imposing additional specific regulatory standards upon interactive advertising would benefit consumers. This is a particularly pressing concern given that absence of demonstrated harm. As such, IAB continues to believe that the existing framework and protective measures should continue to be the means for protecting consumers in the interactive marketplace.

III. The FTC’s Definition of “Online Behavioral Advertising” Needs Greater Precision

The FTC has indicated that the proposed guidelines are a continuation of its efforts in the “online profiling” arena that took place in 2000. At that time, online profiling was described as “data collected over time and across Web pages to determine or predict consumer characteristics or preferences for use in ad delivery on the Web.” The FTC has now proposed a new term—behavioral advertising—to address its concerns, with an accompanying new definition, yet has not explained why there is any need to change the terms and definitions. The basics of cookie-based interactive advertising have not

changed much since 2000. The FTC should explain why it has changed its terminology, and the significance of that change.

If there is a reason for the change, the FTC should also better link the changes to the consumer harms, if any, about which it is concerned. For example, what harms, if any, are tied to the mere collection of data for interactive advertising? IAB knows of none, and would benefit from greater insight into the FTC's thinking. Does the FTC's concern lie truly with the stewardship of the data once collected? In other words, after data has been collected, what harms, if any, are tied to unauthorized access to data stored for interactive advertising? This type of precision will better inform the policy debate that the FTC is seeking to promote.

As noted, the FTC has adopted online behavioral advertising as the term it wishes to use, and has defined the term to mean:

[T]he tracking of a consumer's activities online—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.

This definition, as discussed below, misses the mark.

At the outset, the FTC's definition focuses on early steps of the process that result in online advertising, rather than on the consumer experience or outcome of the process. The FTC has never before defined television or other forms of offline advertising or marketing in that manner, and it should not start now. It has not, for example, defined offline advertising or marketing by focusing on market surveys, consumer questionnaires, or secret shopper programs.

Rather, the FTC's definition of online behavioral advertising should describe the outcome of the interactive advertising process. As one participant at the FTC's town hall noted, the outcome is the display of advertising based on insights derived from past consumer activity.

The goal of online advertising is to display advertising that is relevant to the consumer. A consumer's past activity is used to make inferences regarding the types of advertisements in which the user may be interested. Visiting automobile manufacturer web sites, for example, may suggest that a consumer is contemplating purchasing a car; the inference that the user may have a propensity to purchase a car would result in the user being served banner advertisements for cars when the user visits their daily newspaper's web site. The consumer's past activity (visiting car web sites) is used to make inferences (the consumer is probably shopping for a car) regarding the type of advertisements in which the user may be interested (banner ads about cars). If the inferences are accurate, the advertising that is displayed as the user visits web sites unrelated to cars is very relevant to the consumer. Also, this process reinforces a scenario where the consumer remains in control, *i.e.*, if the user does not wish to buy a car, the user has no obligation to click on an advertisement. Similarly, with the shared motivation

to “get it right,” it does not serve companies well to infer wrongly that the user is in the market for a car, potentially irritating or offending them and possibly losing a more successful marketing opportunity, for example, if the user was scanning auto web sites to determine the best way to reduce their carbon footprint while still commuting to work, and ultimately is an environmentalist who prefers a bicycle purchase.

Second, as a result of the misdirected focus, the FTC’s definition also lacks this notion of inferences—use of behavioral data to derive inferences regarding personal characteristics to predict the advertisements in which consumers may be interested. This should be included in the definition. Otherwise, the FTC’s definition can sweep in online advertising that is simply contextual in nature and not predicated upon inferences drawn from online behavior. For example, advertising regarding vacation packages to a major tennis tournament in New York delivered to all individuals who visit a tennis web site is based on the content or context of the site visited, not on the behavior of the individuals visiting the tennis web site. Online advertising that is not based upon online behavior should fall outside the definition of online behavioral advertising.

Third, specific inclusion of “searches” in the description of the early steps of the process that result in online advertising is too broad for several reasons. Web sites use search queries for multiple purposes. They sometimes use searches to collect data for behavioral advertising, but often they do not. For example, a search on the FTC’s web site will yield one or more documents without advertising. Similarly, a search on the free encyclopedia Wikipedia will yield one or more entries without advertising. Even when advertising is delivered on a resulting search page, that advertising is not necessarily tied to the query itself. For example, searching within a news site for the term “tennis” may direct the user to a story about a recent tennis tournament. It is possible however, that the tennis-related advertising on that page is simply contextually based and not tied to the original search term. So, to the extent that the definition suggests that all search functions result in behavioral advertising, it is incorrect.

In addition, use of search queries for online advertising cannot fairly be characterized as “tracking activities that are completely invisible”—the type of data collection that is the focus of the FTC’s recommendations. Consumers know precisely what queries they have entered and can immediately see the similarity and link between the advertising that is displayed to them and the content they are viewing.

Moreover, when searches result in behavioral advertising, it is based on “the content viewed” by a consumer—an activity already covered by a different part of the FTC’s definition, rendering unnecessary the specific and potentially misleading reference to “searches.”

Finally, the definition should not apply to information collected at and used within an individual site, affiliated sites, or sites under common control or ownership. Such sites may collect the information to provide added value or functionality to users of the site, such as displaying the movies they most recently rented or books they most recently browsed. This is particularly the case because the type of information collected and used for advertising within an individual web site is not an area where the

record indicates any harm or consumer concern. Consumers are aware of, and significantly benefit from, use of information from within a web site or affiliated web sites. Such information is not the type of “invisible tracking” where consumers are unaware of the entity that is collecting the information. There are many retailers and financial institutions, for example, that provide personalized web sites, or deliver products and services when consumers return to a web site based on the consumer’s prior interaction with the business. This concept was recognized in the privacy provisions of the Gramm-Leach-Bliley Act that allow transfer of financial information to affiliates with notice of such transfer. Individuals know the identity of the web operator with whom they are interacting and, due to existing self-regulatory guidelines, the site’s data practices, including those related to the collection and use of personally identifiable information. These practices simply cannot fairly be characterized as “invisible tracking activities.”

IV. Comments Regarding Specific FTC Principles

A. Principle Regarding Transparency and Consumer Control

1. General

The IAB and its members are committed to strong consumer education and meaningful transparency, and look forward to exploring ways to partner with the FTC to enhance consumer awareness of information collection practices in connection with interactive advertising.

Nevertheless, we disagree with the notion that current transparency and disclosures are fundamentally flawed, requiring a seismic shift in regulatory approach such as mandatory choice in all instances of data collection for online advertising. Certainly, the industry recognizes the need for, and is committed to, continued improvement, particularly through new and innovative ways of providing transparency and choice. But these efforts should be built on, and also further, the existing well-considered, effective self-regulatory practices as their base. Providing room for differentiation in these enhancements also allows entities to showcase to business partners and consumers their ability to strike an effective balance, thereby reinforcing the role of competitive marketplace discipline.

First, the fact is that data collection for online advertising is a widespread practice. As discussed above, cost-free content, personalization, and many other benefits of the Internet are achieved only through online advertising. Industry, the FTC, consumer groups, and others should help further educate consumers so that, when they experience personalization or online advertising, they assume that collection of data is taking place and that they can seek out further information on those practices, in the same way that consumers have been educated to know where to seek privacy policies on web sites. That should be the starting point.

Second, the consumer control proposed by the FTC is a significant departure from past consumer choice programs enacted by Congress and overseen by the FTC. The FTC’s proposed guidelines state that

every web site where data is collected for behavioral advertising should provide consumers with a choice whether or not to have their information collected for such purpose. As such, the FTC proposes a choice principle that focuses on collection of data rather than use or disclosure of the data. The principle's breadth is sweeping.

For example, the FTC oversees consumer choice programs in connection with the Fair Credit Reporting Act and GLB, which involve financial and other sensitive personal information. In both cases, the consumer has the legal right to choose whether the personal information may be disclosed to third parties; the consumer does not have the option of blocking the collection of the personal information, other than reaching the decision not to engage with the collecting entity in the first instance. This cost-benefit decision-making should not be obliterated in this context any more than it is elsewhere. At a certain level, engagement in the benefits of products and services at a particular web site necessitates the exchange of some initial amount of information to provide those benefits, in the same way a bank will set its own unique, minimum information collection (albeit more personal information than interactive advertising), to offer services. If consumers deem that initial level of information collection out of sync with those benefits, they can decline to participate or engage further with the site, and use all of the tools embedded in the browser to control those information preferences.

Moreover, the FTC's choice principle would have web sites strike a different bargain than they do now. In effect, the FTC proposes that web sites continue providing content and services to consumers at no cost while providing them directly with the option of blocking the collection of data—in essence, the monetization and underwriting—necessary to continue providing the content and services. This would be a consumer choice program unlike any other enforced by the FTC.

To adhere more closely to the consumer choice programs enacted by Congress and overseen by the FTC, this principle, at most, should call for consumers, in certain instances, to be provided with a choice whether or not to have their information *used* for online advertising.

2. Increased transparency but a lesser need for greater control

IAB believes that companies should use multiple strategies and techniques to further increase and enhance consumer education and awareness of information collection practices in connection with interactive advertising. It benefits both consumers and the industry to expand transparency and consumer education, so that consumers' knowledge and decisions are based on accurate, rather than hyperbolic, representations of what is occurring. Such education also encourages acceptance and online engagement, and ultimately leads to successful results for consumers, advertisers, and the companies serving them.

To elaborate further on the issue of transparency, IAB believes that, in the online environment, consumers visiting a particular web site should be provided meaningful notice of the *types* of individual information collected for interactive advertising purposes, the technologies employed to collect such information, and how such information is used, including that other companies operate on the site and

may collect such information. We are exploring ways in which standardizing descriptions regarding these practices in web site privacy notices can help improve transparency. But due to potential liability for material omissions, there currently are no incentives for shorter notices. We are also concerned that the FTC may be placing too great an emphasis on data collection and usage practices currently explained in privacy policies and ignoring the other important information supplied via this near ubiquitous resource. Privacy policies often provide important information regarding a web site's business operations and relationships with other parties.

Businesses collecting or using information about individual consumers for interactive advertising purposes should also provide choice, where appropriate, to these individuals. However, choice in every instance of collection or use of data will interrupt efficiencies upon which consumers have come to rely with no countervailing benefit. With the starting point being the assumption by consumers that data collection is occurring whenever they experience personalization or online advertising, and meaningful transparency regarding these practices, the situations that call for additional consumer choice narrow substantially. This further allows business practices and standards to focus on the areas where choice can meaningfully distinguish between consumers who are willing to exchange information essential for participation in the basic essence of a web site, but no further, and consumers who are willing to go further for optional, more enhanced capabilities and benefits. Such customer differentiation occurs regularly in other industries, and online advertising should be no different.

As a practical matter, there are more entities operating at a web site than just the publisher. Data is also collected at web sites by advertisers, network advertisers, and web analytics providers, as well as by the publisher. Much of this data is not personally identifiable information, in large part reflecting the marketplace reality that in many cases aggregated, categorized, or anonymized data can be far more beneficial, instructive, and manageable given the vast sums of data traffic occurring every nanosecond on the Internet. There has been no demonstrated need or benefit, or avoided harm, for providing consumers with choices to the collection or use of this data.

Personally identifiable information is different. This tenet has long been a turning point in the evaluation of data practices. Most existing self-regulatory models already call for providing consumers with choice regarding the transfer of personally identifiable information about them to third parties for use for third-party marketing.

IAB believes that consumers should be given information about the choices they have concerning the collection and use of individual information for interactive advertising purposes. Consumers also should receive relevant education regarding cross-industry opportunities to opt out of the collection or use of individual information or other methods to exercise choice. One area for increased public education, for example, is the choices and controls that consumers have available by virtue of their web browsers. Every Internet user already has a robust opt out tool at their disposal as they are able to block cookies before they are downloaded onto their computer. Moreover, web browser filters allow the user to choose their desired level of blocking, whereby they can block all cookies, just third-party cookies, or be notified every time before a cookie is placed and then make a case-by-case decision. Existing consumer

controls located in the browser are particularly effective in this arena. One recent study showed that as many as 42% of Internet users cleaned out their cookies weekly. This type of tool along with tools that will be developed in the future provide the best means of consumer control over the totality of their Internet experience. Others are options like those provided via the NAI to opt out of ad network activity. As companies and industries develop further tools, such as those to preserve opt-out preferences while deleting cookies, those options will also become a part of education campaigns.

Improved transparency and control should not, however, interfere with agreements reached between companies and consumers in EULAs and other forms of contracts.

B. Principles Regarding Reasonable Security and Limited Data Retention

The IAB generally supports the FTC’s restatement of the law regarding data security practices because we believe that any company that maintains information for purposes of interactive advertising should provide reasonable security for that data.

We note that it would be unprecedented, and difficult to justify, to treat non-personally identifiable information in the same manner as personally identifiable information. Virtually every privacy and security regime in the United States treats anonymous, pseudonymous, aggregate, and other types of information that might be capable of identifying an individual, but does not do so, differently from personally identifiable information. For example, in *Klimas v. Comcast Cable Communications*, 465 F.3d 271 (6th Cir. 2006), a federal appellate court recently had the opportunity to review this issue in the context of the treatment of IP addresses under the privacy provisions of the Cable Act. In dismissing the suit’s claim that Comcast had unlawfully collected data about the web surfing activity of its subscribers, the court of appeals held that IP addresses and web surfing information that a cable operator had not correlated to individual subscribers’ names, but had the capability to do so, “standing alone,” did not qualify as “personally identifiable information” protected by the Act. *Id.* at 280; *see also id.* at 276 n. 2. While interactive advertising remains mostly cookie-based, this authoritative court case involving IP addresses underscores the principle that *potentially* identifiable information is legally distinct from *identifying* information.

This is not to say that industry does not support appropriate handling of non-PII. But rather, the governing principle incorporates the notion that the sensitivity of the data is a factor in determining the extent, level and reasonableness of the safeguards. This sliding scale should refer to the sensitivity of the personally identifiable information being protected, such as marketing data traceable to an individual; it should *not* suggest that the same level of safeguards are needed to protect non-personally identifiable information.

Finally, it is unclear why the FTC’s principle needs to separate out data retention. As indicated by the FTC in footnote 8 of its accompanying commentary, data retention and destruction is part of a reasonable data security program for personally identifiable information. Furthermore, data security programs balance data retention and destruction considerations, and the need for retaining data

associated with online advertising extends beyond those listed by the FTC. For example, data may also be retained to satisfy auditing and Sarbanes-Oxley financial controls, contract monitoring, to detect and combat click fraud, and the new federal electronic rules of discovery, most of which are purposes that extend beyond the FTC's jurisdiction and experience.

C. Principle Regarding Affirmative Express Consent for Material Changes

This principle focuses upon a particular situation that calls for additional consumer choice, and transparency about that situation and the available choice. As such, it should be consolidated with the transparency and consumer control principle.

When placed in the context of calls for greater transparency, this principle has the potential for undermining interactive advertising by overly restricting business practices in a changing marketplace. It also could potentially run counter to the goals of the FTC and the industry to ensure transparency and appropriate choice. If businesses at the time of data collection make the types of detailed promises that the FTC appears to be calling for, they face three choices if they later wish to materially modify those practices: dispose of all of the data and start the data collection practices and inference process again, obtain affirmative opt-in consent, or design in the first instance notice and choice materials that are broader, and less educational or useful. It would not take long for businesses to realize that they would be better off not “locking” themselves into detailed descriptions of their practices.

There is a symbiotic relationship between the transparency and choice principles. Under the FTC's proposal, the more specific a company is about its practices, the harder it is to change them. A balance must be struck between specificity in transparency, on the one hand, and flexibility in responding to a changing marketplace on the other. Both principles cannot be so stringent as to “lock” the marketplace into a set of practices at a particular point in time.

Moreover, we believe that, to the extent it is intended to be a restatement of existing law, the principle is overbroad. The Director of the Bureau of Consumer Protection characterized the conduct at issue in *In re Gateway Learning*, cited by the staff at footnote 9, as “particularly egregious . . . in terms of the kind of information that was shared”—age ranges and gender of children—“and the explicit promises that were made [in the original privacy policy] not to share *that* information in the first place.” The remedy in the consent order fashioned to respond to this “egregious” conduct prohibits the company from sharing this sensitive personal information collected under its pre-2003 privacy policy without first obtaining the opt-in consent of consumers whose information it had collected under those specific promises.

But the remedy upon which the FTC staff relies in proposing opt-in consent in Principle 3 is one contained elsewhere in the *Gateway Learning* consent order. That separate remedy in *Gateway Learning* was in the nature of “fencing in” relief—a provision in a final FTC order that is broader than the conduct that is declared unlawful. *Telebrands Corp. v. FTC*, 457 F.3d 354, 357 n.5 (4th Cir. 2006). It is designed to prevent a company from using different means that could lead to the same ends.

Fencing-in provisions often restrict business conduct that is otherwise lawful, and do not reflect a judgment by the FTC that failure to abide by the fencing-in requirements constitutes inherently or presumptively unlawful behavior. The higher standard to which the FTC held the company in *Gateway Learning* for its unlawful behavior involving children’s data is not an appropriate basis for a self-regulatory standard calling for opt-in whenever a company can use data in a manner materially different from promises the company made when it collected the data.

Finally, this principle illustrates why all of the principles should apply only to personally identifiable information. To the extent that a duty arises to obtain affirmative consent, it can only be executed with regard to personally identifiable information. How otherwise would a company be able or expected to communicate with a consumer and obtain the consumer’s affirmative consent? This practical limitation underscores the need for the FTC’s principles to apply only to personally identifiable information used in connection with online behavioral advertising.

D. Principle Regarding Affirmative Express Consent for Use of Sensitive Data

As noted above, IAB believes that consumers should be given information about the choices they have concerning the collection and use of information for interactive advertising purposes. This is particularly so when the information to be used is unquestionably “sensitive” and, as the FTC indicated, “can be traced back to a specific individual.” The Commission does not define “sensitive” and, for many types of information, whether it is viewed as sensitive will differ based on the information, the context in which the information is collected and used, and the view of the consumer. Given these variables, IAB believes that transparency with respect to such practices is the most effective means of empowering consumers in this area.

But some of the practices that have been used as illustrations of inappropriate online advertising either are already addressed by existing self-regulatory programs, or are the unintended consequences of existing law. For example, an online advertisement regarding nutritional supplements intended for adults displayed to users of a website directed to children may already run afoul of CARU’s guidelines on inappropriate advertisements to children. And the same advertisement displayed to children visiting a general audience site may be the result of a web site operator’s deliberate efforts not to collect personally identifiable information, which would otherwise subject it to COPPA. The fact is, knowledge that an advertisement is inappropriate for a particular viewer—a child—requires tracking the child in the first instance.

A key consideration is what data can and should be characterized as “sensitive.” As noted earlier, COPPA, the HIPAA Privacy Rule, and the GLB Privacy Rule already address uses of personally identifiable information collected online from children or by financial institutions or health care providers. But there may be other types of personally identifiable information that could be characterized as “sensitive” and merit heightened protections. For example, as underscored by the order in the *Gateway Learning* case, personally identifiable information *about* children but collected online *from* adults, is not subject to COPPA.

We are aware of discussions undertaken by the NAI regarding additional guidance on the issue of what data can and should be characterized as “sensitive” in this area. We are also aware of long-standing self-regulatory and legal treatment of “sensitive” information. This is a complicated area that merits thoughtful dialogue. IAB will remain vigilant and work with its members and other industry associations to assess existing standards and whether there is any need for additional measures for handling sensitive personally identifiable information under certain business models or practices.

E. Use of Data for Purposes Other than Behavioral Advertising

The FTC has raised the issue of the potential that data collected and stored for online advertising could be used for unrelated harmful purposes. The IAB is not aware of instances where such data has been used for harmful purposes, and agrees that it should not be used for such purposes.

But it has been a long-standing practice for companies to use collected information for multiple purposes, including within the context of online advertising, for related business matters, as well as purposes related to regulatory and law enforcement demands.

For example, many IAB members use data collected initially for online advertising for analytics, content customization, and related business purposes, which are reflected in privacy policies and other forms of notice. Some of these “secondary uses” require personally identifiable information, while others use non-personally identifiable information. None of them, however, are harmful or appear to merit additional protections. IAB may undertake further evaluation of whether there are situations in which it is reasonable to distinguish between primary and secondary uses of data for interactive advertising.

V. **Conclusion**

IAB appreciates this opportunity to comment on the FTC’s proposed online behavioral advertising privacy principles, and the important and effective role that self regulation plays in protecting consumers in the interactive advertising marketplace. IAB looks forward to working with the FTC to enhance consumer awareness regarding the practices associated with interactive advertising.