April 4, 2008

Ms. Jessica Rich
c/o Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Email Address: BehavioralMarketingPrinciples@ftc.gov

VIA OVERNIGHT AND EMAIL DELIVERY

Dear Ms. Rich:

Google would like to thank the Federal Trade Commission for hosting its "Behavioral Advertising: Tracking, Targeting, and Technology" Town Hall in November of last year. The Town Hall brought together important stakeholders from throughout industry, the consumer advocacy community, government, and Internet users to describe and discuss online advertising technologies and methods, as well as the consumer benefits and potential concerns relating to online advertising. The Town Hall proved to be an excellent venue for initiating what we expect will be a thoughtful exchange on the complex topic of behavioral advertising.

We also welcome the opportunity to comment on the staff's draft self-regulatory principles for online behavioral advertising released on December 20 of last year. We begin our comments with a brief discussion of the many benefits of online advertising, which the FTC acknowledged and emphasized both during the Town Hall and in the Commission's release of the draft self-regulatory principles. We then provide an overview of Google's approach to privacy and security as background for our substantive comments on the proposed principles. In addition, we explain why we agree with the FTC's decision to focus its efforts in this matter on self-regulation, which we believe is the most appropriate and productive method of ensuring innovation, competition, and consumer protection.

In our substantive comments on the proposed principles, we discuss three general themes that Google believes the FTC should consider as it moves forward with refining the proposed principles: the importance of distinguishing between personally identifying information (PII) and information that is not personally identifying (non-PII); the need to have a narrower definition of "behavioral advertising"; and the necessity of drawing a distinction between first-party advertising and third-party advertising. Finally, we provide specific comments about four of the principles proposed by FTC staff, which build upon the three themes.

Benefits of Online Advertising

The Town Hall highlighted the real benefits that online advertising offers to consumers by connecting them with information, products, and services they seek. Many Town Hall participants, including Google, demonstrated that relevant online ads are useful to consumers. Our experience that relevant or targeted advertising is useful to our users is supported by industry research. For example, a recent Forrester Research study found a significant increase of up to 35 percent in consumer click-throughs on targeted advertisement. In short, both our own experience and third-party research demonstrate that consumers value relevant advertising.

In addition, online advertising is a critical building block for free expression on the web, the success of businesses of all sizes operating online, and the well-being of the Internet economy, which is growing as an important component of our overall economy.

Online advertising provided by Google and others undeniably promotes freer, more robust, and more diverse speech. For example, we know that many website owners can afford to dedicate themselves to their sites more fully – and sometimes full-time – because a significant percentage of our advertising revenue ends up in the hands of publishers of blogs and other online information resources. In fact, the majority of our advertising revenue from our AdSense network goes to our partners. In 2007, for example, we paid over $4.5 billion in revenue to web publishers that provide AdSense network ads on their sites. Google derives particular satisfaction from helping to enable and support this extraordinary proliferation of online speech and activity.

We have seen in our own business how our advertising network has helped bloggers and small businesses – the "long tail" of the Internet – prosper in ways that would not have been possible just a decade ago. In fact, much of the advertising revenue that we share with web publishers goes to small publishers who use it to support and grow their businesses. In addition, small businesses are able to connect in an affordable and effective manner with otherwise unreachable consumers, including consumers in small, remote, or niche markets. Our AdWords service is attractive to small businesses because it allows an advertiser to decide exactly how much money to spend on advertising – there is no minimum spending requirement – and to tie its spending directly to the response of a potential customer, which helps ensure an excellent return on investment.

Online advertising has also benefited the Internet economy as a whole. The revenue from online advertising has allowed companies like Google to offer services and products to the public for free – everything from search engines to e-mail to online geographic information is supported by online advertising. These free tools serve as platforms for individual creativity, greater economic efficiency, and the creation of new businesses and business models. The growth in online advertising revenue has also spurred innovation, competition, and investment in the online advertising space – all of which produce consumer benefits in the form of more online resources and more relevant information.

Google's Approach to Privacy and Security

Google operates in a business landscape that is marked by rapid change, product innovation, and significant competition. We offer many innovative products and every new product has the central focus of satisfying our users. We believe user trust is essential to building the best possible

products. With every Google product, we work hard to earn and keep that trust with a long-standing commitment to protect the privacy and security of our users' personal information.

At the bedrock of our privacy practices are three design fundamentals:

- **Transparency**: We believe in being upfront with our users about what information we collect and how we use it. This transparency helps our users make informed choices about their personal information. We have been an industry leader in finding new ways to educate users about privacy. For example, our Google Privacy Center (which you can find at www.google.com/privacy) features privacy videos that explain our privacy policies in simple, plain language, along with our privacy policies.

- **Choice**: We strive to design our products in a way that gives users meaningful choices about how they use our products and services and, in cases where we collect data, what information they provide to us. Many of our products, such as our Search services, do not require users to provide any PII at all. When we do ask for personal information, we endeavor to provide features that give users control over that information. For example, our Google Talk instant messaging service includes an "off the record" feature that ensures that nothing typed by the user is saved on our servers.

- **Security**: We take seriously the need to protect the information that our users entrust with us. Google employs some of the world's best engineers in software and network security and has teams dedicated to developing and implementing policies, practices, and technologies to protect this information.

Self-Regulation and Government Regulation

Google has called for the creation of a federal privacy law that would accomplish several goals such as building consumer trust and protections; creating a uniform, flexible, and simplified framework for privacy, which would both create consistent levels of privacy protection across jurisdictions and foster innovation; and putting penalties in place to punish and dissuade bad actors.

We also support the FTC staff's self-regulatory approach, which makes the most sense for a media- and industry-specific regulatory framework and for a business that is so sharply characterized by rapidly changing technology and numerous and fast-evolving business models.

To be effective and credible, however, self-regulation must have as its foundation agreed-upon fair information practices and must be informed by ongoing dialog with and input from consumer advocates, the Commission, and other stakeholders. The FTC staff's draft self-regulatory principles for online behavioral advertising provides an excellent foundation for developing the most effective consumer protection, while maintaining an online environment in which innovation and competition can thrive.

Our hope is that the privacy principles – once finalized and written to ensure that they can be operationalized by industry and will provide consumers with appropriate levels of transparency and choice – will be adopted widely by the online advertising industry and will serve as a model for industry self-regulation in jurisdictions beyond the United States.

Comments on the Proposed Principles

While we find much to support in the staff-proposed self-regulatory principles, we do have some overarching concerns relating to the scope of data covered by the proposed principles and activities apparently intended to be covered by the draft principles.

Distinguishing Between PII and Non-PII

First, although the staff acknowledges that the collection and use of information that does not identify a particular individual poses little risk to consumers, the draft principles do not differentiate between the treatment of PII and non-PII. We do not believe that the record supports a conclusion that it is appropriate to abandon the time-tested distinction between PII and non-PII, especially when it comes at the expense of research and innovation that benefit consumers.

Nevertheless, we believe that the distinction between PII and non-PII often depends on the context in which the information is collected and used. For example, an Internet Protocol (IP) address might be PII when combined with account registration data from an Internet Service Provider. However, IP addresses are not PII when they are collected by web site operators or advertising networks from the Internet browsers of unauthenticated users.

Accordingly, if the FTC staff were to conclude that there is a real need for more robust self-regulatory principles for handling non-PII (as self-regulation such as the Network Advertising Inititiative's principles has done) and define the special circumstances under which non-PII may require higher levels of protection. More simply put, we would ask that the FTC structure the principles in a manner that would treat PII in one way, non-PII in another way, and non-PII that is closer to identifiability in a third way.

Finally, we urge the staff to give careful consideration to how a decision to place further constraints on the collection and use of non-PII could detrimentally affect the robustness of our research, the quality and quantity of our innovation, the protection of our network, and the delivery of better products and services to our users. We have detailed the benefits of our access and use of data such as IP addresses in a recent series of posts on Google's public policy blog (located at googlepublicpolicy.blogspot.com).[1]

Modifying the Definition of "Behavioral Advertising"

For purposes of the Town Hall it was appropriate to define behavioral advertising broadly in order to demonstrate the variety of approaches to online advertising that exists today, each of which involves a wide spectrum of data collection and use practices. However, the draft principles define

[1] See Alma Whitten, "Are IP addresses personal?," *Google Public Policy Blog*, http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html, published February 22, 2008; Hal Varian, "Why data matters," *Google Public Policy Blog*, http://googlepublicpolicy.blogspot.com/2008/03/why-data-matters.html, published March 4, 2008; Niels Provos, "Using log data to help keep you safe," *Google Public Policy Blog*, http://googlepublicpolicy.blogspot.com/2008/03/using-log-data-to-help-keep-you-safe.html, published March 13, 2008; Shuman Ghosemajumder, "Using data to help prevent fraud," *Google Public Policy Blog*, http://googlepublicpolicy.blogspot.com/2008/03/using-data-to-help-prevent-fraud.html, published March 18, 2008; Paul Haahr and Steve Baker, "Making search better in Catalonia, Estonia, and everywhere else," *Google Public Policy Blog*, http://googlepublicpolicy.blogspot.com/2008/03/making-search-better-in-catalonia.html, published March 25, 2008.

behavioral advertising so broadly as to encompass virtually any collection and use of information about individuals' online activities.

An effective self-regulatory framework, in our view, should call on companies to address in an effective way specific activities with specific best practices. If the framework applies to too broad a set of activities, its very breadth will necessarily produce consensus only around a low common denominator in order to permit adherence and compliance by companies engaged in often dissimilar activities.

As currently drafted, the proposed principles would apply to contextual advertising, which we define as advertising that is provided in response to the current activities of a user. For example, our AdWords program allows us to provide ads on Google.com in response to search queries entered by our users. In addition, our AdSense product allows us to provide ads to visitors to the web sites of third-party publisher partners based on the content of pages visited. In essence, then, our contextual advertising allows for the delivery of advertisements based on search queries or our analysis of the content of a web page being viewed.

We believe that this type of advertising should not be considered behavioral advertising, even if such analysis takes into consideration previous search queries. As we have discussed with the FTC staff, we are currently experimenting in our Search service with providing ads based on both the current query and the immediately previous search. For example, a user who types "Italy vacation" into the Google search box might see ads about Tuscany or affordable flights to Rome. If the user were to subsequently search for "weather," we might assume that there is a link between "Italy vacation" and "weather" and deliver ads regarding local weather conditions in Italy.

In the above example, we are serving an ad based on a user's activity on our site, and not the sites of other parties. More specifically, the example is one of first-party advertising that users expect to see in response to the search terms they enter into the Google search box. Note, too, that contextual advertising does not involve the use of PII. The combination of the first-party nature of our Search advertising, the consumer expectation of advertising (ads that appear to the right of our search results) in response to consumer action (a user's search), and the use of non-PII lead to the conclusion that this is not the type of advertising that ought to be the focus of the FTC's efforts to develop effective self-regulatory principles.

The staff should be aware, moreover, that failing to define behavioral advertising precisely, or an attempt to categorize specific activities as elements of behavioral advertising (*e.g.*, search queries, clicks, and other similar online activities) could have unintended, and very negative consequences. For example, as we discuss at length below, we believe that this broad definition could hinder our Search service by effectively prohibiting us from providing useful information to our users about sensitive topics despite the fact that providing such advertising involves no PII and provides great benefits to our users.

Though we believe that the definition of behavioral advertising requires narrowing, we also note that the definition does not capture online advertising provided on the basis of user profiles created by means other than consumers' online activities. Thus, for example, online advertising based on user profiles created upon registering for a web-based email account would possibly not be included in the staff's definition. As well, other forms of online advertising such as advertising based on demographic information of consumers obtained from offline resources may not be captured by the

definition.

First-Party Advertising vs. Third-Party Advertising

The proposed principles do not distinguish between data collection and use in what we will refer to in our comments as first-party advertising on the one hand and such activities performed in third-party advertising on the other. Making such a distinction is important, and we discuss it in two dimensions.

First, data collection and use on one site involves different privacy and security considerations from data collection and use across multiple sites owned and operated by different parties. For example, if a website dedicated to cancer treatment offers ads about cancer medication to its visitors that would appear to be appropriate. However, providing ads to those same individuals once they have moved to another type of website (one dedicated to sports, for example) based on the fact that they previously visited the cancer treatment site potentially merits a different analysis.

Second, the proposed principles need to define their applicability to first-party activities and third-party activities to be workable. For example, in Web 2.0 the traditional definition of a web page is often inapplicable. A web page hosted by Google – for example our *i*Google page – may feature embedded Google Gadgets, which are simple applications that can be added by our users to their *i*Google pages and that may contain ads. In a Web 2.0 world, any web page could have any number of third party applications embedded in it – each one providing a different service, collecting different data, using the data in multiple ways, and providing advertising based on disparate criteria. In the near future, these applications that are embedded into one page but are provided by different parties may actually exist on more than one page. For example, a user of Facebook and MySpace may have the same third party application embedded into both her Facebook profile page and her MySpace profile page.

In some instances, the user may have a direct relationship with an application embedded into a page and the provider of that page. In those cases both the application provider and the provider of the page may be first party advertisers – but only one would have the ability to provide the appropriate notice and choice called for in the proposed principles.

In other instances the application provider may merely be a third party with no direct relationship with the user of the page, even though the user chose to include that application on a web page. In such instances, it would also be important for the provider of the web page to be distinguished from the third party application provider, which would ultimately be better situated to provide notice and choice to consumers.

Specific Comments

Principle 1 – Transparency and consumer control

Given how seriously Google takes the principles of transparency and choice, we believe that the FTC's language must be precise and workable in order for the principles to succeed and gain wide adoption. As noted above, we support fully the principles of transparency and choice for our users and we apply these principles to our products and policies. However, Google's experience is that choice is often more appropriate over PII rather than non-PII, and more appropriate for use than

collection of data. Indeed, we design our products to give our users meaningful choice over PII in a way designed to reduce privacy risks. We believe that requiring choice to be built for non-PII might in certain circumstances result inadvertently in increased privacy risks for our users.

Our Search service is a case in point. Any user can visit the Google web site from any browser and use our search engine without providing PII as an "unauthenticated" user – a user who has not registered for our services or who has registered for our services but who has not logged in for the session in question. For these services, Google retains very little data – typically standard server log information. We also may collect a unique cookie ID generated for the browser from which the request originated.

On the other hand, users may use Google Search in an authenticated state, in which case we associate their search queries with their registration information (which is generally limited to a name, a login name, an existing email address, and the country where the user resides).

When using Google Search our users therefore have the choice between interacting with our service in an unauthenticated state or an authenticated state, and if they choose to do so in an authenticated state they can further limit or eliminate the association of search queries with their registration information through the use of Web History. Web History is a feature that allows authenticated users to view and search across the full text of the pages they have visited, including Google searches, web pages, images, videos and news stories. Users also have the choice to pause or disable Web History and manage their web activity by removing items from Web History at any time.

Though Web History provides several choices to our users, it is unclear whether the language of Principle 1 contemplates these methods of providing choice. It is also unclear what would be the benefit of attempting to provide choice to an unauthenticated user who, by definition, is not providing us with PII.

Furthermore, we believe that providing the type of choice required by Principle 1 may require the collection of actual PII from a user, thus essentially compelling an unauthenticated user to become an authenticated user. For example, if the principle were interpreted to require an unauthenticated user to opt out of the collection of non-PII, the only way to be able to prove that we have given that opportunity to each of our users would be to require them to register and then opt out. Otherwise, we would have no way of demonstrating that we actually gave to each user of our services the choice to opt out of the collection of non-PII by our services.

We believe that setting forth uniform standards for choice may work in certain contexts. For example, uniform standards for transparency and choice for third-party display advertising services would be appropriate. However, in other areas – such as in first-party search-based advertising – we believe that it is appropriate for Internet companies to innovate and experiment with the choices they offer, but inappropriate to mandate that choice be offered in all circumstances. In these contexts, as long as consumers are well-informed, able to select the sites they visit, and able to navigate to a competing service with the click of a mouse if they are not satisfied with the choices offered on one site, we see no reason for specific types of choice to be mandated with respect to all data collected (PII and non-PII) for the purpose of behavioral advertising (as defined by the proposed principles) – especially when such requirements could detrimentally impact services that consumers value as well as consumers' data privacy and security. In these cases, transparency in the form of consumer-friendly explanations of data collection and retention policies ought to be the

focus of self-regulatory principles.

Moreover, implementing the choice model contemplated by this principle would be immensely complex in a Web 2.0 world, where – at the invitation of a user – a dozen parties might be collecting different data for different purposes on a single page. How would this requirement be met where a user has a relationship with a site and also, separately, with each of the applications (or even potentially various advertisers within the page or application) she embeds for personal use on that site, especially where some of the applications may collaborate with each other? In this situation, consumers need to understand the activities to which a particular site's privacy policy applies, and those where it does not, and they need to know where they can learn about the privacy policy that does apply. But it is unworkable to require a site operator to establish, vouch for, and monitor compliance with respect to independently provided functionality. Any such requirement will inevitably limit the functionality available to and desired by users.

We have been and continue to be strong advocates for better notice by third party display advertisers in the form of a link to a web page with information for opting out of the delivery of targeted ads, and other useful consumer information about the display ad. We believe that providing this kind of transparency and choice in connection with a display ad provided by a third-party ad server would protect consumers, provide useful feedback to advertisers, and not hinder this type of advertising. We have attached to these comments a mock-up of the type of notice with which we have experimented.

Principle 2 – Reasonable security, and limited data retention, for consumer data

This principle requires data collectors to provide reasonable security for consumer data based on the sensitivity of the data in question, the nature of a company's business, the risks involved, and the available technology. This is a reasonable standard – indeed, our belief is that it is the current standard – as applied to PII. If the staff intends to expand this requirement to cover non-PII then, at a minimum, more specificity is needed as is the rationale for covering non-PII.

In addition, Google believes that data retention practices are part and parcel of reasonable security practices, and need not be called out separately. For example, as we have disclosed to the public and discussed with the Commission, in March 2007 Google made the decision to anonymize the cookie ID and the last octet (typically one to three digits) of the IP address associated with search queries after 18 months. Even though neither an IP address nor a unique cookie ID is PII, we believe that our users would prefer that we further anonymize this data after a reasonable period of time.

We believe that our 18 month retention period accomplishes several legitimate research and development, business, security, and regulatory compliance goals as discussed in our series of blog posts on data referenced above.

Principle 3 – Affirmative express consent for material changes to existing privacy promises

This principle would require affirmative express consent for material changes to an online company's privacy policy. The current standard, set by the FTC in various consent agreements, requires data collectors to provide choice when it proposes to use PII collected in a manner that is not consistent with the policy governing use of such data at the time of collection.

Depending on the circumstances, including the nature of the PII and the nature of the policy change, choice may be either opt-in or opt-out as appropriate. It is not clear why this change is needed and it is difficult to see how this could be achieved in practice, particularly with respect to non-PII data about unauthenticated users.

More specifically, the principle calls for obtaining "affirmative express consent from affected consumers" in a "corporate merger situation to the extent the merger creates material changes in the way companies collect, use, and share data." As noted above, the proposed principles apply to all data collected and used in connection with "behavioral advertising." It would not be possible for Google or any other company to seek and obtain such affirmative express consent from unauthenticated users whose data (non-PII because the users are not authenticated) may be used in a materially different way from how such use is described in its existing privacy policy.

In addition, Principle 3 makes no distinction between materially different practices involving data collected and used after the change in question on the one hand and data collected and used prior to the change in question on the other. We believe that this is a distinction that requires the FTC's attention.

Principle 4 – Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising

This principle would either require the affirmative consent, or simply prohibit, collection of sensitive personal data for behavioral advertising. We believe that this is a principle that could significantly impact both our Search service and other services that we provide.

We are particularly concerned about this principle in light of the broad definition proposed for behavioral advertising. Under the proposed definition for behavioral advertising, this principle could preclude legitimate contextual advertising practices, which are viewed as positive by consumers. For example, if a user searches for "HIV" with Google's search engine, the user will likely see – and would likely be surprised not to see – ads relating to HIV treatments, clinics, or other resources along with the search results provided by Google. Such a search, particularly in an unauthenticated environment, says absolutely nothing about the searcher's health status. Similarly, the fact that someone navigates to sites containing information on cancer, Christianity, or gay rights is hardly an indication that the user has cancer, is a Christian, or is gay. They might, however, want to purchase a book about any one of those topics as just one of many examples of what the user may intend.

We also note that the principle applies to the collection of "sensitive data." The principle does not define "sensitive data," but does provide examples of such data including information about health conditions and information about sexual orientation. However, as noted above, the proposed principles do not distinguish between PII and non-PII in the definition of "data." As a result, Principle 4 would not allow Google to collect a search query for "cancer treatment" or "alcoholics anonymous" from unauthenticated users because we do not have any relationship with an unauthenticated user and we have no way to obtain that user's consent – affirmative and express or otherwise – prior to collecting the search query.

Furthermore, the principle applies to "collection," which as can be seen in the above example is problematic. Many, many web services collect information every second that may be considered

sensitive – even standard log data such as a referring uniform resource locator may contain sensitive information – and there is no workable way to either stop that collection or put into effect a system for obtaining consent prior to such collection.

Accordingly, we would recommend the clarification of the definition of "sensitive data" and the refinement of the definitions of "behavioral advertising" and "data." We would also suggest that the FTC staff consider restricting the use of "sensitive data" rather than the collection of such data to ensure that any requirement for consent is reasonable and achievable.

Conclusion

Google wishes to thank the FTC for its attention to our comments and for the Commission's continuing commitment to protecting the privacy and security of consumers – a responsibility that we wholeheartedly share.

As we have stated above, we welcome and support the FTC's efforts in the area of online advertising, and we wish to continue working with the Commission to ensure that the principles, once finalized, are workable and widely adopted even beyond the United States.

Should you wish to contact us regarding our comments, please do not hesitate to contact Pablo Chavez, Google Senior Policy Counsel, by email at pablochavez@google.com or by phone at 202.346.1237.

Sincerely,

Alan Davidson
Senior Policy Counsel and
Head of U.S. Public Policy
Google Inc.

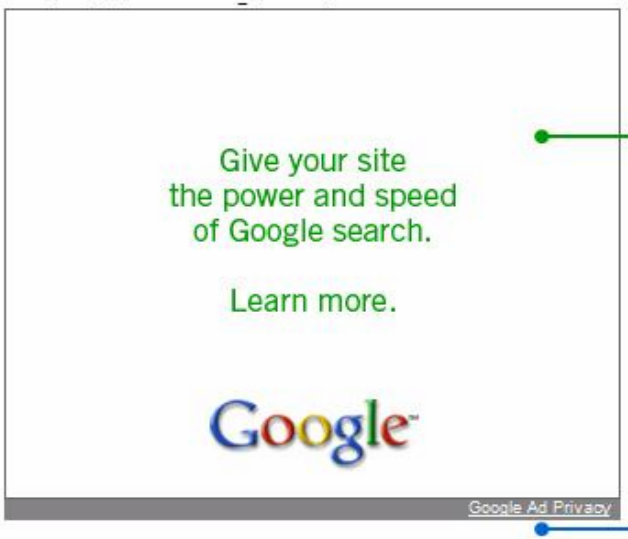
Attachment

ATTACHMENT

Google experimenting with ads with notice

Google

Sample graphical ad with privacy notice



Advertising landing page

Google privacy information page