February 18, 2011

Donald S. Clark, Secretary
Federal Trade Commission
Office of the Secretary, Room H-113 (Annex W)
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Re: FTC Staff Preliminary Report on Protecting Consumer Privacy – File No. P095416

Dear Secretary Clark:

The Future of Privacy Forum ("FPF") is a think tank seeking to advance responsible data practices and is supported by leaders in business, education and consumer advocacy. FPF thanks the Federal Trade Commission ("FTC") for providing this opportunity to comment upon the Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (December 1, 2010) ("the Report"). FPF offers what we believe are unique insights reflecting best practices and developing innovations regarding data privacy and hope these insights help shape the Report and the emerging framework going forward.[1]

We thank the Commission for bringing interested parties together for the privacy workshops that preceded the Report. These events were an excellent opportunity for the various stakeholders in data privacy to communicate with the FTC and each other, sharing practical experiences and the latest privacy innovations. We look forward to the anticipated public sessions following the close of the comment period on the Report for further useful exchanges.

We commend the FTC for proposing a framework for businesses that will improve and advance consumer privacy and is a catalyst further meaningful discussion, research and development of improved privacy practices.

The comments herein do not address every question raised in the Report. FPF has restricted its comments to subjects consistent with the organization's activities and experience examining consumer privacy:

- Special choice mechanisms for online behavioral advertising (e.g., Do Not Track mechanisms)
- Scope of online data retained and the duration of such retention
- Commonly accepted collection and use of online data which may not be subject to heightened notice and choice expectations

[1] The views expressed herein do not necessarily reflect those of the Advisory Board or supporters of the Future of Privacy Forum.

- Notice and choice regarding use of data collected by entities that do not have a direct relationship with consumers
- Collection and choice mechanisms for sensitive data
- Development and implementation of enhanced privacy notice mechanisms

I. Special Choice for Online Behavioral Advertising: Do Not Track

The proposal in the Report for a special choice mechanism for online behavioral advertising denominated "Do Not Track" ("DNT") raises important questions about whether a universal choice mechanism can be designed for consumers to control online behavioral advertising and whether a law is necessary to mandate such a choice mechanism. FPF fully supports enhanced consumer control over the sharing of online information by others to deliver targeted advertising. We believe that the creation of effective choice mechanism will occur through the combined efforts of browser companies, ad networks, consumers and the government. We do not believe that a new law is easily achievable or desirable, given the potential for progress through the collaboration we envision.

Since its creation in 2008, FPF has focused on better ways for consumers to exercise control over online tracking that is used in targeting online advertising. In 2009, the Future of Privacy Forum, in cooperation with the Center for Democracy and Technology, launched an effort to improve the current cookie-based opt-out mechanism offered by many online behavioral advertising companies.[2] Aware of the fact that many opt-out cookies are deleted by consumers or their anti-spyware programs, we convened companies, trade groups, advocates and technologists for a number of discussions aimed at formulating a more reliable process for providing consumers with options to limit the Web tracking taking place for behavioral advertising purposes.

In December 2010, FPF convened a panel on the Do Not Track issue which included representatives from browser companies[3], consumer and privacy organizations[4], technologists, ad networks and policy groups. The presentations and discussions at that session suggest that through multilateral efforts, effective consumer choice mechanisms can emerge, with the need for a new law mandating such mechanisms (even assuming such a law with the requisite precision could be drafted and passed through Congress). We envision the multilateral efforts of browser companies, ad networks, consumers and the government would result in choice mechanisms of superior quality and greater flexibility in a shorter time span.

[2] Many online analytics companies offer consumers a similar cookie based opt-out choice.
[3] Sid Stamm represented Mozilla on the panel and Internet Explorer product manager Dean Hachamovitch attended the program.
[4] Michelle De Mooy of Consumer action and Erica Newland of CDT presented at the program.

The "Do Not Track Header," a solution put forward by one browser company, is a prime example of a choice mechanism that is emerging and is an approach that has received recent public attention since the issuance of the Report. It uses a special hypertext transfer protocol ("HTTP") header field to communicate consumer choices and involves the following steps:

- Browser companies provide consumers with an option in the preferences panel of the browser that would enable a special HTTP header and an API that websites or services could use for the purpose of setting this header for consumers who request this.
- Ad network servers that receive this header would recognize that the consumer has indicated that they do not want their activity online used to tailor advertising to them across unrelated websites.[5]

Services that offer consumers a cookie-based opt-out would treat consumers presenting the DNT header in the same manner they treated consumers relaying an opt-out cookie. When presented with the DNT header, companies would refrain from appending data acquired from third party sources in order to tailor advertising to users across websites. Companies would recognize the DNT header as an indication that there shall be "no targeting" based on previous unrelated activity. Moreover, the consumer choice communicated through the DNT header would be honored without regard to the method by which online data is collected, including cookies, device fingerprinting, local shared objects or other identifiers.

However, the DNT header would not affect tailoring of advertising for a user based on inferences made about a user based on the presentation of browser information or activity during a consumers visit to a particular website. Thus geo-targeting based on IP address or tailoring of ads based on a consumer's previous visit to the same website should be permitted.

Allowing third parties to activate a DNT header at the request of a consumer creates a number of benefits for consumers. First, this would allow the option to be promoted by third parties, including government, advocates and trade groups. Second, it would be compatible with the self-regulatory program that has already been adopted by many leading trade groups.

A DNT header could provide greater stability and resilience for consumer choices. Opt-out cookies are often deleted inadvertently by consumers. On the other hand, this header should not be subject to inadvertent deletion or deactivation.

Moreover, the DNT header could allow consumers to express their choices in a more granular and nuanced fashion than current choice options. Today, consumers can prevent or limit tracking by adjusting cookie or privacy settings within their browser or using browser options or third party browser plug-ins, which limit the data that is shared by their browsing activity. But these options are

[5] Whether two or more websites are related should be assessed from the perspective of the reasonable consumer.

unable to provide high degrees of nuance that can distinguish between the various ways that websites use data. These tools underblock, overblock, or in some cases, completely prevent the delivery of any third-party content or ads.[6]

The DNT header could facilitate greater nuance by accepting a variety of alphanumeric codes related to consumer preferences regarding a variety of data collection and use practices. For example, a DNT header field could be designed to indicate a consumer's desire to:

- refuse all behavioral tracking
- accept tracking based solely on online activity, to the exclusion of offline activity
- accept tracking based solely on non-sensitive information

The most productive way to advance a self-regulatory approach to special choice mechanisms is to convene a multi-stakeholder group to facilitate the necessary cooperation between browser companies, ad networks, consumer representatives, government and policy groups. No system requiring nuanced cooperation and technology development across business models and government policy will spring into existence without interactions that address the concerns of the key stakeholders. We urge the FTC to partner with the Department of Commerce ("Commerce") to convene such a group, in a process much as the Commerce has called for in its report. We recognize that other browser companies have generated alternative approaches to that described above and we appreciate the benefits of those approaches. Bridging the approaches of the different browsers would be well suited to such a multi-stakeholder solution.

II. Retention

Personal data that is not held by businesses, by definition, is not exposed to misuse. Thus, specified retention periods/deadlines for deletion will further privacy protection.

The concept of limited retention and specific deadlines for deletion of personal data is emerging despite the fact that it is easier administratively and simply less burdensome to retain what has been collected. One of the deterrents to the specification of a retention period (a deadline for deletion) is the concern that once committed to one retention period, changing to a longer period could be viewed as a material change in practices requiring consumer notice and choice. The FTC should recognize that a company's need to retain data can change over time, due to competition, security and fraud detection, concerns, or other factors. The FTC should allow companies some degree of flexibility to experiment with retention periods. Through such experimentation, multi-stakeholder groups may formulate best practices for data retention calibrated to the wide variety of ways that online data is collected and used.

III. Commonly Accepted Practices

The concept of "commonly accepted practices" concerning the use of personal data for which providing notice and choice is minimized or eliminated in theory is a good one. The key challenge is defining how the concept should be applied to new or innovative ways to use data that almost immediately are "commonly accepted." Or to put it another way, can a new use of data immediately

[6] For example, tools that aggressively restrict third party cookies may interfere with non-advertising website content (e.g., widgets and apps) provided by third parties.

become “commonly accepted” because of its inoffensive and useful nature? Consider two innovations introduced by Facebook in the past few years: Facebook Newsfeed and Beacon.

Before the introduction of Newsfeed, Facebook users had to click through the pages of each of their friends to view any new information posted or any changes they had made to their profiles. Newsfeed automatically broadcasts changes made by a Facebook user to the pages of their friends. Many users were surprised and joined Facebook protest groups. Certainly, few would have opted in to this feature in a blanket manner. Despite the fact that this feature would likely not have been considered “commonly accepted” due to its novelty, it soon became an essential part of the Facebook experience and was soon copied by competitors. Today, much of the Facebook user engagement is due to the Newsfeed where they learn about their friends’ activities.

In contrast, however, is the Facebook Beacon program, where users were alarmed and rejected the program with such vehemence that it did not succeed. Beacon was a Facebook feature that transmitted data from external websites to Facebook to share user activity on external websites with their Facebook friends. Activities on partner websites were published in a user’s Newsfeed.

How can the “commonly accepted practice” concept distinguish between these two examples? If a new use is within the scope of the previously defined uses, subject to a reasonable consumer’s reading of existing public notices, no new consent should be required. If a new use is beyond the scope of the previously outlined uses, then the company should assess the privacy impact. Additionally, affirmative consent should be required if the change:

- involves sharing the information with additional parties
- increases the risk of harm to the user
- involves advertising or marketing-related data and is used in an unexpected manner
- is a material change to the way previously collected data is handled
- makes something public that was private previously

If the new use is transparent and obvious to users, and also provides added value to the user, then an opt-out system would appear permissible as long as the opt-out is clear and conspicuous.

We offer the foregoing for the Commission’s consideration and public discussion during the next phase of the Report’s development. We believe this approach to “commonly accepted practices” will prevent harm, assures user autonomy, and also allow room for continued innovation of new and novel services for consumers.

IV. Data Enhancement

Improved practices around data “enhancement” should focus on the practice of appending data used online to target ads across unrelated websites. A significant portion of the data used today for ad targeting is actually data about consumers that has been appended to a cookie. Current industry standards are unclear as to when and how enhanced notice or choice applies to such data. Consumers who do not understand or feel they have no control over this process are likely to be concerned about data enhancement for behavioral advertising based on website visits or searches. The practice of appending offline data, which was the subject of great controversy nearly a decade ago following the DoubleClick-Abacus merger, is now commonplace, but standards for such a data merger have not continued to evolve. Going forward, the industry should consider greater

transparency in the way that publishers, including search engines, disclose their retention and sharing of user activity data. This may permit consumers to exercise more control over the entities with which they share data that may later be added to profiles used by other Web publishers.

V. Sensitive Information

There is no clear, comprehensive definition of sensitive data --- that category of personal data deserving special protection. Of course, there are clear areas where certain types of personally identifiable data have already been well-defined as sensitive, but large gaps exist and data practices vary.[7] Some companies[8] refrain from using data about a consumers visit to health-related websites; others do use health data but refrain from creating certain categories such as cancer, incontinence, or impotence. With regard to health-related data, the Interactive Advertising Bureau ("IAB") and Direct Marketing Association ("DMA") self regulatory principles exclude the collection and use of pharmaceutical prescriptions and medical records about a specific individual.

Previous efforts to define sensitive data have been difficult. In 2008, the Network Advertising Initiative ("NAI") sought to expand the categories its members would avoid and proposed a set of restricted categories.[9] After criticism from advocates and the media, it withdrew this proposal and formalized a more limited set of restrictions.[10]

Ad networks owned by Yahoo, AOL and Microsoft generally maintain internal lists of restricted categories that will not be made available for marketing. These lists are generally confidential and are based on the editorial judgment of company executives.

Although research studies have examined general consumer views of behavioral advertising and some have found that consumers harbor concerns, very little work has been done to determine whether consumers differentiate between various types of health information used in this manner. The FTC should explore avenues at its disposal to encourage research into consumer sensitivities in this area and to better define "sensitive data."

VI. Improved Privacy Notices and Use of Symbols

It is a given, as explained in the Report, that detailed privacy notices are ineffective in many respects because they are not read by consumers. There is a compelling need for better mechanisms for consumer notice and choice.

[7] Examples include protected health information subject to HIPAA, consumer financial information subject to GLBA, and consumer reports subject to FCRA.
[8] DoubleClick does not use sensitive health data for behavioral ads, except for re-targeting visitors to a web site by that same company.
[9] Examples of health-related topics identified on the draft list of restricted categories included HIV/AIDS status, sexually-related conditions, psychiatric conditions, cancer status, and abortion-related information.
[10] The health-related category in the final list was "[p]recise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history."

Websites immediately inform a visitor of the purpose of the site and its features in order to make a sale or attract viewers. Similarly, enhanced online privacy notice mechanisms should immediately inform consumers of how their data will be treated in a simple, clear and immediate way. [11]

Enhanced privacy notice mechanisms might include symbols, short phrases, colors, diagrams, dashboards or any of the tools available to a Web designer who seeks to provide users with an engaging user experience. When companies embrace this concept of engaging consumers about data use as a core feature of the user experience, innovators and creative designers can take on the challenge of simplifying the description of complex practices and providing appropriate choices.

We believe that one potential means of providing such enhanced notice could be the use of symbols and icons to represent (1) compliance with a defined set of data practices and safeguards and/or (2) specific practices and safeguards. An example of the first approach is the "forward I" adopted by the Digital Advertising Association to indicate compliance with the Self Regulatory Principles for Online Behavioral Advertising. The "forward I" is an important achievement and FPF was pleased to conduct some of the original research around the use of icons for behavioral advertising communications.

Important examples of the second approach include the arrow symbol used by the Apple's iPhone to indicate that location sharing is occurring. Similarly, the Mozilla Foundation has developed a series of icons designed to indicate specific data practices.[12] This includes individual icons illustrating whether visitor data may be (1) shared with advertisers, (2) bartered or sold, (3) shared with law enforcement without legal process, and (4) stored for one, three, six, or 18 months or indefinitely. We look forward to the results of further studies evaluating the effectiveness of these techniques in informing consumers and to the development of similar tools in the future. And we urge the Commission to explore the use of symbols and icons to inform consumers about their privacy.

****

We hope that these comments contribute to the ongoing efforts of the FTC to advance responsible and dynamic practices and we look forward to continuing to support the FTC leadership in this area.

Sincerely yours,

Jules Polonetsky

Christopher Wolf

[11] Off-line privacy notice off-line may not be feasible with the same immediacy, but might be provided at other appropriate occasions, such as near a cash register or at the entry of a store, and through the use of commonly-understood symbols.

[12] These icons are described in greater detail at http://www.fastcodesign.com/1662961/mozillas-privacy-icons-tell-you-whos-sniffing-your-data-on-the-web.