Performance Marketing Association, Inc.

February 18, 2011

Via electronic filing

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Performance Marketing Associations Comments on the Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change

The Performance Marketing Association ("PMA")[1] is a not-for-profit trade association that represents the interests of the rapidly expanding online performance marketing industry. Our membership includes over a 100 companies and many individuals that are leading the performance marketing industry.

The online performance marketing industry accounts for an estimated 8 billion dollars in annual domestic revenue and continues to experience explosive growth regardless of the down economy. The heart of the performance marketing industry and online advertising relies on tracking advertisements served to online consumers. All online ads, whether banner, search, email or any other medium rely on tracking mechanisms. Without tracking technologies the performance marketing industry would have no method to track the ads it serves on behalf of advertisers.

Although we agree with the FTC that consumer privacy is of utmost importance, the language of the Preliminary FTC Staff Report[2] on Protecting Consumer Privacy would effectively destroy this billion-dollar online performance marketing industry.

Allowing consumers to browse anonymously online is not and should not be a reasonable consumer expectation. When consumers visit local retail establishments, they do not expect to browse anonymously and undetected through the stores. What is commonly expected is that a visit to a retail establishment may involve a store clerk assisting and watching the consumer's movements, security cameras tracking and recording the consumer's actions, a store clerk verifying the consumer's identity upon purchasing goods, and in many stores the tracking of a consumers preferences in order to better serve their needs on their next visit.

[1] For more information on the PMA you may visit us at www.performancemarketingassociation.com.
[2] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report (Dec. 1, 2010) ("FTC Staff Report").

79 Daily Dr. #106
Camarillo, CA 93010
805.445.9700
www.performancemarketingassociation.com

It would be ridiculous to prohibit a retail establishment, for example a jewelry store, from observing consumers while they shopped around their store or to require a library to not observe, collect information and track visitors to the library. The principals set forth in the FTC's Staff Report would do exactly that in an online context. The proposed principals would allow consumers to visit online retail establishments, service providers, public and private websites without being tracked by those sites. Allowing users to visit sites anonymously would hinder businesses and website owners from performing basic and necessary functions such as preventing and tracking fraud.

As the rapid and prolific growth of Internet sites such as Facebook, MySpace, Foursquare and YouTube increases, consumer expectation of online privacy is rapidly decreasing. Millions of consumers visit these and other sites on a daily, if not hourly, basis to post status updates, tell their friends, and sometimes random strangers, where they are at any given moment and upload personal videos for the entire world to see. Facebook currently has over 500 million users and more than half of those users log-into Facebook every single day and creates an average of 90 pieces of content.[3] Although some social networkers may be concerned about their privacy the vast majority of online users today readily post personal information about themselves online for the world at large to view. Given the prolific daily use of social networking and other content posting sites it seems that this concern for protecting consumer privacy may be exaggerated and is not actually an issue for millions of online consumers.

The companies that are violating consumer privacy, misusing personally identifiable information and causing concern to consumers will not be stopped by additional regulation. These types of malicious companies ignore existing rules when they steal or misuse consumer data, so increased regulation will not curb this type of behavior. In fact implementation of many of these proposed principles could actually increase the amount of internet fraud as websites would no longer be able to track fraudulent users or block access from malicious IP addresses and domains.

In order to provide greater protection for consumer privacy, we believe the FTC should support industry initiatives and self-regulation. The PMA supports the *Self-Regulatory Program for Online Behavioral Advertising* that has been developed by industry leading organizations including the Better Business Bureau, Interactive Advertising Bureau and the Direct Marketing Association.[4] Self-regulatory programs such as this are the best way to educate consumers and companies on important privacy principals and the most effective way to ensure compliance. As more companies offer simplified choice mechanisms and participate in self-regulatory programs, more consumers will be able to control their online footprint.

Outlining notice and choice in a posted privacy policy is a commonly accepted practice of which consumers are aware. The focus should be on simplifying privacy policies and ensuring that all online businesses have a posted policy to which they adhere. Providing notice in a posted privacy policy, and a

[3] http://www.facebook.com/press/info.php?statistics

[4] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009)*, available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

means by which the consumer can easily opt-out of having their information shared, meets consumer expectations and effectively protects consumer privacy. If a consumer is concerned about how an online business will share their personally identifiable information, they can read how the company uses their information in a posted privacy policy and at that point choose whether or not to provide their information to that company.

Industry self-regulation is the only practically way to increase consumer privacy protections as no government imposed regulation will be able to address all of the nuances of the rapidly expanding and daily evolving online industry.

The PMA has signed the Direct Marketing Association's response to this FTC Staff Report and as that response provides a good general overview of our response, this letter will focus on answering specific questions which were raised in the FTC report and providing examples of how this proposal will affect real businesses, particularly as they impact performance advertising.

FTC QUESTIONS FOR COMMENT ON PROPOSED FRAMEWORK

Q: Is it feasible for the framework to apply to data that can be reasonably linked to a specific consumer, computer, or other device?

A: Obtaining consent to collect non-personally identifiable information is not necessary, as by the very nature of this type of information it does not affect consumer privacy rights. Nor is this feasible, as in many situations collection of non-personally identifiable information occurs prior to the consumer accessing the companies' sites or services. For example, if a consumer visits a web page from their mobile phone many sites employ technology that allows the site to track the type of device that is accessing the site and modify the browser type to provide optimal viewing for the mobile device. And they do this without the need of any personally identifiable information.

In addition, many websites and services prohibit site visits or registrations from IP addresses located outside of the United States or IP addresses and domains that are listed on a recognized black list. This type of tracking and blocking of non-personally identifiable information, namely IP addresses or domains is necessary in order to protect the security and integrity of many internet sites.

Q: How should the framework apply to data, while not currently considered "linkable", may become so in the future?

A: Current tracking technologies rely on unique but anonymous attributes. It is not conceivable to us where or why this would change. There is burden in using PII, which works against the effectiveness and efficiency of online advertising. As such, it is not feasible to apply the framework to data that may at some future point become PII as there are too many unknown variables.

Q: Should the concept of "specific business purpose" or "need" be defined further and, if so, how?

79 Daily Dr. #106
Camarillo, CA 93010
805.445.9700
www.performancemarketingassociation.com

A: A specific business purpose or need varies greatly from business to business and industry to industry so there is no feasible way to provide a definition that would encompass all of the different legitimate business purposes for which data is collected. The best way to handle this issue is to encourage businesses to provide a clear and concise description of their specific business purposes and need for collection of consumer data in their posted privacy policies.

Q: Is there a way to prescribe a reasonable retention period?

A: A reasonable retention period is different for each and every business and each business has different business purposes for retaining information. For example some companies have a 30 day merchandise return policy, some a year and some have unlimited return policies. In order to process a return and refund those companies must retain personally identifiable information. Medical companies dealing with medical histories must retain patient records indefinitely in many cases. This is an example where a storage limit could be detrimental to someone's health.

Q: How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?

A: These principles cannot apply to legacy data systems, if the data owner already owns data that was collected in accordance with existing laws; then applying these new principles to existing data would result in data owners having to destroy vast quantities of data. This could arguably be an unconstitutional deprivation of property rights or at least amount to civil forfeiture of property. Data is valuable and many businesses have built their services around the collection and use of data for a wide array of purposes so in order to impose new regulations on businesses that collected data in accordance with the laws existing at the time of collection would be unjust and would destroy thousands, if not hundreds of thousands, of businesses. And as mentioned above, there are use cases where it is in consumers' best interest to have their data stored and maintained.

Q: How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?

A: The incentive for companies to develop and deploy enhanced consumer privacy protections will be market driven. As more consumers become aware of their privacy rights and choices, those businesses that offer clear, concise and easily understood choices will attract more consumers than those businesses that ignore consumer privacy. That being said, the PMA believes there is opportunity for industry to provide clear, concise and consistent policies to consumers and we recommend these be included as part of the self-regulation program.

Q: Is the list of "commonly accepted practices" of the report to broad or too narrow?

A: The list is definitely to narrow and leaves out many accepted uses of personally and non-personally identifiable data. The problem is not just that the list is to broad or too narrow, the problem is with the term "commonly accepted practices" as this insinuates that all practices not on this list are

unaccepted practices. And what is so wonderful about innovation and technology advancements in this country, we can assume there are practices not yet conceived but will be perfectly reasonable for consumers. This must be rephrased so as to eliminate this insinuation. We support the DMA coalition's suggestion to instead use the term "information practices where choice is not required."

Q: What types of first-party marketing should be considered "commonly accepted practices"?

A: All types of first party-marketing. Specifically, affiliate marketing should be considered first-party, as they present ads often as the initial interaction with a consumer.

Q: Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing?

A: Consumers should still be given a choice if the sensitive data being collected includes financial or health information.

Q: Should first-party marketing be limited to the context in which the data is collected from the consumer?

A: First-party marketing should not be limited to just the context in which the data was collected. For example, if information is collected online for first-party marketing that same party should be allowed to use it in other contexts such as for mobile or print marketing, such as offering a relevant coupon. This has become a highly valued consumer benefit and important to re-marketing and customer retention efforts.

Q: Should marketing to consumers by commonly branded affiliates be considered first-party marketing?

A: All Affiliates, just like all publishers of advertising, should be considered first-party marketing. Publishers of ads typically present the first interaction with a consumer, or an interaction previous to the online retailer. Online advertising would cease to function if publisher was subject to third-party opt-out rules; the consumer would not be able to go from the ad to the advertiser when the ad was clicked.

Q: How should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both online and offline, to enrich its database?

A: This should be allowed, as this is an important tool used to verify legitimacy of collected information and to match with additional information in order to obtain a complete customer profile. This is particularly important in identifying fraud and matching user to blacklists, for example.

Q: What is the most appropriate way to obtain consent?

79 Daily Dr. #106
Camarillo, CA 93010
805.445.9700
www.performancemarketingassociation.com

A: Simply through a posted privacy policy which clearly and concisely explains the company's use of the consumers data.

Q: Should the method of consent be different for different contexts?

A: The method of consent must be different for different contexts as the method to consent to consumer data being collected in person, over the phone, via the internet or in a mobile context is necessarily different.

Q: Would a uniform icon or graphic for presenting options be feasible and effective?

A: Yes! The PMA supports the Icon developed by the *Self-Regulatory Program for Online Behavioral Advertising* and believes that the promotion of a single, recognizable icon is the best way to provide consumers with an easy mechanism to control their online privacy choices.

Q: Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices?

A: It is always appropriate to offer choice as a "take it or leave it" proposition. This proposition is common in many, if not all traditional business models. This is the same as a restaurant having a "no shoes, no service" policy. Businesses, whether online or offline, have the right to only serve those customers who comply with their policy. The businesses' policy should be clearly communicated in its written privacy policy.

Q: What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide?

A: It is not possible for a company that does not interact with the consumer to provide that consumer with choice mechanisms, so nothing could be provided.

Q: Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

A: As data brokers do not interact directly with consumers it is not feasible for a data broker to provide choice mechanisms to consumers. However, it seems reasonable for businesses that do have direct interaction with consumers to include their general use of data brokers in their privacy policies displayed to consumers.

Q: Should companies be able to charge a reasonable cost for certain types of access to data and should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?

A: The burden on companies to compile, sort and provide access to consumers' data would be overwhelming for many small to medium sized businesses and a financial strain on even large companies. However providing consumers free access to their data is a legitimate concern. Many state laws already address this issue of providing consumers access to their data so any regulation in this area should mirror state law.

For example established California State law[5] already addresses this specific issue and requires that any business, with more than 20 employees, that has disclosed customer information belonging to a resident of California, to third parties for direct marketing purposes must provide, on request, the names and addresses of those third parties and the categories of information that was disclosed. The California law goes on to enumerate various exceptions to this requirement for businesses that include the appropriate information in their privacy policies and allow consumers to opt-out of the sharing of their information. As this law already applies to all businesses that have customers in California, it effectively means that it applies to all online businesses with a national presence. As this law already applies broadly to online businesses and provides effective means for consumers to access their data while restricting the burden of compliance a similar nationwide standard may be a good solution.

In sum, the PMA supports the FTC's desire to increase protections for consumer privacy however the PMA wishes to point out how important this issue is to the performance marketing industry and how implementation of the proposed privacy principals outlined in the FTC Staff Report would have a detrimental impact on our industry. The most effective means to provide consumers with greater privacy choices is to encourage and promote industry self-regulation and consumer education. The PMA urges the FTC to rethink the scope of the proposed principals and spend additional time researching and familiarizing itself with the types of consumer data that is collected, the legitimate and the seemingly endless ways in which that data is necessarily used.

The PMA welcomes questions from the FTC and is available to provide any further assistance that is needed.[6]

Sincerely,

Rebecca Madigan
Executive Director
Performance Marketing Association

[5] CA Civil Code Section 1798.83

[6] This comment was drafted by PMA Member Sarah de Diego, Esq. All questions may be directed to the PMA at 79 Daily Drive. #106, Camarillo, CA 93020, via telephone to 805.445.9700 or email to rebecca@performancemarketingassociation.com