Before the

FEDERAL TRADE COMMISSION

IN THE MATTER OF A PROPOSED PRIVACY FRAMEWORK

Project No: P095416

COMMENTS OF:

PROMOTION MARKETING ASSOCIATION, INC.
650 First Ave, Suite 2 SW
New York, NY 10016

Edward M. Kabak
Chief Legal Officer

Counsel of Record:
Marc S. Roth
La Toya C. Sutton
MANATT, PHELPS & PHILLIPS, LLP

Ronald R. Urbach
Gary A. Kibel
DAVIS & GILBERT LLP

COMMENTS OF THE PROMOTION MARKETING ASSOCIATION, INC. ON THE FEDERAL TRADE COMMISSION'S STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS
PROJECT NO. P095416

The Promotion Marketing Association, Inc. ("PMA") respectfully submits these Comments in response to the request by the Federal Trade Commission ("FTC" or "Commission") for public comments on the Commission's Preliminary Staff Report regarding the protection of consumer privacy. *See Request for Public Comment on the Federal Trade Commission's Preliminary Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, December 1, 2010 (FTC File No. P095416) ("Staff Report").

Established in 1911, the PMA is the premier not-for-profit organization and resource for research, education, and collaboration for marketing professionals. Representing the over $1 trillion integrated marketing industry, the organization is comprised of Fortune 500 companies, top marketing agencies, law firms, retailers, service providers and academia, representing thousands of brands worldwide. Championing the highest standards of excellence and recognition in the promotion and integrated marketing industry globally, the PMA's objective is to foster a better understanding of promotion and integrated marketing and its role in the overall marketing process.

I. Executive Summary

While the PMA supports the Commission's efforts to ensure that businesses take appropriate measures to protect consumer information and provide customers with choice as to how information about them is collected and used, certain provisions of the FTC's proposed framework, particularly its suggestion for a government mandated Do Not Track mechanism, are unnecessarily restrictive on the flow of information, and would be detrimental to both online businesses and consumers. Additionally, proposed regulation of commonly accepted practices, first party marketing, and data collection and retention limits may not sufficiently embrace future situations or be fully effective as privacy solutions. As explained in more detail below, the proposed framework could undercut industry efforts to develop its own consumer privacy safeguards that serve the needs of the industry, and instead purport to impose a universal solution

to the multifaceted problem of data security. PMA believes that industry efforts in providing consumers with greater transparency and ability to exercise control over how their information is collected and used should be given more time to gain greater public awareness and usage.

PMA notes that the FTC's report is intended to provide legislators and policy makers with a framework to consider when enacting laws or implementing policy. As such, the report and its conclusions will be seriously considered by those who are in a position to develop privacy laws and best practices. PMA therefore believes that care should be taken not to make unwarranted assumptions about consumer perceptions and desires.

II. Privacy Policies Provide Useful Information to Consumers

The PMA agrees with the FTC's conclusion that consumers should have greater access to the information collected about them. To that end, responsible marketers should, and do, provide consumers with information about how their information may be collected and used, most commonly through the posting of a privacy policy on a website. These policies disclose important information to consumers that enable them to make informed decisions about whether they will provide information to that website operator. The PMA believes the FTC's observation of these policies as doing a "poor job of informing consumers about companies' data practices or disclosing changes to their practices"[1] and "often opaque, lack uniformity, and are too long and difficult to navigate"[2] to be unwarranted if considered categorically, since these policies serve as tangible references for consumers regarding the manner in which their information is being used. While individual companies should review their policies to ensure they are accurately and efficiently communicating with the consumer, the idea that these policies are categorically ineffective is unfair to those companies that currently work diligently to secure informed consumer choice.

The backbone of FTC's proposed framework is "privacy by design" – the concept of tailoring privacy practices to meet the individual needs of a particular company as it serves their consumers. Such a principle can not be achieved if the company is simultaneously forced to adopt a standardized policy that may not address the particular needs of that business or gloss over important differences in data practices between companies. The idea of creating

[1] Staff Report, page 69.
[2] Staff Report, page 70.

standardized policies across industries, each of which may use consumer information in significantly different ways, is impractical, if not impossible.

III. Industry Self-Regulation Has Not Been Given Fair a Chance

The FTC claims in its Staff Report that it has repeatedly called for additional efforts from industry to enhance the data security tools available to consumers. This coalition, called the Digital Advertising Alliance, developed guidelines to address that call. In 2009, a group of the nation's largest media and marketing associations came together to develop cross-industry guidelines, called the *Self-Regulatory Principles for Online Behavioral Advertising*. The seven core principles of those guidelines, many of which mirror the core principles outlined in the FTC's Proposed Framework, formed the basis for a self-regulatory program announced in October 2010, the Self-Regulatory Program for Online Behavioral Advertising ("Program"). This Program is intended to apply consumer-friendly standards to online behavioral advertising across the Internet. As the FTC is aware, the companies participating in the program display a particular icon in their online advertisement, and when consumers click on the icon, they are presented with a description of what information was used to display that advertisement, as well as a number of options, enabling them to opt out of being tracked for the purposes of online marketing. Significantly, compliance is enforced by the Better Business Bureau, a leader in advocating for consumer friendly business practices.

As the FTC develops its national privacy framework, the PMA recommends that the FTC refrain from implementing a government mandated behavioral advertising mechanism until the industry's Program has had an adequate opportunity for success. In its Staff Report, the FTC dismissively notes this huge undertaking to self-regulate within the industry, and then goes on to state that "an effective mechanism has yet to be implemented on an industry-wide basis."[3] Considering that the Staff Report was published barely two months after the Program was announced, it is not surprising that the Commission would draw such a conclusion. The industry has simply not had the time and opportunities it needs to properly advertise and implement this Program. The fact that this Program was developed by a coalition of trade groups, representing over 5,000 corporations, should speak to the potential for far-reaching, industry-wide implementation of this Program, if it is given the time needed for companies and consumers to

[3] Staff Report, page 64.

learn more about the choices and tools it makes available. As stated in the Staff Report, "the FTC repeatedly has called on stakeholders to create better tools to allow consumers to control the collection and use of their online browsing data."[4] The Digital Advertising Alliance has done exactly what the FTC has asked of the industry: develop an effective tool and invest in the education of its members regarding the importance of safeguarding the private and sensitive information of online consumers.

Many of the problems with self-regulation articulated in the Staff Report – that industry efforts have fallen short, that consumers are unaware of existing mechanisms, that existing mechanisms may not make clear the scope of choices being offered, and that consumers may not understand the technical limitations of existing mechanisms – have all, or with time at least, can all be addressed through the Digital Advertising Alliance's existing Program. Increased awareness and education are necessary components of any effort to provide new consumer choices and change privacy controls. These obstacles are not unique to self regulatory efforts – indeed the government will face the same problems should it chose to implement its own Do Not Track mechanism – and can be overcome with time and effort.

Furthermore, self-regulation is the industry's best option in terms of allowing technological growth. The legal and regulatory system is ill-equipped to keep up with the ever evolving Internet landscape. Self-regulation allows those who best understand the needs and capabilities of the online marketing industry to revise and implement policy changes as quickly as those revisions can be distributed through the Internet. For these reasons, should the FTC adopt a privacy framework that includes Do Not Track, it should keep in mind the urgent need for an adaptable and flexible framework, one capable of addressing unforeseen issues and as yet unimagined consumer services.

IV. Proposed Do Not Track Mechanism Would Deprive Both Businesses and Consumers

Besides the existence of a self-regulatory program that fulfills the needs outlined in the Staff Report, the proposed Do Not Track mechanism,we submit, goes much further than necessary to protect consumer privacy data – essentially throwing out the baby with the bathwater. While the Commission describes its proposed mechanism as a "more uniform and

[4] Staff Report, page 63.

comprehensive consumer choice mechanism," the idea is simply a suggestion that a one-size-fits-all program be imposed on an industry that is extremely varied, from the products and services it offers to the level of sophistication of its end users.

The implementation of such a mechanism would likely increase the cost of advertising by reducing the availability of behavioral advertising as a valid marketing tool, harming both the consumer and industry members. Increased advertising cost means less helpful information will be conveyed to the consumer. It also means online marketers will be restricted from using a manner of presenting consumers with relevant messages that has proven to be a critical tool for reaching new customers.

While the suggestion of such a mechanism may sound desirable in theory, in practice, it is not clear that the creation of a mechanism that will accomplish all of the things the FTC hopes it will is even technologically feasible. What is clear is that such a mechanism has the capability of making consumers' privacy choices static, a state unsuited for the fluid exchange of information, ideas, and goods that has cultivated the online marketplace as a worthwhile destination for both consumers and businesses. Additional safeguards are certainly needed; however, a static choice across the board could deprive consumers of the opportunity to receive content and information in ways that are not yet available. The PMA recommends that any opt out or opt in mechanism that may be implemented, whether developed by the FTC or through industry self regulation, must be able to adapt to the constantly changing Internet environment, to ensure that technological advancement is not stifled.

Additionally, it seems that the mechanism contemplated in the Staff Report would force consumers to make categorical decisions regarding access to their private information. This too would stifle innovation and limit the useful information available to consumers. Rather than adopting a mechanism that requires wholesale privacy decisions, the PMA urges the FTC to allow consumers to retain the ability to make informed, granular choices about their data sharing practices.

V. Consumer Choice and "Commonly Accepted" Practices

The PMA agrees that there are often times when it is not necessary to obtain a new or separate consent from a consumer to engage in certain practices that are commonplace or

reasonably expected by the consumer. The FTC has asked whether the proposed list of "commonly accepted practices" in the Staff Report is too broad or too narrow.

The issue is not whether the proposed list is too broad or too narrow, but whether it is possible for the FTC to set forth a comprehensive list at all. A consumer's expectation of privacy is an evolving standard. What is unexpected today may seem commonplace in just a short time period of time given the rapid changes in technology and services.

Furthermore, the proposed list of commonly accepted practices does not recognize that there may be peculiarities specific to different industries. What is commonplace in one industry may seem invasive in another. For example, a data sharing practice that may seem commonplace for a publishing company may seem bothersome to users of a social networking service that is targeted towards a particular vertical. At a minimum, the idea of commonly accepted practices should be industry and technology agnostic. Further, query whether federal regulators should at this juncture purport to determine what is commonly accepted to all consumers. The FTC, we submit, should in any event eschew rigid standards that fail to recognize the quick pace at which technology is advancing and being adopted by the public.

VI. First-Party Marketing

The proposal in the Staff Report that companies only collect data from a consumer with whom a company directly interacts would require a sea change in the way many companies collect data, share data, and provide disclosures today to consumers. In many industries, companies share data with their corporate affiliates who offer similar and beneficial products and services. These practices are often disclosed in a company's privacy policy. If the FTC were to adopt the position that sharing with affiliates could only be accomplished upon obtaining the consent of the consumer, then countless companies would need to revise their privacy policies and practices to meet this new standard. Consumers would be inundated with requests to consent to practices that had already been in place and disclosed in a privacy policy. It would also turn a perceived advantage of having a corporate family with many related and integrated affiliates into an impediment. An opt out approach to affiliate sharing has been and should be the accepted standard, provided that the company in question has made both the disclosure regarding affiliate sharing and the ease of opting out readily available to the consumer.

VII. Transparency and Improved Privacy Notices

For years the FTC has encouraged companies to disclose their privacy practices in privacy policies and to make those privacy policies readily and easily available to consumers. However, the Staff Report dismisses the effectiveness of privacy policies and espouses new disclosures separate and apart from the privacy policy. While the FTC's intent is clearly to ensure that consumers are provided with the most critical information, there is a concern that this proposed approach could have the reverse effect. If a company is required to provide individual notifications to comply with guidelines from the FTC, other federal agencies, and self-regulatory bodies, while at the same time complying with new legislation on both the federal and state levels, the number of notices a company might be obligated to provide could result in information overload to consumers. Consumers will then likely tune out the barrage of notifications. The result could potentially be less consumer awareness of a company's data collection and use practices. One's ability to exercise choice is directly related to the ease in which the information necessary to evaluate that choice is provided.

VIII. Data Collection Limits, Data Retention Periods and Enhancement

The PMA supports the principle that unnecessary data collection should be avoided by all companies. Companies do collect data that they intend to use now or may have a need for in the future. The proposed standard in the Staff Report to limit data collection to "only the information needed to fulfill a specific legitimate business need" seems to discount this latter use. It is not always the case that a company can determine the specific business purpose at the moment of data collection. A company may collect related data under the belief that it might have value at a later date, and the company may want to simplify the data collection process for consumers by requesting the data once as opposed to continually going back to consumers each time they want to collect a new piece of data for a newly proposed use. The standard should recognize that collection may include data which a company currently needs or may reasonable need in the future.

The PMA also supports the idea that data should only be retained for as long as there is a legitimate business purpose. However, this should be adopted as a flexible principle rather than a regulatory requirement. It could be detrimental to businesses and consumers to prescribe specific retention periods. The reasons for a company to retain data, and for consumers to want a company to retain their data, are very fact-specific. Tying retention periods to a legitimate

business purpose may not always be appropriate if the retention is for the benefit of the consumer who wishes to have their historical data available or, as noted above, a new use for the data might arise in the future. Rather than prescribe specific retention periods, the industry and the FTC should continue to promote sound data security practices so that all data, regardless of the period of time for which it is kept, remains secure.