



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

**COMMENTS
OF THE
DIRECT MARKETING ASSOCIATION, INC.
ON
ONLINE BEHAVIORAL ADVERTISING
PROPOSED PRINCIPLES**

Jerry Cerasale
Senior Vice President, Government Affairs
Direct Marketing Association
1615 L Street, NW Suite 1100
Washington, D.C. 20036
202/861-2423

Counsel:
Stuart P. Ingis
Alisa M. Bergman
Venable LLP
575 7th Street, NW
Washington, DC 20004
202/344-4613

April 11, 2008

Executive Summary

Behavioral advertising is helping fuel the continued growth of rich online content choices, allowing for more effective advertising that benefits both consumers and businesses. The Direct Marketing Association (“DMA”) has been at the forefront of self-regulation regarding offline and online privacy issues for decades, and many of the issues being considered in connection with the Federal Trade Commission’s proposed online behavioral advertising self-regulatory principles¹ already are the subject of our extensive self-regulatory efforts.

Adoption of any potential principles in this area should be carefully considered in the context of the current self-regulatory and technological landscape to ensure that they address any shortcomings in these areas—and real harms or concerns—so as not to unnecessarily foreclose important consumer benefits and impede the continued tremendous growth of the online medium.

DMA believes that it is important to evaluate the following issues in connection with the Commission’s proposed principles:

- **Scope.** The definition of behavioral advertising is not limited in scope and potentially could be interpreted to apply to any information collected online that is used in the delivery of advertising, without regard to whether the information is, or even could become, personally identifiable. This would represent a marked shift from prior approaches to privacy protection.

DMA also believes that any principles should exclude the following three categories, which already are addressed through current effective self-regulatory frameworks: (A) information entered by consumers at the Web site or online service; (B) information practices at a single Web site or within a family of sites under common ownership or control; and (C) context-based ads.

- **Transparency and Control.** DMA has worked closely with our members for years to develop and foster transparency through robust privacy policy disclosures. DMA is evaluating specific language that describes behavioral advertising, which companies could include in their privacy notices to further transparency to consumers.

As reflected in our guidelines, any consumer choice principle should be flexible and able to be tailored depending on factors such as the nature of the information and the types of uses thereof, as well as the mechanisms for honoring consumer choices. DMA believes that the proposed control principle exceeds current self-regulatory frameworks regarding consumer control/choice because it requires choice for collection of information used for behavioral advertising.

¹ Online Behavioral Advertising—Moving the Discussion Forward to Possible Self-Regulatory Principles: Statement of the Bureau of Consumer Protection Proposing Governing Principles For Online Behavioral Advertising and Requesting Comment, Federal Trade Commission, Dec. 20, 2007.

- **Reasonable Security, and Limited Data Retention, for Consumer Data.** DMA believes that the security measures necessary to provide sufficient data protection will vary based on the nature of the information being secured and the potential risk.

In addition, consistent with Commission actions in the area of data security, data retention issues should be considered as part of a reasonable data security program, rather than being separated as the Commission proposes in connection with this principle.

- **Affirmative Express Consent for Material Changes to Existing Privacy Promises.** DMA's many years of experience with this issue have demonstrated that adoption of a flexible principle concerning notification of changes, which takes into account the type of notice and/or choice needed depending on the circumstances, is the best approach to protecting consumers and ensuring that they receive relevant information.

Consistent with current best practices and certain legal requirements, companies should set forth the methods by which they will notify consumers about changes in their privacy policies, and then determine what types of notice and/or choices are appropriate under the circumstances. Moreover, at a minimum, this type of principle should be focused on material changes with respect to narrower practices affecting third-party uses of personal information for behavioral advertising, and not all privacy practices.

- **“Express Consent” or a Prohibition on Use of “Sensitive Data” for Behavioral Advertising.** The current regulatory and self-regulatory standards that govern the types of notice and consent required for use of sensitive data, and the factors to consider in connection with the appropriateness of sending advertising based on such data, are working well. Many industry sectors and types of data that traditionally are considered sensitive already are the subject of extensive regulation.

About the Direct Marketing Association

The Direct Marketing Association, Inc. (“DMA”) (www.the-dma.org) is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. DMA advocates industry standards for responsible marketing, promotes relevance as the key to reaching consumers with desirable offers, and provides cutting-edge research, education, and networking opportunities to improve results throughout the end-to-end direct marketing process. Founded in 1917, DMA today represents more than 3,600 companies from dozens of vertical industries in the U.S. and 50 other nations, including a majority of the Fortune 100 companies, as well as nonprofit organizations. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them.

DMA's leadership also extends into the Internet and electronic commerce areas through the companies that are members of DMA's Internet Alliance. DMA member companies, given

their track record in delivering high-quality goods and services to consumers, have a major stake in the success of online commerce. The healthy, continued development of electronic commerce depends on consumer trust.

DMA has long been a leader in establishing comprehensive self-regulatory guidelines for its members on important issues related to privacy and e-commerce. DMA and its member companies have a major stake in the success of electronic commerce and Internet marketing and advertising, and are among those benefiting from its growth. Our members understand that their success on the Internet is dependent on consumers' confidence in the online medium, and support efforts that enrich a user's experience while fostering consumer trust in online channels. In our experience, industry guidelines are the most effective way to address the continuously changing technological landscape. Such guidelines are flexible and adaptable, in a timely manner, to changes in markets, business practices, and advances in technology.

In looking to adopt any new self-regulatory framework or best practices, it is important to understand the current foundations on which we are building and then determine whether there are any changed circumstances or new and emerging issues that would warrant updates to current guidelines or the adoption of new guidelines. As detailed in these comments, DMA has been at the forefront of self-regulation regarding offline and online privacy issues for decades, and many of the issues being considered in connection with the proposed online behavioral advertising principles already are the subject of extensive self-regulatory efforts. Therefore, it is important to review the Commission's proposal in the context of these broader self-regulatory efforts and the online environment in which any such principles would operate.

To this end, we set forth below (1) a summary of the benefits of behavioral advertising online, (2) a discussion about the breadth and scope of the Commission's proposed online behavioral advertising self-regulatory principles, an understanding of which will be important to fully assessing their potential implications; and (3) a comparison of each of the Commission's proposed principles with the current, corresponding DMA guideline that addresses that issue. We also set forth an analysis of the practical implications and specific concerns raised by each principle, as well as discuss some of the types of technological tools available to effectuate transparency and consumer choices regarding uses of information for behavioral advertising.

To further inform this discussion and provide the broader context and state of the direct marketing industry's best privacy practices, we have included as Appendix A an extensive discussion of DMA's self-regulatory efforts, including descriptions of:

- several DMA programs which are essential to protecting privacy online that are industry tools and common best practices;
- DMA's self-regulatory *Guidelines for Ethical Business Practice*, which protect consumers' privacy by addressing complaints concerning practices contrary to the *Guidelines*;
- several technology solutions supported by DMA that help consumers choose and enforce how their personal data is collected and used by businesses; and

- important DMA public education initiatives that help the government, businesses, and, most importantly, consumers better understand the information collection process.

I. Benefits of Behavioral Advertising

The focus on behavioral advertising is an important one in that online advertising is helping fuel the continued growth of rich online content choices. Behavioral advertising allows for more effective advertising, which benefits both consumers and businesses. Consumers benefit by receiving offers and information about products and services that are of value to them; businesses also benefit in that they can focus advertising resources to better ensure that their ads are not seen by consumers who have no interest in their products and services. Importantly for consumers, behavioral advertising helps underwrite cost-free offerings of content or content at far lower costs than otherwise would be possible. Since such advertising is more effective, the revenues therefrom can subsidize these free offerings, obviating the need for access or subscription charges in many instances. Moreover, behavioral advertising promotes competition and innovation by, for example, helping maintain the low barriers to entry that have played a fundamental role in the growth of the online medium. Thus, any potential principles or new practices in this area should be carefully considered prior to adoption to ensure that they are addressing real harms or concerns so as not to unnecessarily foreclose these important consumer benefits and the continued tremendous growth of the medium.

II. The Scope of Activities that Constitute “Behavioral Advertising” Should Focus on Instances Where Further Self-Regulatory Efforts May Be Appropriate or Beneficial to Consumers

DMA and its member companies have long recognized that promoting best practices through effective self-regulation enhances online trust and confidence. Addressing potential concerns about emerging practices and curbing potential abuses through self-regulation is the best approach to ensuring that the online medium can continue to grow and thrive. To this end, our guidelines are flexible, organic documents that can respond quickly to changes in technologies, new business models, and the online environment. We regularly evaluate areas in which self-regulation is appropriate, and currently are evaluating our guidelines in connection with the Commission’s proposed principles on behavioral advertising. In addition, we are working in a coalition with other industry associations to collectively evaluate best practices in this space. *See* “Associations Letter” in this proceeding, to which DMA is a signatory, outlining some of these efforts.

As our many years of experience demonstrate, critical to any discussion or evaluation of these or any proposed principles is a true understanding of any particular business practice and an evaluation of whether there exist concerns that may warrant additional self-regulation. Indeed, an important theme articulated at the Commission’s recent behavioral advertising workshop was the need for a determination of potential harm from any of the practices being

discussed. *See, e.g.,* Roundtable Discussion of Data Collection, Use, and Protection during the FTC Town Hall entitled “eBehavioral Advertising: Tracking, Targeting, & Technology” (Nov. 1, 2007).

The Commission’s proposed self-regulatory principles apply to online “behavioral advertising,” which is defined as:

the 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.

Such a definition is not exhaustive or limited in scope and, therefore, potentially could be interpreted to apply to any type of information collected online used in the delivery of advertising, without regard to whether the information is, or even could become, personally identifiable information. Such an approach would be a marked shift from prior approaches to privacy protection.

The distinction between identifiable and non-identifiable data in privacy laws and self-regulatory frameworks underscores the fact that non-identifiable data does not raise privacy issues per se. Indeed, many of the U.S. privacy frameworks recognize the need to use, and in fact encourage the use of, non-identifiable data for important and useful purposes, such as to help with research for health longitudinal studies, to help ensure the continued availability of meaningful children’s content online, and to improve the quality of customer products, services, and offerings.² Thus, consistent with all other privacy frameworks, the focus of any principles should be on practices related to personally identifiable information.

Moreover, the proposed definition of behavioral advertising could be read to include, for example, any type of information entered by the consumer in a commercial transaction. Application of certain of the principles to such information does not seem appropriate or practical. We, therefore, believe that it will be important to identify any specific practices at which these principles are targeted and focus the scope of this definition accordingly.

Specifically, DMA believes that the scope of activities that fall within the ambit of behavioral advertising should be more clearly delineated and, at a minimum, should exclude the following three categories, which already are addressed through current effective self-regulatory frameworks: (A) information entered by consumers at the Web site or online service with which they are interacting; (B) information practices occurring at a single Web site or within a family of sites with common ownership or control, as compared to practices across a network of unrelated sites; and (C) context-based ads. We discuss each of these issues in turn below.

² *See, e.g., Frequently Asked Questions about the Children’s Online Privacy Protection Rule*, FAQ # 38, Federal Trade Commission: “. . . Many sites have found creative ways to provide rich content for children, while complying with COPPA. For example, sites may choose to:

- Offer activities that do not require the collection or disclosure of personal information;
- Use screen names or other anonymous techniques to personalize the site; . . .”

A. Self-Entered Consumer Information Already is Subject to Extensive Self-Regulation

DMA believes that personally identifiable information that a consumer enters is an area effectively covered under existing self-regulation. As described in more detail below in Section II A, under our self-regulatory approach, online companies post privacy policies that detail the types of personally identifiable information collected, how its used, and consumer choices with respect to use. When consumers register at a Web site or with an online service, provide an e-mail address to sign up for a newsletter, or engage in a transaction, they are consciously providing certain information to Web sites with which they have chosen to interact. Consumers have the ability to read the privacy policy of the site or service to understand how such information will be used and their choices regarding such use. Recognizing that understanding the “rules of the road” is important to furthering consumer choice, DMA member companies are continuing to explore ways to make privacy policies even more user-friendly through the use of new technologies, standardization of terms, and other means to make policies easier to read and understand.

Companies not only are subject to legal constraints on their use of information in the form of deceptive practices actions for not following their stated practices set forth in their privacy policies, but also are subject to sanctions through participation in self-regulatory programs, such as those of DMA. Additionally, there are reputational constraints that will help ensure that privacy commitments are honored. For these reasons, we believe that this is an area where there already exist significant self-regulatory efforts.

B. Practices Occurring at a Single Web Site or an Affiliated Site Do Not Raise Unique Issues that Require Additional Self-Regulation

DMA believes that the definition of behavioral advertising should not apply to practices occurring at a single Web site or family of sites under common ownership or control. Just as in the offline world where, for example, the salesclerk at a retail store checkout counter may make helpful recommendations about particular ties to match a shirt, or alternative shirts to consider prior to making the purchase, consumers appreciate and have come to expect the Web sites they visit to show them advertising and otherwise make recommendations based on prior purchases or pages viewed. Some of the most successful sites on the Web have built their business practices around such a business model. Among the most prominent examples are Web sites that offer personalized recommendations for books, electronics, music, and movies to consumers, suggesting similar or related products or services in which they may be interested based on prior purchases or pages viewed.

In addition, these Web sites provide consumers with useful suggestions regarding what others who have purchased the same or similar product also viewed or purchased when choosing the particular product in which they are interested, helping facilitate useful price and quality comparisons and the purchase of complimentary products. For example, if a consumer searches for a digital camera online, he may be provided with information regarding the types of accessories that other consumers have purchased. Similarly, the Web site may make recommendations regarding additional cameras in his particular price range or with comparable

features viewed by other consumers to enable invaluable comparisons. Given that the consumer has taken steps to interact with a particular Web site and has had the opportunity to read the site's privacy policy, which would address data collection and use and choices regarding marketing, as well as the ability to choose not to do business with a site, it does not seem that additional self-regulation would be necessary for such practices.

In addition, conduct occurring at a single Web site is in some ways analogous to the concept of an "established business relationship" concept embodied in various marketing regulatory frameworks, such as the telemarketing and fax contexts, in which consumers have decided to have a relationship with a company and, thus, have a different expectation and relationship with such companies.³ Having chosen to interact with a particular Web site, consumers are expressing a comfort level with the Web site's reputation and a level of trust in connection with the site's collection and use of their data. Similarly, self-regulatory frameworks, like that of DMA, always have recognized the increased expectations and value tied to companies' marketing to their own customers.

Another related concept is the treatment of behavioral advertising practices in connection with a family of Web sites under common ownership or control. Marketing by companies under common ownership or control benefits consumers by enabling them to receive wider varieties of product and service offerings; it also enables unique partnering arrangements, which can result in significant cost savings to consumers. Moreover, the additional advertising and marketing enabled by affiliated entities fosters competition not only among merchants but among advertisers and affiliates as well, which helps keep consumer prices low. In addition, this approach to marketing enables lower barriers to entry for new product and service offerings, which also promotes competition. Consumers have come to expect and want data sharing with affiliated Web sites to enable them to take advantage of additional marketing opportunities. This approach has been accepted in regulatory frameworks, such as that of the Gramm-Leach Bliley Act ("GLB"), where covered financial institutions provide consumers with notice of affiliate sharing practices regarding sensitive financial information.

As these examples highlight, there exist extensive regulatory and self-regulatory efforts regarding practices occurring at a particular Web site and regarding affiliate sharing that work well, providing significant benefits to consumers and the businesses that serve them. Our members do not receive a level of complaints that suggests harm or concern about such practices by their customers. There is, thus, no demonstrated need, in the experience of our members, for adjustments to the current frameworks or approaches in the form of additional self-regulation.

C. Additional Self-Regulation is Not Needed for Context-Based Ad Delivery

DMA also does not believe that additional self-regulation is needed in connection with "context-based ads," where the Web site's context is used to determine the types of advertisements to be delivered or displayed. This type of approach to advertising has been used in the offline world in connection with television, newspaper, and radio programs, has withstood the test of time, and has proven successful. By way of example, if a magazine or Web site is

³ See, e.g., Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227; Junk Fax Prevention Act of 2005, 47 U.S.C. § 227.

focused on music, the ads on the site or in the magazine may provide information about upcoming concerts in a particular area or album release dates. We are not aware of concerns about this approach in the online space that would merit new self-regulatory standards in connection with these practices. Indeed, the experience of our member companies has been that consumers appreciate and want this type of ad tailoring and are not surprised, for example, to be offered tennis rackets when visiting the Web site of a magazine focused on tennis interests. Thus, we do not believe that additional self-regulation is necessary for context-based ads.

III. Principle 1—Transparency and Consumer Control

As the following comparison of the Commission’s proposed principles with our current guidelines demonstrates, transparency and consumer choice have always been bedrocks of DMA’s privacy guidelines. We have worked closely with our members to develop and foster transparency through robust privacy policy disclosures.

A. Transparency

The FTC’s proposed principle states:

Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers’ activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers’ interests, and (2) consumers can choose whether or not to have their information collected for such purpose.

The requirements of DMA’s *Online Marketing Guidelines*⁴ on this issue are as follows:

If your organization operates an online site, you should make information practices available to visitors in a prominent place on your Web site’s home page or in a place that is easily accessible from the home page. The notice about information practices on your Web site should be easy to find, read, and understand so that a visitor is able to comprehend the scope of the notice. The notice should be available prior to or at the time personally identifiable information is collected.

If the organization collects personally identifiable information from visitors, the notice should include:

- *The nature of personally identifiable information collected about individual visitors online, and the types of uses you make of such information, including marketing uses that you may make of that information.*

⁴ Available at <http://www.the-dma.org/guidelines/onlineguidelines.shtml>.

- *Whether you transfer personally identifiable information to third parties for use by them for their own marketing and the mechanism by which the visitor can exercise choice not to have such information transferred.*
- *Whether personally identifiable information is collected by, used by or transferred to agents (entities working on your behalf) as part of the business activities related to the visitor’s actions on the site, including to fulfill orders or to provide information or requested services.*
- *Whether you use cookies or other passive means of data collection, and whether such data collected are for internal purposes or transferred to third parties for marketing purposes.*
- *If you knowingly permit network advertisers to collect information on their own behalf or on behalf of their clients on your Web site, you should also provide notice of the network advertisers that collect information from your site and a mechanism by which a visitor can find those network advertisers to obtain their privacy statements and to exercise the choice of not having such information collected. (Network advertisers are third parties that attempt to target online advertising and make it more relevant to visitors based on Web traffic information collected over time across Web sites of others.)⁵*

As evidenced by the above guidelines, DMA members are fully committed to transparency and ensuring that consumers are provided with information regarding online practices to enable them to make informed decisions about how information collected about them will be used. As the Commission recognizes in citing its *Dot Com Disclosures* publication in connection with this proposed principle,⁶ we believe that it is important to factor context into the contours of a transparency principle, striking the right balance between ensuring that consumers receive notice of practices through meaningful mechanisms rather than those that could be burdensome or otherwise encumber the online process. Different types of notices may be appropriate in different scenarios. In addition, as the Commission also recognizes in *Dot Com Disclosures*, technologies like hyperlinks,⁷ frames, and pop-ups could be useful in displaying important information.

Further evidencing our strong commitment to helping members address transparency requirements under our guidelines, DMA offers its members tools in the form of “privacy policy

⁵ As a result of this Guideline, our members who also use the services of network advertising companies implicitly have adopted this portion of the Network Advertising Initiative’s (“NAI”) Self-Regulatory principles. DMA has coordinated with NAI and other self-regulatory organizations to help ensure that companies are providing transparency regarding these practices.

⁶ See *Dot Com Disclosures—Information about Online Advertising*, available at <http://www.ftc.gov/bcp/online/pubs/buspubs/dotcom/index.pdf>.

⁷ See *id.* at 8. “Hyperlinked disclosures may be particularly useful if the disclosure is lengthy or if it needs to be repeated (because of multiple triggers, for example).”

generators” to assist companies in drafting the various types of privacy notices required under different regulatory frameworks (*e.g.*, requirements under children’s or financial privacy laws), as well as a generator to help companies comply with our self-regulatory guidelines and practices.⁸ In addition, DMA member companies always are actively looking at ways to improve the content of notices and the mechanisms for providing them as they learn from their interactions with consumers.

As the efforts outlined above demonstrate, DMA supports—and our members are committed to—transparency. DMA also is evaluating specific language that describes behavioral advertising, which companies could include in their privacy notices to further transparency to consumers. Such language would be based upon the transparency concepts set out in the Commission’s proposed principle.

B. Any Consumer Control Principle Must Be Flexible so that it Could Be Tailored Depending on Such Factors as the Nature of the Information and the Types of Uses

The Commission’s proposed principle regarding consumer control would require Web sites that collect data for behavioral advertising to provide consumers with choice, through a “clear, easy-to-use, and accessible” method, regarding whether to have their information collected for such purposes.

Providing consumers with choices is a fundamental tenet of direct marketing best practices and, accordingly, a bedrock of the DMA guidelines. True to this approach, DMA continues to work with its members to determine what types of consumer empowerment are appropriate to address the evolving needs of consumers in today’s marketplace. We have worked hard to help educate consumers regarding our member companies’ commitment to choices through adoption of consumer education and awareness campaigns. Notable among these efforts is our consumer information site, the DMAChoice Web site, which is designed specifically for consumers, providing information and tips about a wide range of topics, including marketing preference services. *See, e.g.*, <http://www.dmachoice.org/consumerassistance.php>

As reflected in our guidelines, requirements to provide consumer choice afford both flexibility to address considerations such as the types of information being collected and the potential uses thereof, as well as the mechanisms for honoring consumer choices, which are a function of such factors as the unique considerations of the medium and available technology. We believe that these concepts should be at the foundation of any self-regulatory framework governing consumer control. However, in order for choice to be effective, it does not need to occur at each and every point that data is collected or used. Choice at every instance of collection or use is impractical. For example, choice to all collection of information that will be used for marketing purposes does not make sense when information is collected for multiple purposes. This is particularly true when some of the purposes are essential to the proper functioning of the Web site.

⁸ *See, e.g.*, <http://www.the-dma.org/privacy/childrensppg.shtml> (Children’s Privacy Policy Generator), <http://www.the-dma.org/privacy/creating.shtml> (general audience Web site Privacy Policy Generator).

Regarding honoring consumer preferences, DMA’s guidelines require member companies to afford consumers with choices not to have personally identifiable information collected online used for marketing purposes with respect to the company’s own marketing, as well as to opt out of the marketing process regarding the rental, sale, or exchange of data about them. In addition, the DMA guidelines require companies to use the applicable DMA Preference Service name-removal list in connection with prospecting lists. Specifically, Article 31 of our *Guidelines for Ethical Business Practice (“Guidelines”)*⁹ provides in relevant part:

- *A marketer should provide existing and prospective customers with notice of an opportunity to modify or eliminate direct marketing communications to be received from that company. This guideline applies to senders of marketing offers.*

In addition, as noted above, Article 38 provides in relevant part:

If your organization collects personally identifiable information from visitors, your notice should include: . . .

- *Whether you transfer personally identifiable information to third parties for use by them for their own marketing and the mechanism by which the visitor can exercise choice not to have such information transferred*

Article 38 goes on to state:

Honoring Choice

You should honor a visitor’s choice regarding use and transfer of personally identifiable information made in accordance with your stated policy. If you have promised to honor the visitor’s choice for a specific time period, and if that time period subsequently expires, then you should provide that visitor with a new notice and choice. You should provide choices of opting out online. You may also offer opt-out options by mail or telephone.

The proposed control principle would far exceed current self-regulatory frameworks regarding consumer control/choice, requiring choice for collection of information used for behavioral advertising.

Moreover, evaluation of this proposal in context and coupled with the Commission’s proposed definition of behavioral advertising which, as discussed above, is not tied to personally identifiable information, further underscores the fundamental nature of this type of change. There are many instances in which non-identifiable data is collected at Web sites and used for purposes other than delivery of advertising that are critical to the proper functioning of the site,

⁹ Available at <http://www.the-dma.org/guidelines/ethicalguidelines.shtml>

such as to deliver the requested content, and determine Web browser views, which should be carefully considered.

In addition, technological tools are available to assist consumers in expressing their choices with respect to collection of information. For example, there are a number of ways for consumers to use existing technology, such as browser settings to limit the use of cookies, as well as to anonymously browse the Internet.

IV. Principle 2—Reasonable Security, and Limited Data Retention, for Consumer Data

Under the Commission’s proposed principle, companies that collect and/or store consumer data for behavioral advertising purposes should provide reasonable security for that data based on the sensitivity of the data, the nature of the company’s business operations, the types of risks that a company faces, and the reasonable protections available to the company. Moreover, the Commission’s proposed principle states that “[c]ompanies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.”

DMA’s *Online Marketing Guidelines* state as follows:

Your organization should use security technologies and methods to guard against unauthorized access, alteration, or dissemination of personally identifiable information during transfer and storage. Your procedures should require that employees and agents of your organization who have access to personally identifiable information use and disclose that information only in a lawful and authorized manner.

In addition, Article 37 of DMA’s *Guidelines for Ethical Business Practice* provides:

The protection of personally identifiable information is the responsibility of all marketers. Therefore, marketing companies should assume the following responsibilities to provide secure transactions for consumers and to protect databases containing consumers’ personally identifiable information against unauthorized access, alteration, or dissemination of data:

- *Marketers should establish information security policies and practices that assure the uninterrupted security of information systems.*
- *Marketers should create and implement staff policies, procedures, training, and responsiveness measures to protect personally identifiable information handled in the everyday performance of duties.*

- *Marketers should employ and routinely reassess protective physical safeguards and technological measures in support of information security policies.*
- *Marketers should inform all business partners and service providers that handle personally identifiable information of their responsibility to ensure that their policies, procedures, and practices maintain a level of security consistent with the marketer’s applicable information security policies.*

DMA agrees with the Commission that the security measures necessary to provide sufficient protection will vary based on the nature of the information being secured and the potential risk presented by the particular company practice. At a minimum, to present any risk, the data at issue would need to be personally identifiable—it would be difficult to justify imposing such obligations in connection with non-personally identifiable information.

However, consistent with Commission actions in the area of data security, data retention issues should be considered as part of a reasonable data security program, rather than being separated as the Commission proposes in connection with this principle. For example, in *In re BJ’s Wholesale Club* and *In re Life is Good*, the Commission considered the reasonableness of the data retention practices at issue in light of the totality of the measures deployed to protect personally identifiable consumer information against unreasonable access.¹⁰ Thus, data retention issues should be considered under a reasonableness standard, rather than as measured by legitimate business or law enforcement needs as proposed. Legitimate business and law enforcement needs are important characteristics of reasonableness, but there also are other factors that may be relevant. Similarly, some practices within these categories may be “reasonable,” while others may not be.

V. Principle 3—Affirmative Express Consent for Material Changes to Existing Privacy Promises

Under the Commission’s proposed principle concerning material changes to privacy policies, companies would need to obtain affirmative express consent from affected consumers prior to using data in a way that is materially different from the promises that they made when collecting the data. As discussed below, we believe that a general application of this approach in all contexts does not appropriately balance the various factors that should be considered in determining what type of notice and/or choice mechanism is appropriate.

There currently are strong self-regulatory frameworks in place to address the types of notice and/or consent appropriate for informing consumers regarding material changes to existing privacy promises. Such principles have the benefit of years of experience in connection with new and emerging business models and practices, particularly in the wake of the dot.com boom and changed circumstances in the online world. These standards and best practices are

¹⁰ *In the Matter of BJ’s Wholesale Club, Inc.*, File No. 042 3160; *In the Matter of Life is good, Inc., a corporation, and Life is good Retail, Inc., a corporation*, FTC Matter No. 072-3046.

working well, and provide ample guidance to companies regarding how best to address these issues when they arise. Thus, DMA does not believe additional self-regulation in this area is needed.

Consistent with current best practices and certain legal requirements, companies should set forth the methods by which they will notify consumers about changes in their privacy policies, and then determine what types of notice and/or choices are appropriate under the circumstances. Moreover, at a minimum, this type of principle should be focused on material changes with respect to narrower practices affecting third-party uses of personal information for behavioral advertising and not all privacy practices.

Factors such as the following should be weighed by companies in determining the appropriate course of action under the circumstances: (1) type of customer relationship (*e.g.*, membership-type in which consumers have ongoing interaction); (2) type of information at issue (*e.g.*, sensitive personally identifiable information, such as information collected from children online or health data); (3) nature of the change; (4) reason for a change in circumstances (*e.g.*, merger or other corporate restructuring, materially different product/service); (5) in the case of a merger, acquisition, bankruptcy sale, etc., factors such as the line of business of the new entity and any agreement to maintain prior commitments; and (6) use of the information, such as for Web site or business optimization, market research, or direct marketing. Such balancing of relevant factors is consistent with the approach that the Commission took in connection with merger activities and new parental notice and consent for changed information practices under the Children’s Online Privacy Protection Act (“COPPA”).¹¹

DMA agrees that providing consumers with notice and, where appropriate, choice concerning material changes to privacy policies is important to ensuring that consumers can make informed decisions regarding how information about them is collected, used, and shared with third parties. However, many years of experience with this issue has demonstrated that adoption of a flexible principle concerning notification of changes, which takes into account the type of notice and/or choice needed depending on the circumstances, is the best approach to protecting consumers and ensuring that they receive relevant information. This approach promotes efficiency and, at the same time, continued growth and availability of new content, products, and services online, which may require material changes to prior promises.

This type of flexible approach is embodied in DMA’s *Online Marketing Guidelines*, which provide that:

If your organization’s policy changes materially with respect to the sharing of personally identifiable information with third parties for marketing purposes, you will update your policy and give consumers conspicuous notice to that effect, offering an opportunity to opt out.

¹¹ See 64 Fed. Reg. 59888, 59897 (Nov. 3, 1999). In providing examples of situations where new parental notice and consent are needed for changed information practices, the FTC looked at amount and type of information submitted previously versus that going forward, whether the marketing involved materially new or different services than those previously described, and issues related to similarity of lines of business in conjunction with merger activities.

Also, Article 38 of our *Guidelines for Ethical Business Practice* provides in relevant part:

If your organization’s policy changes materially with respect to the sharing of personally identifiable information with third parties for marketing purposes, you will update your policy and give consumers conspicuous notice to that effect, offering an opportunity to opt out.

Similarly, affording different levels of notice and/or choice, depending on the circumstances, has been effective and is consistent with consumer protection standards. Indeed, recognizing the importance of consumer trust and brand reputation, companies have strong incentives to ensure that the mechanisms they choose for notice and/or choice are meaningful.

With respect to the *Gateway Learning* case, which is cited by the Commission in footnote 9 in support of this proposed principle, this case is distinguishable because it involved 1) information about children, and 2) violations of stated promises. As with most Commission consent agreements, in such circumstances companies may be held to a higher standard than they otherwise would have been given that the Commission is remedying alleged bad conduct. Thus, while it may have been appropriate to apply an affirmative express consent standard in that or similar contexts, adopting such an approach as the foundation of this principle would unnecessarily go beyond legal requirements and current best practices.

Finally, adoption of a flexible approach will best account for instances where notice and affirmative consent for material changes are, or could be, legally required in certain contexts. For example, under the COPPA rule, which addresses sensitive children’s information, new parental notice and consent for changed information practices is required in certain circumstances.¹² Moreover, the personally identifiable information at issue in COPPA is unique in that it is collected from children online, warranting the higher standard of notice and affirmative express consent from parents in connection with material changes to privacy promises in certain instances. Thus, while appropriate under some circumstances, this approach should not be more broadly applied to all situations where companies wish to provide notice and choice regarding material changes in privacy policies, as the Commission’s proposed principle would do.

VI. Principle 4—Prior to Adopting an “Express Consent” Requirement or a Prohibition on Use of “Sensitive Data” for Behavioral Advertising, Potential Harms Should Be Identified and Weighed Against the Benefits of Use

The current regulatory and self-regulatory standards that govern not only the types of notice and consent required for use of “sensitive data,” but the factors to consider in connection with the appropriateness of sending advertising based on such data, are working well. Thus, DMA does not believe that any additional consents or prohibitions are necessary. Set forth

¹² *Id.*

below are a comparison of the Commission’s proposed principle with the current regulatory framework and DMA guidelines concerning sensitive data, followed by a discussion of the questions raised by the Commission in connection with this principle.

A. The Current Regulatory and Self-Regulatory Frameworks

Under the Commission’s proposed principle, companies would be allowed to collect sensitive data for behavioral advertising only if they had obtained affirmative express consent from the consumer to receive such advertising or, alternatively, such practices would be prohibited outright.

In considering this principle, it is important to note that many industry sectors and types of data that traditionally are considered sensitive, and that the Commission provides as examples, already are the subject of extensive regulation: for example, children’s, health, and financial information are covered respectively under COPPA, the Health Insurance Portability and Accountability Act (“HIPAA”), and GLB. Additional self-regulation in connection with these types of sensitive data, which represent some of the most heavily regulated areas, thus, is not necessary.

Further, there are many current self-regulatory frameworks, including that of DMA, that address not only the types of consent for use of sensitive data, but the appropriateness of using such data in connection with marketing. Specifically, with respect to children’s information, the *DMA Guidelines for Ethical Business Practice*¹³ provide that:

Offers and the manner in which they are presented that are suitable for adults only should not be made to children. In determining the suitability of a communication with children online or in any other medium, marketers should address the age range, knowledge, sophistication, and maturity of their intended audience. See Article 13, page 9.

These *Guidelines* also provide that:

Marketers should take into account the age range, knowledge, sophistication, and maturity of children when collecting information from them. Marketers should limit the collection, use, and dissemination of information collected from or about children to information required for the promotion, sale, and delivery of goods and services, provision of customer services, conducting market research, and engaging in other appropriate marketing activities.

Marketers should effectively explain that the information is being requested for marketing purposes. Information not appropriate for marketing purposes should not be collected. See Article 15, page 9.

¹³ See n.9 *infra*.

As these excerpts from our best practices demonstrate, extensive guidelines regarding the appropriateness of use of such information exist, and our experience has been that they are working well.

This is also the case in connection with another area that the Commission's proposed principles identify as potentially being sensitive. Regarding the use of health-related data, the DMA *Guidelines* provide in relevant part that:

Consumers should not be required to release personally identifiable health-related information about themselves to be used for marketing purposes as a condition of receiving insurance coverage, treatment or information, or otherwise completing their health care-related transaction. See Article 33, ¶ 6, page 17.

These *Guidelines* also provide that:

The text, appearance, and nature of solicitations directed to consumers on the basis of health-related data should take into account the sensitive nature of such data. See Article 33, ¶ 7, page 17.

Given the extensive regulation and self-regulatory efforts in this area, DMA does not believe that new self-regulatory efforts need to be undertaken.

B. Input on the Questions Posed by the Commission

In connection with this principle, the Commission seeks specific input on (1) what classes of information should be considered sensitive, and (2) whether using sensitive data for behavioral targeting should not be permitted, rather than subject to consumer choice.

With regard to what information should be considered sensitive, although in another context, DMA has defined sensitive data to include data pertaining to children, older adults, health care or treatment, account numbers, or financial transactions. *See Guidelines* Article 36, page 19. This approach has worked well, and we believe that these categories reflect the types of data that consumers consider to be sensitive.

Regarding the question of an outright prohibition against the use of sensitive data for behavioral advertising, DMA does not consider such an approach to be in the best interest of consumers, as it could restrict the availability of useful services and information. As the excerpts from our *Guidelines* set out above demonstrate, respecting the sensitivity of this type of data through ensuring that advertising is appropriate, and honoring consumer choice, will help ensure that consumers can continue to receive important information.

VII. Conclusion

DMA is a long-time leader in the marketing industry's self-regulation and peer regulation. For decades, we have worked to develop practices that will address and protect consumer privacy. We understand that our online and offline worlds are more dynamic than ever, and will continue to develop effective business practices in a timely manner to address consumer concerns as these mediums evolve.

DMA commends the Commission for its consideration of these issues and for encouraging and facilitating a stakeholders' dialogue on behavioral advertising practices. We look forward to working with you on these issues and are available to answer any questions.

APPENDIX A

THE DIRECT MARKETING ASSOCIATION'S SELF-REGULATORY INITIATIVES

I. DMA'S ONLINE SELF-REGULATORY PROGRAMS

DMA's members understand and respect the privacy needs of consumers and can react much more quickly than the government to new conditions in the marketplace; therefore, DMA has developed a self-regulatory response to privacy. For decades, DMA and its members have worked to develop effective consumer notice and choice practices as a fundamental element of self-regulation.

Below is a brief description of DMA's business practice tools created to incorporate both notice and choice elements and to bolster a responsible exchange of consumer information.

A. Privacy Commitments and the DMA Guidelines

DMA is providing leadership in the offline and online worlds through the privacy commitments in its guidelines (see below). It is a condition of membership in DMA that companies, including online businesses, follow a set of privacy protection practices:

- Providing customers with annual notice of their ability to opt out of information exchanges; for online marketing, providing notice to both customers and prospects in each solicitation;
- Honoring customer opt-out requests not to have their contact information transferred to others for marketing purposes;
- Accepting and maintaining consumer requests to be on an in-house suppress file for prospective customers to stop receiving unwanted commercial solicitations; and
- Using DMA's Preference Service suppression files.

B. DMA's Online Marketing Guidelines

DMA also is providing leadership in the online world. DMA's *Online Marketing Guidelines* ("Online Guidelines")¹ explain and highlight issues unique to online and Internet marketing. When marketing online, companies are advised that the notice they provide to consumers regarding their information practices should be placed either in a prominent place on their Web site's home page or in a place that is easily accessible from the home page. The notice should state whether the marketer collects personal information online from individuals; provide certain disclosures, including whether cookies or other passive means of data collection are used; identify the marketer; and provide an e-mail address, postal address, and telephone number at which the marketer can be contacted. Marketers sharing personal information collected online

¹ Available at www.the-dma.org/guidelines/onlineguidelines.shtml.

also are required to provide consumers with an opportunity to opt out from the rental, exchange, or sale of this information for commercial purposes.

Under the Online Guidelines, a marketer who permits network advertisers to collect information from its Web site also should provide notice of the network advertisers that that collect information from the site and a mechanism by which visitors can find those network advertisers to obtain their privacy statements and have the ability to exercise the choice of not having such information collected.

DMA's Online Guidelines also provide best practices for commercial electronic mail solicitations.

C. Online Advertising and Affiliate Marketing

Another issue that DMA has sought to address through self-regulatory best practices is the role of advertisers in ensuring that their advertisements are being disseminated responsibly. In some instances, there may be advertisers with good intentions who do not understand where their ads are appearing online. To help address some of these issues, DMA adopted best practices regarding online advertising networks and affiliate marketing.² These best practices state, among other things, that marketers should obtain assurances that their partners will comply with legal requirements and DMA's Ethical guidelines, undertake due diligence in entering into these partnerships, define parameters for ad placement, and develop a monitoring system for online advertising and affiliate networks.

D. Software Downloads

In yet another effort to keep pace with the changing technologies and in continuing to build consumer confidence, DMA, working with its members, in 2006 developed and adopted Standards for Software Downloads as part of our *Guidelines for Ethical Business Practice* ("Ethical Guidelines") (see below), to specifically discourage illegitimate software download practices that threaten to undermine electronic commerce and Internet advertising.³ This Guideline encourages members to provide notice and choice regarding software that may be downloaded onto a consumer's personal computer or similar devices.

This Guideline also details responsible practices for marketers offering software or other similar technology that is installed on a computer used to further legitimate marketing purposes. Specifically, such programs must provide a user with clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects of having the software or other similar technology installed. Marketers also must give the user an easy means to uninstall the technology and/or disable all functionality. Finally, marketers should always provide an easily

² See DMA Best Practices for Online Advertising Networks and Affiliate Marketing (available at <http://www.the-dma.org/guidelines/onlineadvertisingandaffiliatenetworkBP.pdf>).

³ Use of Software or Other Similar Technology Installed on a Computer or Similar Device, DMA *Guidelines for Ethical Business Practice*, at 23 (available at <http://www.the-dma.org/guidelines/ethicalguidelines.shtml>).

accessible link to privacy policies and contact information, as well as clear identification of the company making the offer.

E. DMA's Privacy Policy Generator

Another effective DMA program developed to help members provide effective notice and choice to consumers is DMA's Privacy Policy Generator.⁴ This tool allows companies to create and post effective privacy policies.

DMA's Privacy Policy Generator enables companies, through a series of questions, to develop customized privacy policies for posting on their Web sites based on the companies' policies regarding the collection, use, and sharing of personal information. The utility of this tool, and the ease with which it is used, is demonstrated by the hundreds of companies that have used it and sent these policies to DMA for review.

DMA also created a Children's Privacy Policy Generator that allows direct marketers to create effective children's privacy policies, and a Gramm-Leach-Bliley Act Privacy Policy Generator, which helps financial institutions comply with the Act's privacy notice requirements.

All of these Privacy Policy Generators are easy to use, and guide marketers through an online step approach through which marketers answer a series of questions. From these questions, marketers are able to determine which disclosures they need to make in the privacy policies posted on their Web sites based on their information practices.

II. DMA'S ETHICS GUIDELINES

DMA's self-regulatory guidelines and procedures provide a comprehensive and meaningful approach to addressing consumer privacy. At the cornerstone of DMA's self-regulatory approach are DMA's *Guidelines for Ethical Business Practice* ("Ethical Guidelines").⁵ These Ethical Guidelines were adopted to aid its members and others engaged in direct marketing in determining ethical conduct in dealing with customers and other businesses, which will be in the best interest of their customers. DMA has undertaken extensive efforts to ensure that its members market ethically for the protection of consumers. Indeed, on a daily basis, DMA gives its members advice on how to ensure that they are complying with these Guidelines.

In an effort to strengthen sound business practices in the marketplace, DMA established its Committee on Ethical Business Practice to review direct marketing promotions and practices that may violate the Ethical Guidelines. The Committee reviews potential Guidelines violations of both association members and non-members. The Committee has applied the Ethical Guidelines to hundreds of direct marketing cases concerning deception, unfair business practices, personal information protection, and other ethics issues.

⁴ Available at www.the-dma.org/privacy/creating.shtml

⁵ Available at www.the-dma.org/guidelines/ethicalguidelines.shtml

A. The Process

The Committee receives promotions and practices for review in a number of ways: through consumers, member companies, non-members, or sometimes consumer protection agencies. If the majority of the Committee believes that the promotion or practice brought to its attention potentially violates the Ethical Guidelines, DMA staff contacts the company and points out the potential Guidelines violation. The company is then given an opportunity to respond. If the Committee does not believe the promotion violates the Ethical Guidelines, the case is closed and the company is not contacted. Cases closed without company contact are handled confidentially.

Most companies cooperate with the Committee's efforts and agree to modify the questioned promotion or practice. Because cooperation with the Committee and compliance with DMA's Ethical Guidelines are voluntary, a confidential and meaningful dialogue about the particular promotion or practices usually occurs, and the Committee and the company are typically able to reach a satisfactory conclusion.

In those cases where the Committee is successful in obtaining the company's cooperation to change the promotion or practice, or where the Committee is persuaded that no violation occurred, the case proceedings remain confidential. The confidentiality protects all parties and helps ensure that the Committee's goal of obtaining compliance with the Ethical Guidelines is met.

In those rare instances where the Committee cannot come to a satisfactory resolution with a member or non-member company, that is, the Committee believes that the violations are continuing, the case may be referred to DMA's Board of Directors for further action. Cases referred to the Board of Directors are made public by the Committee. Board action could include censure, suspension of membership, or expulsion from DMA. The Board also may decide to publicize its action. Companies with promotions or practices that are found to violate the law in addition to the Ethical Guidelines are referred to appropriate law enforcement authorities for handling.

The Ethical Guidelines have proven to be an effective means of ensuring ethical marketing practices by non-members as well. Although non-members are not bound by the DMA Ethical Guidelines, it has been our experience that non-member companies comply with Guidelines and policies so as to comport with industry standard practices. The net effect is to increase good business practices for the industry and to increase consumer confidence in the marketplace. In addition, where a non-member company's practice is illegal, we are able to refer the case to the appropriate federal and/or state law enforcement authority.

B. The Committee on Ethical Business Practice's Self-Regulatory Approach

DMA's self-regulatory approach has proven successful in addressing complaints regarding practices contrary to DMA's Ethical Guidelines. Working with both members and non-members, DMA has gained voluntary cooperation in adhering to these Guidelines. As a result of DMA's efforts, many companies have reformed their practices in areas such as

sweepstakes, predictive dialing, unsolicited faxes, and e-mail to address the concerns raised by activities that are in violation of the Ethical Guidelines.

III. TECHNOLOGY SOLUTIONS

Technology is playing an increasingly important role in helping users determine and enforce the ways in which information about them is used and collected. DMA and marketers have been, and continue to be, instrumental in the development of this important technology by encouraging, supporting, and indeed helping to develop and promote, such software.

Since its inception, DMA has been involved in an initiative that supports this concept—the Platform for Privacy Principles (“P3P”). This initiative, undertaken by the World Wide Web Consortium, has developed a “negotiation” approach for protecting privacy. A broad coalition of information providers, advertising and marketing specialists, software developers, credit services, telecommunications companies, and consumer and online advocates worked together on P3P to achieve a technological solution that will protect privacy without hindering the development of the Internet as a civic and commercial channel. P3P allows a user to agree to or modify the privacy practices of a Web site, and be fully informed of the site’s practices before interacting with or disclosing information to a site. There also have been several announcements by companies of other commercial products that will empower consumers with respect to privacy online. As technology continues to improve, so will consumer empowerment tools. We support the continued responsible use of this cutting-edge solution as regulators, businesses, and consumers evaluate it.

IV. PUBLIC EDUCATION

Another important part of DMA’s efforts is educating consumers and businesses about the numerous DMA programs that are available to them. DMA has a vital interest in educating its members and the general public about the responsibilities of people who collect and use data, as well as the self-regulatory process. We take great pride in our education initiatives because, through them, individuals and businesses will better understand the potential benefits of interactivity and the choices individuals have to control information that they submit to these businesses.

DMA also has made a special effort to empower children, parents, educators, and librarians by establishing its www.cybersavvy.org Web page for them and providing them with tools, information, and resources to ensure safe Web surfing. Additionally, we produced a “hard copy” version of the Web site, *Get CyberSavvy*. *Get CyberSavvy* has the distinction of being awarded first place honors for excellence in consumer education by the National Association of Consumer Affairs Administrators.

In addition, DMA communicates regularly with consumer affairs professionals through e-mail newsletters and alerts, and exhibits information at consumer affairs conferences.