Before the
DEPARTMENT OF COMMERCE
Washington, DC 20230

COMMENTS
of the
DIRECT MARKETING ASSOCIATION, INC.

Responding to the Request for Public Comments
on "Commercial Data Privacy and Innovation in the Internet Economy:
A Dynamic Policy Framework"

Docket No. 101214614-0614-01

January 28, 2010

Linda Woolley
Executive Vice President, Government Affairs
Gerald Cerasale
Senior Vice President, Government Affairs
Rachel Thomas
Vice President, Government Affairs
Direct Marketing Association, Inc.
1615 L Street, NW Suite 1100
Washington, DC 20036
(202) 861-2444

Counsel:
Stuart Ingis
Emilio Cividanes
Kelly DeMarchis
Venable LLP
575 Seventh Street, NW
Washington, DC 20004
(202) 344-4613

Direct Marketing Association, Inc.

Comments on "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework"

Docket No. 101214614-0614-01

The Direct Marketing Association ("DMA") appreciates this opportunity to provide comments in response to the request for public comment by the Department of Commerce ("Department") regarding the framework for consumer privacy proposed in its December 2010 Internet Policy Task Force Report, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (the "Report"). We appreciate the Department's focus on commercial data privacy, and we welcome the opportunity to continue to work with the Department on these important issues.

The 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. The 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, the DMA today represents thousands of companies from dozens of vertical industries in the United States and 50 other nations, including a majority of the Fortune 100 companies, as well as nonprofit organizations. Included are cataloguers, 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.

I. The Existing Sectoral Framework in U.S. Privacy Law Should be Maintained in Order to Foster Innovation While Preserving Consumer Choice

The DMA believes it is of paramount importance that the existing "sectoral" framework of United States privacy law be maintained in order to continue the balancing act of fostering innovation while preserving consumer choice; however, it is important to recognize and be wary of the possibility that one segment of an industry could be singled out for special treatment with respect to the same data and business practices. Instead of having Congress or the federal government parse who is "in," and who is "out," self-regulation is the more effective means of delineating categories of data collection, as we have done in the development of the Self-Regulatory Principles for Online Behavioral Advertising ("Principles"), discussed below.

The Internet is no longer a distinct industry, but penetrates every area of Americans' business and private lives. Our member companies grapple each day with the business and ethical consequences of this expansion and the attendant technological innovation. However, the DMA does not believe that this rapid pace of change heralds a need for new regulation. On the contrary, today's vibrant Internet ecosystem results

from, and demonstrates the need to retain, the existing U.S. approach to privacy regulation, which has allowed innovation to flourish while preserving consumer choice.

The United States was the birthplace of the Internet and remains the global leader in online technological innovation. As the Internet became available to consumers in the late 1990s, regulatory bodies and Congress assessed the need to regulate the new medium. The result was a broad consensus in favor of avoiding heavy-handed regulation in order to foster technological innovation and economic growth.

With this balance in mind, U.S. privacy regulation is founded on several core principles often referred to as "fair information practices," or FIPPs, which are designed to ensure that consumers can exercise meaningful control over their private information while allowing beneficial information use to continue. As summarized by the Federal Trade Commission in a report to Congress, these principles are:

1. Notice/awareness,
2. Choice/consent,
3. Access/participation,
4. Integrity/security, and
5. Enforcement/redress.[1]

Over the decades, the fair information practices have served as a flexible and adaptable framework to guide companies as they consider how best to preserve consumer choice while promoting innovation and economic growth and allowing beneficial uses of information to continue. The flexibility of the FIPPs have allowed companies to implement appropriate consumer response mechanisms, depending on the type of data. For example, data that is personal, i.e., information about an identified individual that raises no special privacy concerns, has historically been subject to a notice and choice regime under the FIPPs. This regime has worked to protect consumer privacy while maintaining beneficial data flows. Information that is considered to be private, such as health information, has been governed more restrictively under the FIPPs (and DMA Guidelines). Absent a specific showing that particular information should be treated as private information, or establishment of harm to the individual, the FIPPs-guided distinction between personal and private information dictates that notice and choice should continue to apply to personal information. This proven standard should continue to guide companies going forward.

In keeping with this balanced approach, Congress has largely followed a "sectoral" framework in U.S. privacy legislation. Federal privacy statutes that apply to businesses typically address particular areas of concern, such as children's online privacy, or specific sectors perceived as handling sensitive information, such as the

[1] Federal Trade Commission, "Fair Information Practice Principles," in *Privacy Online: A Report to Congress* (June 1998), *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited January 7, 2011).

financial and health care industries entities. The DMA believes that compelling policy reasons support this reluctance to regulate business privacy practices more broadly. It would not be feasible or prudent to impose a "one size fits all" set of standards across the economy, given the wide variation in different industries' information collection and uses.

II. Consumers Continue to Enjoy the Benefits of Online Advertising and Marketing

The DMA has represented businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques for nearly 95 years, and direct marketing practices have been in use for even longer. Marketing can be distinguished from advertising in that it is dependent upon data and analytics, helping companies reach the "right" audiences for their products and services.

One hundred years ago, direct marketers sent "offers" to prospective, likely customers through the mail; for example, a Sears catalogue would be sent to targeted customers rather than every postal address. While the rise of the Internet has made it quicker and easier for marketers to present consumers with relevant offers, the concept and underlying principles of direct marketing remain the same. Today, it is the goal of every company in the U.S.—if not the world—to engage consumers in direct, personal conversations about their interests and preferences. This is, quite simply, the most recent development in the long evolution of marketing and advertising practices that drive our economy.

Today, online advertising is a highly dynamic market characterized by rapid technological change. Advertising, and the marketing data that drives it, has provided critical support for the explosion of innovation that has characterized e-commerce from its beginnings. In addition to turning to the Internet for its e-commerce resources, consumers have come to expect rich online content and services to be made available at little or no cost. This is possible due to the subsidy provided by online advertising. This arrangement between consumers and content providers—advertising in return for free content and services—has become a primary driver of online commerce. The evidence for the growth of Internet commerce is compelling and indicates that the commercial data practices in place heretofore have indeed already ensured that the "Internet fulfills its social and economic potential."[2] That is not to say that commercial data practices cannot, and should not, evolve to align with consumer expectations and needs.

In this environment, regulation that is specific to a technology or business model could deter entry into the e-commerce market, thwart innovation, and limit competition in the sale of online advertising. And, to the extent that existing laws regulate particular technologies, their practices with regard to marketing should not be restricted by the existing regime. No company can succeed in today's highly competitive marketplace

[2] Report, p. vi.

unless it wins and retains the trust of its customers. Rather than impose disparate regulation, the government should promote industry self-regulatory approaches that protect privacy while promoting competition among technologies and business models, allowing the marketplace to decide which practices and technologies provide the greatest level of benefits to consumers. Fewer choices for online ad sales could exacerbate the already significant financial pressure on advertiser-supported media.

While there are those who may claim that privacy concerns affect online usage, this argument is discredited by American consumers' evident enthusiasm for Internet technologies and the resulting growth in online economic activity.[3] In 2010 alone, more than 106 million consumers planned to shop on Cyber Monday—a considerable jump from the previous year's count of 96.5 million, and nearly double the rate five years ago.[4] Over seven million of those consumers planned to use their smart phones for Cyber Monday shopping. Further, American consumers use the Internet avidly for a variety of purposes beyond e-commerce, quickly embracing emerging technologies like cloud computing, mobile computing, and social networking. Particularly in social networking environments, consumers proactively provide companies with information about their interests and preferences by "liking" or "following" their favorite brands.

Consumers' embrace of e-commerce shows that they widely value the convenience, customization, and features that companies can offer online. The very recent rise of tablet computers, e-readers, and smart phones attests to consumers' continued embrace of rapid innovation and new technologies. Consumers continue to value website personalization and free online content. Most consumers have historically preferred free websites supported by advertising instead of paid sites with subscription fees. Consumers would likely be frustrated by paywalls and diminished free content in lieu of the *status quo*, especially as more of their Internet usage occurs through mobile devices. Also important to this calculus is the fact that most of the information exchange that fuels Internet content does not intrude on consumers' Internet usage.

It is evident that the prevailing U.S. approach to privacy regulation strikes an appropriate balance that benefits consumers and industry alike. Thus, the DMA cautions against premature and counterproductive legislation that would have the effect of disturbing consumers' active engagement with the Internet. Unnecessary restrictions on online advertising will reduce the relevance of commercial messages to consumers, and

---

[3] In the face of exponential growth in e-commerce, this same argument, offered again and again since the 1990s, has become tiresome. The $1.028 billion sales of Cyber Monday of 2010, representing a 16% increase from Cyber Monday sales of the previous year, should end this tired refrain, and the government should now move beyond it as well. Press Release, comScore, Billion Dollar Bonanza: Cyber Monday Surpasses $1 Billion in U.S. Spending as Heaviest Online Shopping Day in History (Dec. 1, 2010), *available at* http://comscore.com/Press_Events/Press_Releases/2010/12/Billion_Dollar_Bonanza_Cyber_Monday_Surpasses_1_Billion_in_U.S._Spending.

[4] Press Release, Shop.org, Over 106 Million Americans to Shop on Cyber Monday, According to Shop.org Survey (Nov. 28, 2010), *available at* http://www.shop.org/press/20101128.

as online advertising becomes less effective, it will impede companies' ability to provide ad-supported content and services to the public. This could hinder innovation or drive businesses to shift from offering free content and services to demanding direct payment from consumers. Given that consumers have repeatedly shown an unwillingness to pay for such content and services, a general retraction in the e-commerce market would be a likely result, stifling one of the most powerful engines of the American economy.

III. The DMA Supports Voluntary Codes of Conduct as the Best Primary Mechanism for Addressing Online Privacy

The DMA is encouraged by the positive highlighting of self-regulatory codes throughout the Report. Further, the DMA agrees with the Department's recognition that efforts led by the private sector to develop voluntary codes of conduct are the preferred approach for addressing the interplay of online privacy and online advertising practices. Sweeping legislation is not necessary given that self-regulation and other existing tools continue to be effective in preserving the fair information principles. Absent evidence of chronic and purposeful violations of industry best practices or standards, government enforcement is not necessary, and the record at this point in time does not support the adoption of agency enforcement mechanisms. We believe that additional efforts in the area of self-regulation will continue to bear fruit and, with the Department's input, can fully address all of the privacy concerns set forth in the Report.

Specifically, the self-regulatory approach is the most efficient and effective way to respond to privacy issues related to marketing and advertising. Advertising and marketing provide great benefits to consumers by making them aware of products, services, and offers that may interest them. As described above, advancements in technology have simply enabled marketers and advertisers to deliver offers that are more relevant and, therefore, potentially more valuable to consumers.

The Report recommends that the government recognize a revitalized set of FIPPs as a foundation for commercial data privacy.[5] The DMA believes that the FIPPs are useful to help companies analyze their privacy practices. They also are a valuable framework for policy discussions in the privacy area. A FIPPs-based framework that promotes the development of robust voluntary codes of conduct could build upon the efforts already undertaken by industry to advance robust self-regulatory initiatives that address privacy issues in an evolving and effective manner. The FIPPs should not, however, form the basis for legislation, and any processes and policies that are developed based upon the FIPPs should be applied in a competitively and technologically neutral fashion. No framework imposed upon the industry, no matter how elastic, can encompass the diverse number of companies and types of data practices into an effective one-size-fits-all solution that will fairly regulate the entire industry.

[5] Report, p. 4.

The DMA supports the Department's view that harm continues to be the appropriate framework through which to preserve consumer choice without hindering innovation. Receiving such messages does not harm consumers in any conceivable way, because unwanted messages can easily be ignored. While advancements in technology that enable data collection and uses in support of advertising have raised some privacy questions, the DMA believes that these questions are being adequately addressed through self-regulation and submits that self-regulation generally remains the most appropriate method for industry to improve marketing practices with input from government authorities. Until or unless it is shown that consumers are harmed by the receipt of advertising messages, the fact that those messages are delivered with the aid of new technologies or through new channels does not warrant additional legislation or regulation to protect consumers.

Long-standing and successful self-regulatory programs such as the DMA's *Guidelines for Ethical Business Practice* (the "Guidelines") provide meaningful controls and accountability.[6] DMA member companies have a major stake in the success of e-commerce and Internet marketing. They understand that their businesses depend on consumers' continued confidence in the online medium, and they support efforts that enrich a user's experience while fostering consumer trust in online channels.

The DMA and its members have developed standards for online data practices and many other business activities as part of our comprehensive Guidelines. Under the current Guidelines, companies should:

- Not display, disclose, rent, sell or exchange data and selection criteria that may reasonably be considered sensitive or intimate, where there is a reasonable consumer expectation that the information will be kept confidential;[7]

- Not transfer personally identifiable health-related data gained in a medical treatment context for marketing purposes without the specific prior consent of the consumers;[8]

- Treat personally identifiable health-related information volunteered by or inferred about consumers outside a treatment context as sensitive and personal information, and provide clear notice and the opportunity to opt out and take the information's sensitive into account in making any solicitations;[9]

---

[6] Direct Marketing Association Guidelines for Ethical Business Practice, *available at* http://www.dmaresponsibility.org/Guidelines/.
[7] Guidelines, Article 32.
[8] Guidelines, Article 33.
[9] *Id.*

- Not rent, sell, exchange, transfer, or use marketing lists in violation of the Guidelines;[10]

- Provide notice of online information practices, including marketing practices, in a way that is prominent and easy to find, read, and understand, and that allows visitors to comprehend the scope of the notice and how they can exercise their choices regarding use of information;[11]

- Identify and provide contact information for the entity responsible for a website;[12]

- Comply with the new self-regulatory principles for online behavioral advertising, discussed above;[13]

- Assume certain responsibilities to provide secure transactions for consumers and to protect databases containing consumers' personally identifiable information against unauthorized access, alteration, or dissemination of data;[14]

- Restrict data collection and marketing for children online or via wireless devices, consistent with the Children's Online Privacy Protection Rule;[15] and

- Follow specific rules for data compilers, including suppressing a consumer's information from their databases upon request, explaining the nature and types of their sources to consumers upon request, reviewing customer companies' use of data and requiring customers to state the purpose of their data use, and reviewing promotional materials used in connection with sensitive marketing data.[16]

- Marketing data should be used only for marketing purposes.[17]

These examples are only a sample of the standards contained in the Guidelines, which provide DMA member companies with a comprehensive blueprint for ethical marketing practices.

The DMA maintains a robust accountability program to ensure compliance with the Guidelines, which is a condition of DMA membership.[18] Complaints are accepted

---

[10] Guidelines, Article 35.
[11] Guidelines, Article 38.
[12] *Id.*
[13] *Id.*
[14] Guidelines, Article 37.
[15] Guidelines, Article 16.
[16] Guidelines, Article 36.
[17] Guidelines, Article 32.
[18] DMA Corporate Responsibility Resource Center, *available at* http://www.dmaresponsibility.org/.

from consumers as well as from companies who may be concerned that their competitors are not playing fair by complying with the Guidelines. These complaints are reviewed and investigated by the DMA Corporate Responsibility Team, in conjunction with the DMA Committee on Ethical Business Practice. If a potential violation is found to exist, the company will be contacted and advised on how it can come into full compliance. While most companies work with DMA to come into compliance, in cases where a company does not cooperate and there is evidence of continued non-compliance, DMA may take action to make the results of an investigation public. For DMA member companies, action might also include censure, suspension, or expulsion from membership. If DMA believes that violations of law may also have occurred—by a member or non-member company—the case will be referred to the appropriate federal or state law enforcement authorities and may also be made public. An annual Ethics Case Report is published, summarizing the findings of the Committee on Ethical Business Practice.

The Self-Regulatory Principles for Online Behavioral Advertising released in July 2009 and now codified in the DMA Guidelines, are another recent example of effective industry response to an emerging consumer concern.[19] The Self-Regulatory Principles are designed to address consumer concerns about the use of personal information and interest-based advertising while preserving the innovative and robust advertising that supports the vast array of free online content and delivers relevant offers to consumers.

DMA, in conjunction with other participating trade associations, drafted, developed, and deployed these Self-Regulatory Principles in less time than it took Congress and the Federal Trade Commission (the "FTC") collectively to pass the CAN-SPAM Act of 2003 and promulgate accompanying final regulations, and in less time than it took the FTC and various other federal agencies to develop model privacy notices for financial institutions. These Self-Regulatory Principles require advertisers and websites to inform consumers about data collection practices and enable them to exercise control over that information. They define "online behavioral advertising" as the "collection of data from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate websites for the purpose of using such data to predict user preferences or interests to delivery of advertising to that computer or device based on the preferences or interests inferred from such web viewing behaviors."[20] The Self-Regulatory Principles call on companies to:

- Provide enhanced notice outside of the company's privacy policy on any web pages where data is collected or used for online behavioral advertising purposes;

[19] 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.the-dma.org/government/ven-principles%2007-01-09%20FINAL.pdf.

[20] Self-Regulatory Principles for Online Behavioral Advertising, *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf (last visited January 10, 2011).

- Provide choice mechanisms that will enable users of websites at which data is collected for online behavioral advertising purposes the ability to choose whether data is collected and used or transferred to non-affiliate for such purposes;

- Provide reasonable security for, and limited retention of, data collected and used for online behavioral advertising purposes;

- Obtain consent before applying any material change to their online behavioral advertising data collection and use prior to such material change; and

- Provide heightened protection for certain sensitive data.

Building on the Principles, in October 2010, the nation's largest media and marketing associations launched the Self-Regulatory Program for Online Behavioral Advertising (the "Program"), giving consumers enhanced control over the collection and use of data regarding their Web viewing for online behavioral advertising purposes (*see* www.AboutAds.info). The Program promotes the use of the "Advertising Option Icon" and accompanying language to be displayed within or near online advertisements or on Web pages where data is collected and used for online behavioral advertising or "OBA." The Advertising Option Icon indicates a company's use of OBA and adherence to the Principles guiding the Program. By clicking on the icon, consumers can link to a clear disclosure statement regarding the company's online behavioral advertising data collection and use practices as well as an easy-to-use opt-out mechanism. The AboutAds Consumer Opt-Out Page allows consumers to easily opt-out of some or all of the interest-based ads they receive, if they choose (*see* www.aboutads.info/choices).

Monitoring and enforcement of the Program will be handled jointly by the DMA and the Council of Better Business Bureaus ("BBB"). The DMA's accountability program will actively enforce the Principles: while the initial focus will be on efforts to assist companies with coming into compliance, future monitoring and enforcement activities will ensure accountability among not only DMA member companies, but the entire advertising and marketing industries.

In particular, the DMA believes that the promising Self-Regulatory Principles for Online Behavioral Advertising, and the related cross-industry Self-Regulatory Program, should be given an adequate opportunity to become fully effective before additional regulation is considered in this area.

While data collection and uses in support of advertising have raised some privacy concerns, the DMA believes that these questions have been successfully addressed through self-regulation. Without evidence of consumer harm, the DMA agrees with the Department that self-regulation generally remains the most appropriate method for industry to deal with new and existing practices related to marketing and advertising.

The DMA acknowledges that steps beyond self-regulation may be appropriate where a specific practice is found to cause identifiable and concrete harm to consumers. When warranted, such practices should be addressed on a case-by-case basis to avoid unnecessarily disrupting e-commerce and the entire online ecosystem.

IV. Specific Comments on Certain of the FIPPs Discussed in the Report

The DMA believes that the benefits of data collection and sharing for marketing purposes outweighs any burden placed on consumers by these practices. Any restrictions placed on data practices that would disrupt this beneficial cycle should not apply in relation to marketing for the reasons discussed below.

A. Enhanced Transparency

The Report favorably cites "enhanced transparency" as a way to improve on the current notice-and-choice framework and provide consumers with clear information with which to make informed choices about their personal data.[21] The DMA supports enhanced notice and choice as a standard to be adopted.

Notice and choice should remain the fundamental principles of U.S. privacy law. The model is familiar to consumers and has been effective for decades in allowing innovation to flourish while preserving consumer control over information. DMA has maintained for some thirty years a "mail preference service," now called www.dmachoice.org, that allows consumers to opt-out of direct mail. The emphasis should be on improving the notice and choice model, not jettisoning the system for something untested and unfamiliar to consumers.

A successful example of this process comes from the area of online behavioral advertising. After the FTC expressed concern about these practices, the Self-Regulatory Program for Online Behavioral Advertising, discussed above, developed the Advertising Option Icon that indicates a company's use of online behavioral advertising. Featured in billions of ad impressions during its first month of use, the Advertising Option Icon is becoming a beacon of trust for consumers, letting them know when the advertisements they see are interest-based. The AboutAds Consumer Opt-Out Page currently allows consumers to opt-out of online behavioral advertising from nearly 60 companies,[22] and dozens of additional companies are currently in the process of being integrated into the tool. We expect business participation to become even more robust in the coming months. This is a clear example of enhanced notice and choice developed through industry self-regulation being used to effectively address and alleviate an area of consumer concern.

---

[21] Report, p. 34.

[22] Those 60 participating companies place over 90% of all behavioral advertisements on the Internet. The reach of the program will grow beyond 90% as more companies are integrated into the Advertising Option Icon and www.aboutads.info.

First party marketing provides another example in which a mandatory "one size fits all" application of the FIPPs is neither necessary nor appropriate. Consumers already enjoy choice in first party marketing—affected through industry or company opt-out mechanisms—in numerous situations deemed necessary under existing regulation or industry practice. These tailored choice mechanisms, which exist in every direct marketing channel, reflect the studied review of policymakers and industry regarding consumer preferences and expectations for first party marketing. Mandatory collection of additional consent in areas where consumers are aware of, and significantly benefit from, the use of such information by first parties is not necessary.

Third party marketing is also an area where self-regulation and flexible standards in the application of the FIPPs is effective. Third party marketing is a widely accepted and frequently used practice among commercial and non-profit entities, and it provides numerous benefits to consumers. Marketing that uses third party data benefits small entities by giving them access to consumer data which larger companies can afford to maintain in-house. Third party data providers undertake the costly process of maintaining up-to-date databases. This enhances competition and provides consumers with additional information to use when comparing offers and services. Like first party marketing, it helps relevant advertisements to be delivered to interested consumers.

Small businesses as well as non-profits and government agencies rely on using third party data to in order to identify relevant consumers for their products and services and keep their marketing costs down. This information also assists political candidates, who use this information to communicate relevant messages to interested citizens. In addition to these uses, third party data helps drive other segments of the economy by providing analytics to identifying promising new retail locations for businesses, conducting market research, and developing strategies for media placement.

Consumers have come to rely upon the many benefits that responsible marketing bring to commerce. Market innovators rely upon advertising revenues to create and implement new products and services. Online advertising can be targeted based on context (the content of a website or webpage) or on the browsing history associated with a particular computer, and targeted advertising subsidizes online content and services. Conducted responsibly, this type of collaboration does not jeopardize consumer privacy. It relies largely on anonymous data that is not linked back to a named individual, much of which may be discarded after a single online session. The benefits of this process far outweigh any risks to consumers, and any specific, realistic concerns can be addressed on a case-by-case basis while allowing other marketing activities to continue unhindered. Moreover, as the DMA Guidelines require, marketing data may only be used for marketing purposes, or for non-marketing purposes like personalization in content (such as setting up news feeds or serving up news based on the clear preference of a user). DMA's existing Guidelines require that data should not be used for a non-disclosed purpose and that any material change to that purpose or new use requires notice and consent. These requirements prevent the data from being used for non-marketing

purposes that have a serious impact on major determinations about consumers, such as decisions about employment or credit.

The Report also discusses the development of Privacy Impact Assessments, or PIAs, and internal company audits, as potential ways for companies to increase transparency and accountability about their data practices. DMA fears that a formal requirement for PIAs will yield the equivalent of excessively long privacy policies, which are not beneficial or helpful to consumers. Instead of a full-fledged endorsement of these tools at this time, the Department should continue to explore the many different possible accountability mechanisms that may possible ensure companies' compliance with their own data principles and practices. Accountability mechanisms should remain flexible and innovative, just like the data practices that they are designed to monitor.

B. Individual Participation

The Report's support of enhanced transparency to consumers may be tied to the Report's desire to encourage individual participation and control over their own data. One component of individual participation suggested in the Report would include seeking individual consent for the collection, use dissemination, and maintenance of personally identifiable information.

Marketing data sets are benign and do not require access and correction. Currently, there is no public policy basis that supports accuracy for marketing and advertising data. In general, marketing causes no identifiable harm to consumers. There is no empirical evidence that consumers accord the same level of concern over the privacy of information that cannot be identified with them, and information that is aggregated or encrypted does not require the same level of privacy protection as information specifically associated with an identified consumer. Marketing allows consumers to receive information about commercial opportunities that they may value, and consumers are free to respond (or not) as they see fit. If a consumer does not value a particular message, the consumer will simply ignore it. Marketers do not need to know precise information about consumers, but only seek to understand the general characteristics of the individuals to whom they are marketing products and services. Moreover, marketing carries societal benefits as a facilitator of economic growth, and is a form of constitutionally protected speech. Against this set of facts, it is unrealistic to suggest that rights of access and correction be extended to marketing databases. The data contained with them, the uses of this data, and the structures of marketing databases is entirely different when compared with credit reporting databases.

There are also practical considerations counseling against expanded access for marketing databases. The cost of implementing access and correction for marketing databases is prohibitive. Much of this data is handled by database compilation companies. These types of companies undergo significant efforts to ensure that their data is correct, and they provide a mechanism through which a consumer can contact the company to correct or remove information. Mandating additional or redundant access

will add significant costs to be passed on to consumers who already have a means of access to these databases. Expanded access also raises significant privacy, data security and cost considerations. Once access is permitted, the data contained within the databases becomes less secure by virtue of the fact that persons may access and alter the data. As a consequence, expanded access rights will require appropriate authentication and verification systems to be implemented. These types of checks are expensive to implement, and require additional expenditures for data integration, security, and customer service on top of the basic access functionality that would be added. When viewed as a whole, the enormous expenditures and burdens are not warranted by data that does not cause any identifiable harm to consumers.

Where appropriate and provided by law, consumers are already provided with access to data and have the ability to correct and ensue the accuracy of data related to them. The most common examples are under the Fair Credit Reporting Act ("FCRA"), when data is used for employment, credit, and insurance purposes, and the Health Insurance Portability and Accountability Act ("HIPAA"). Consumers are provided with access to data governed by these statutes and have the ability to correct and ensure the accuracy of data related to them. In the marketing context, the application of FCRA and HIPAA standards is not appropriate. Marketing data is not used to make significant determinations about consumers in the same way that FCRA and HIPAA governed data is. In fact, providing consumers with access to marketing data may make the data less secure, as companies would have to add personally identifying information to anonymous data in order to be able to provide correction rights to the data.

C. Purpose Specification and Use Limitation

The Report focuses on purpose specification and use limitation as a way to bring consumer expectations inline with actual information practices. While simplifying consumer privacy notices and fostering greater transparency represent sensible policy objectives, the Department should more thoroughly examine the degree to which purpose specification and use limitation promote those objectives. Companies should be permitted to specify purpose and use in a sufficiently general manner to permit ongoing innovation. A less flexible approach is apt to be counterproductive, by creating the incentive for businesses to provide broad and detailed privacy notices to encompass any potential use of information. Rather than endorse rigid purpose specification and use limitations, the Department should encourage industry to examine the most effective approaches and mechanisms to evolving privacy policies and notices to address new uses and practices.

V. Any Potential Legislation Should Create a Safe Harbor For Companies That Comply with Voluntary, Enforceable Codes of Conduct

Self-regulatory codes are the most effective way to deal with online consumer privacy. But, to the extent that legislation is eventually promoted as a potential solution, it must contain a safe harbor for businesses that adhere to relevant self-regulatory codes.

A robust safe harbor would encourage companies to participate in self-regulatory efforts and would help ensure the broad support of industry that is necessary to ensure active enforcement of such codes.

The DMA believes that the Self-Regulatory Program for Online Behavioral Advertising should be recognized as a qualifying voluntary code under any legislative proposal. The Program has the support of and enjoys participation by a broad spectrum of the online advertising industry, and features active enforcement mechanisms (of which the DMA is one). These participants are committed to fostering compliance and accountability across the industry, and have signaled this commitment through their participation in the program. The Program supports the long-standing values of providing consumers with information and choice and encourages consumer trust in the online marketplace.

VI. The DMA Agrees That Global Interoperability Should Be Encouraged

The DMA supports the efforts of the Department of Commerce in taking the lead to encourage global interoperability. We agree that, "[a]s a leader in the global Internet economy, it is incumbent on the United States to develop an online privacy framework that enhances the trust and encourages innovation,"[23] and we believe (1) that any online framework is best developed by the industry through self-regulatory principles; and (2) that the Department of Commerce is uniquely situated to advocate for the adoption of industry-developed self-regulatory principles throughout the world.

VII. The DMA Strongly Supports A Uniform National Standard For Security Breach Notification

The DMA strongly supports the need for a national standard for security breach notification that would pre-empt the patchwork of state requirements in this area, and looks forward to working with the Department of Commerce on this issue.

* * *

The DMA appreciates the opportunity to provide these Comments to the Department of Commerce. Please contact Linda Woolley at 202-861-2444 or lwoolley@the-dma.org with any questions.

[23] Report, p. 6.