Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

COMMENTS
of the
DIRECT MARKETING ASSOCIATION, INC.

Responding to the Request for Public Comments
on the Preliminary Federal Trade Commission Staff Report
"Protecting Consumer Privacy in an Era of Rapid Change:
A Proposed Framework for Businesses and Policymakers"

File No. P095416

February 18, 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 "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

File No. P095416

Via Electronic Filing

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

RE: Comments on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

Dear Secretary Clark:

The Direct Marketing Association ("DMA") appreciates this opportunity to provide comments in response to the request for public comment by the Federal Trade Commission ("FTC" or "Commission") regarding the framework for consumer privacy proposed in its December 2010 preliminary staff report (the "Report"). We commend the Commission for its continued leadership in the area of consumer privacy and welcome the opportunity to continue to work with the Commission 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.

In these comments, the DMA first offers the following general remarks on how the Commission can address consumer privacy issues in a manner that preserves the United States' global leadership of the thriving Internet economy:

- Consumers benefit from a host of services that rely on third-party data use and sharing, including marketing and advertising.
- The existing framework of sectoral privacy laws built on the Fair Information Practice Principles ("FIPPs") should be maintained. It has successfully fostered innovation while protecting consumers, and the Commission provides no basis for abandoning it now.
- Specifically, the notice and choice model should remain a fundamental principle of U.S. privacy regulation.
- Industry self-regulation, developed in dialogue with the Commission, is generally the best approach to addressing privacy issues in the context of marketing practices.

In addition, we provide the following comments on specific aspects of the Report's proposed privacy framework:

- Although a wide range of commercial entities may benefit from the Commission's views set out in the Report, the DMA cautions against requiring all commercial entities to comply with any "one size fits all" framework.
- The DMA also opposes expanding privacy regulation or principles to include information that is not personally identifiable, such as Internet Protocol addresses.
- While companies may benefit from using "privacy by design" as a lens to evaluate and improve their internal processes, this concept should not become a regulatory requirement.
- In the area of consumer choice, the DMA believes that the Commission's approach of identifying "commonly accepted practices" is too narrow and will thwart innovation. Instead, the Commission should focus on identifying a limited number of practices that *should* require choice.
    - The DMA agrees with the Commission that choice should not be required with first-party marketing.
    - The DMA believes that third-party data use and sharing are commonly-accepted practices, but that choice is appropriate for such practices in the area of marketing.
    - When choice is provided, opt-out choice remains the appropriate form of consent for advertising and marketing practices, by both first and third parties, which do not involve sensitive information.
    - Finally, the DMA believes that choice can and should be provided without interfering with the consumer experience.
- The Report calls for a "Do Not Track" choice mechanism in the context of online behavioral advertising. The Self-Regulatory Principles for Online Behavioral Advertising, currently entering widespread cross-industry implementation, successfully address the Commission's call for a uniform and enforceable choice mechanism.
- The DMA generally supports transparency in data practices but has concerns about the Commission's proposals for new and burdensome obligations.

- The Report does not provide evidence to support any need for new data access, correction, and accuracy standards beyond the consumer rights already provided by key sector-specific laws.
- The DMA would welcome additional guidance from the Commission regarding how complex data practices can best be communicated in privacy policies; however, the DMA notes that current policies are partly shaped by the Commission's enforcement focus on this area.

I. General Remarks

A. Consumers benefit from a host of services that rely on third-party data use and sharing, including marketing and advertising.

Third-party data use and sharing are essential for business success in today's information economy. Businesses use data to drive a host of decisions, from what products to develop and offer to where new retail locations should be established. Third-party data also promotes competition by helping new or smaller businesses compete with larger companies, without the need to amass their own data from scratch. Consumers benefit from these behind-the-scenes activities, which support and enrich the offerings available to consumers through the marketplace.

In particular, third-party data use and sharing are fundamental to current marketing and advertising practices. The impact on the U.S. economy of marketing should not be underestimated. In 2009, marketers – commercial and nonprofit – spent $149.3 billion on direct marketing, which accounted for 54.3% of all ad expenditures in the United States. Measured against total U.S. sales, these marketing expenditures generated approximately $1.783 trillion in incremental sales. In 2009, direct marketing accounted for 8.3% of total U.S. gross domestic product. Also in 2009, there were 1.4 million direct marketing employees in the U.S. Their collective sales efforts directly supported 8.4 million other jobs, accounting for a total of 9.9 million U.S. jobs.[1]

The role of marketing and advertising online is even more significant, as the personalized advertising available online supports a wealth of free Internet content and services that have created the current Internet experience that consumers have come to know. All over the world, corporate executives talk about developing a "personal relationship" with their customers. Customers want to be treated in an individual, personalized way. Consumers have become accustomed to receiving weather, sports scores, stock quotes, and other commercial content that is of specific interest to them. Small businesses have been a direct beneficiary of online commerce, which has opened up an expanded worldwide marketplace. It used to be that if you lived in a rural area, you only had access to the goods and services of your community. Now, a small business can sell its wares all over the world thanks to e-commerce. Someone who lives in rural Maine can buy cake decorating tools from a merchant in England quickly and easily.

[1] Statistics available at http://www.the-dma.org/aboutdma/whatisthedma.shtml.

Global marketplaces like eBay and others were once unfathomable and now not only exist, but thrive because they are widely trusted and accepted by consumers. The existence of free online email services, social networking websites, blogging tools, online forums and the other services that have become an ubiquitous part of daily life is also due to the subsidy of these services by online advertising and marketing.

Although consumers largely cannot escape online advertising and marketing, personalized advertising provides substantial benefits to consumers. Behavioral and contextual advertising provides valuable information to consumers and helps promote informed buying decisions. Consumers respond in far higher numbers to targeted, interactive advertising than to conventional advertising, and the cost savings garnered from this higher yield rate can be passed on to all consumers. Targeted advertising has reduced barriers to entry for small businesses while increasing competition in the online marketplace, resulting in the robust online market for diverse products and services with which U.S. consumers have become familiar.

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. 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 for Ethical Business Practice* require, marketing data may only be used for marketing purposes, or for non-marketing purposes like personalization of content (such as setting up news feeds or serving up news based on the clear preference of a user). The DMA 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.

B. The existing framework of sectoral privacy laws built on the Fair Information Practices should be maintained. It has successfully fostered innovation while protecting consumers, and the Commission provides no basis for abandoning it now.

As discussed in the DMA's earlier comments at the conclusion of the Commission's roundtable series, and reiterated below, the DMA believes it is of paramount importance that the existing "sectoral" framework of United States privacy law be maintained in order to continue fostering innovation while at the same time preserving consumer choice; however, it is also important to avoid singling out one

segment of an industry or one particular technology for special restrictions with respect to the same data and business practices. Specifically, privacy rules should not unwittingly become a means by which some online advertising business models obtain advantages over others. Different standards for different technologies likely would foster consumer confusion and risk while according some online entities artificial business advantages. Instead of having the federal government decide which business practices are "in" and "out," self-regulation is the more effective means of addressing information practices with regard to online behavioral advertising, as we have done in the development of the Self-Regulatory Principles for Online Behavioral Advertising (the "Self-Regulatory Principles"), discussed below.

The Internet is no longer a distinct industry. It permeates 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, the Commission, other 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 known as "fair information practice principles," 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 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.[2]

Over the decades, the FIPPs have been proven to be a flexible and adaptable framework that preserves consumer choice while promoting innovation and economic growth and allowing beneficial uses of information to continue.

[2] 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).

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 financial industry or health care 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. Sweeping legislation is not necessary given that self-regulation and other existing tools continue to be effective in preserving the fair information principles.

It is a myth that consumers do not feel comfortable making purchases on the Internet. It is a further perpetration of the myth to conclude that if consumers just felt more comfortable, then they would purchase even more. It is a red herring that Do Not Track or giving consumers access or the ability to correct marketing data would actually increase Internet sales. There is no basis in fact or experience that gives any credence to these statements or that should lead regulators to these conclusions. Online commerce in the United States continues to rise. One research study reports that the proportion of the general U.S. population that has purchased products such as books, music, toys or clothing online rose from 36% to 52% in the period from May 2000 to May 2010. The proportion of the general population that has made travel reservations or bought travel services rose from 22% to 52% in the same time period.[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 of five years ago.[4] Over seven million of those consumers planned to use their smart phones for Cyber Monday shopping.[5] 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.

The rise of the Internet has led to an explosion of innovation that has transformed every aspect of our lives, generating advances ranging from more efficient business

---

[3] Pew Internet Project, *Online Product Research* (Sept. 29, 2010), *available at* http://www.pewinternet.org/~/media//Files/Reports/2010/PIP%20Online%20Product%20Research%20final.pdf.

[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.

[5] 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.

communications to unprecedented forms of digital entertainment. Advertising has provided critical support for this development across business models and technologies. Online commerce is thriving and increasing, and this e-commerce is spurred by online advertising and marketing. In addition to turning to the Internet for its e-commerce resources, consumers have come to expect rich online content and services at little or no cost.

Complementing existing sector-specific laws and regulations, robust self-regulation has arisen to address concerns expressed by the Commission regarding certain online advertising practices. One example is found in the ubiquitous adoption of privacy policies, which are not mandated by federal law, but have been almost universally adopted due to the strong influence of industry self-regulation. Another example is the DMA and other industry leaders' release of the Self-Regulatory Principles for Online Behavioral Advertising in July 2009.[6] The Self-Regulatory Principles correspond with tenets proposed by the Commission Staff Report in February 2009,[7] and also address public education and industry accountability issues raised by the Commission. 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 the ability to deliver relevant advertising to consumers.

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. Consumers' embrace of e-commerce shows that they widely value the convenience, customization, and features that companies can offer online and that they do not perceive a harm arising from these services. It is evident that the prevailing U.S. approach to privacy regulation strikes an appropriate balance that benefits consumers and industry alike.

The DMA cautions against new legislation, regulation, or policies that could disrupt this beneficial cycle. In this environment, regulation that is specific to a technology or business model could deter entry, thwart innovation, and limit competition in the sale of online advertising. Unnecessary restrictions on online advertising could reduce the relevance of commercial messages to consumers. Moreover, if 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. The Commission should largely retain its existing approach of

---

[6] 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.

[7] Federal Trade Commission Staff Report, *Self-Regulatory Principles For Online Behavioral Advertising* (February 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

encouraging companies to provide consumers with notice of information practices and the ability to opt out of unwanted practices.

The DMA also believes that the Commission's current approach of promoting the fair information practices through harm-based enforcement respects the individualized nature of privacy preferences. The rapid embrace of new technologies, has illustrated that consumers have very different preferences about what information is private and what constitutes a sufficient reason to share information. The Commission's harm-based approach recognizes that tangible harm to consumers is the most meaningful and objective yardstick to determine whether regulation or enforcement is needed. It preserves consumers' individual choice and freedom unless an identifiable harm may ensue.

Finally, the DMA cautions that, given the penetration of the Internet into all areas of business, regulation of the online ecosystem amounts to regulation across industries. Any significant new regulation would likely have economic "ripple effects" that are difficult to predict. This type of instability is to be avoided at any time, but especially when the economy is fragile. The existing approach to private regulation has defended the fair information practices while fostering innovation. The DMA urges the Commission to focus on clarifying and refining the existing approach, which has been proven effective.

C. Specifically, the notice and choice model should remain a fundamental principle of U.S. privacy regulation.

The Report raises concerns about the notice and choice model. Not only is the notice and choice model one of the fundamental foundational principles in U.S. privacy law, it serves as the cornerstone of the nearly $2 trillion in annual sales attributable to marketing. Particularly in this economy, the U.S. government should tread carefully and resort to data-driven justifications before proposing approaches that could interfere with this robust sector of the economy. The DMA does not believe that the concerns identified so far by the Commission justify a wholesale abandonment of the notice and choice model.

New regulation is not warranted given that companies have already shown a widespread willingness to adopt detailed privacy policies. Moreover, the notice and choice model is familiar to consumers, and implemented in conjunction with the other fair information principles, has been effective for decades in allowing innovation to flourish while preserving consumer control over information. The emphasis should be on improving the notice and choice model based on additional guidance from the Commission which, to date, has issued little concrete advice on how website policies could be improved. Further Commission guidance on how privacy policies can be made more friendly to consumers would be welcome.

When practices for which a traditional privacy policy does not provide sufficient transparency are identified, self-regulation in dialogue with the Commission provides an effective forum to develop a specialized policy. As online operations become increasingly complex, case-by-case policy responses will help to ensure that consumers are receiving adequate notice to make a meaningful choice about whether to use a website or service. Industry's development of enhanced notice and choice in response to the Commission's call for action regarding online behavioral advertising, as part of the Self-Regulatory Principles, is an example of industry self-regulation addressing an area where the Commission called for a specialized policy response.

D. Industry self-regulation, developed in dialogue with the Commission, is generally the best approach to addressing privacy issues in the context of marketing practices.

A successful example of self-regulation is found in the *DMA Guidelines for Ethical Business Practice* ("Guidelines").[8] 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;[9]

- Not transfer personally identifiable health-related data gained in a medical treatment context for marketing purposes without the specific prior consent of the consumers;[10]

- 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;[11]

- Not rent, sell, exchange, transfer, or use marketing lists in violation of the Guidelines;[12]

- Provide notice of online information practices, including marketing practices, in a way that is prominent and easy to find, read, and understand, and that

[8] Direct Marketing Association Guidelines for Ethical Business Practice, *available at* http://www.dmaresponsibility.org/Guidelines/.
[9] Guidelines, Article 32.
[10] Guidelines, Article 33.
[11] *Id.*
[12] Guidelines, Article 35.

allows visitors to comprehend the scope of the notice and how they can exercise their choices regarding use of information;[13]

- Identify and provide contact information for the entity responsible for a website;[14]

- Comply with the new self-regulatory principles for online behavioral advertising, discussed above;[15]

- 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;[16]

- Restrict data collection and marketing for children online or via wireless devices, consistent with the Children's Online Privacy Protection Rule;[17] 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.[18]

The Guidelines also apply to what the Report calls "information brokers," who receive consumer data from a variety of sources and potentially use it for purposes that consumers never anticipated.[19] The Report recognizes that for these types of companies that do not have direct consumer facing relationships, it would be challenging to provide choice to consumers at the point of data collection or use. The Commission should recognize that industry self-regulation, including the DMA Guidelines, already effectively impose responsibilities on these types of companies for the benefit of the consumer. The DMA Guidelines require that information companies suppress consumer information when requested, honor consumer requests for more information about the nature and types of sources used to compile marketing databases, protect against the inappropriate use of sensitive information, and require their customers to state the purpose for which the data will be used.[20] These self-regulatory principles impose protections on consumer information while taking into account the unique position that these companies occupy in the information market.

---

[13] Guidelines, Article 38.
[14] *Id.*
[15] *Id.*
[16] Guidelines, Article 37.
[17] Guidelines, Article 16.
[18] Guidelines, Article 36.
[19] Report, p. 63.
[20] Guidelines, Article 36.

These examples are only a sample of the restrictions contained in the Guidelines, which provide DMA member companies with a comprehensive blueprint for ethical marketing practices. Compliance with the Guidelines is required for all DMA members and the DMA can take action to enforce compliance by its members. In addition, companies that represent to the public that they are DMA members but fail to comply with the Guidelines may be liable for deceptive advertising.

The DMA has a long history of proactive and robust enforcement. The DMA's Committee on Ethical Business Practice examines promotions and practices that may violate DMA Guidelines. The Committee works with both member and non-member companies to gain voluntary cooperation in adhering to the guidelines and to increase good business practices for direct marketers.

The DMA Guidelines have been applied to hundreds of direct marketing cases concerning deception, unfair business practices, personal information protection, and other ethics issues. In order to educate marketing professionals on acceptable marketing practices, a case report is regularly issued which summarizes questioned direct marketing promotions and how cases were administered. The report also is used to educate regulators and others interested in consumer protection issues about DMA Guidelines and how they are implemented.

The DMA Corporate Responsibility team and Ethics Operating Committee receive matters for review in a number of ways: from consumers, member companies, non-members, or, sometimes, consumer protection agencies. The Committee reviews the matters that are received by the DMA concerning possible violations of the ethics guidelines. Complaints referred to the Committee are reviewed against the Guidelines for Ethical Business Practice and if a majority of Committee members believe there is a potential violation, the company is contacted. If a potential violation is found to exist, the company will be contacted and advised on how it can come into full compliance. Most companies work with the Committees to cease or change the questioned practice. However, if a member company does not cooperate and the Committees believe there are ongoing guidelines violations, the Committees can recommend that action be taken by the Board of Directors and can make case results public. Board action could include censure, suspension or expulsion from membership, and the Board may also make its actions public. If a non-member or a member company does not cooperate with the Committees and the Committees believe violations of law may also have occurred, referral of the case is generally made to federal and/or state law enforcement authorities for their review. For example, in the period spanning February 2009 through February 2010, the DMA Ethics Operating Committee reviewed 34 cases, of which four were made public. One case during this period was referred to the Federal Trade Commission, United States Postal Inspection Service, and the Nevada Attorney General.

II. Specific Comments on the Report

A. Although a wide range of commercial entities may benefit from the Commission's views set out in the Report, the DMA cautions against requiring all commercial entities to comply with any "one size fits all" framework.

The Report[21] proposes to extend the Framework to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. This application of the Commission's Proposed Framework to all commercial entities may be a useful tool for companies to analyze their data practices. However, the DMA cautions that it would not be appropriate to impose a regulatory framework that applies to all commercial entities.

First, it is not feasible to devise a framework that applies to all commercial entities as a matter of regulation. In today's information economy, the wide range of data practices, rapidly changing technological platforms, and the diversity in the types of data generated and collected, especially in the online realm, all make it impossible to devise a single regulatory solution that would be suitable across entities. Any attempt to do so would likely result in punishing certain business models and technologies in favor of promoting others, instead of letting the marketplace encourage continued innovation. Second, a uniform regulatory framework would be a broad and unwarranted reformulation of current privacy rules that would confer obligations both upon entities that collect data directly from consumers as well as entities that do not have consumer-facing relationships. The Commission has not provided any basis for abandoning the sectoral approach to privacy regulation that, as detailed above, has permitted the Internet and the U.S. economy to flourish. Indeed, many entities that are covered by existing sector-specific laws could face inconsistent obligations. For these reasons, the DMA believes that the Commission should not attempt to impose a "one size fits all" regulatory framework across our widely varied, rapidly innovative private sector.

B. The DMA also opposes expanding privacy regulation or principles to include information that is not personally identifiable, such as Internet Protocol addresses.

Traditionally, the applicability of privacy and data security rules hinges on whether the data constitutes personally identifiable information ("PII"). Yet in recent discussions about PII, concerns have been raised that data that is not inherently personally identifiable, such as clickstream data, browsing behavior, and search queries, may nevertheless raise privacy concerns when it is significantly detailed or granular.

---

[21] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 2010) (hereafter, the "Report").

The DMA suggests that any effort to expand the definition of PII to include data that is not inherently personally identifiable would be detrimental to consumers by removing an important policy distinction that treats non-PII differently from PII. This distinction is familiar to consumers and makes intuitive sense. Many businesses, including many of the DMA's member companies, have built their entire business model around the distinction between PII and non-PII and have made strategic decisions in a number of critical areas based on this distinction.

Instead of expanding principles to fit the types of information for which they were not intended, the Commission should instead support efforts to anonymize and de-identify data. The Report downplays the significance of the distinction between PII and anonymized and de-identified data. There is no empirical evidence to support the idea that consumers equate the potential harm arising from the collection and disclosure of actual PII with a potential harm from the collection and disclosure of anonymized, aggregate data. Furthermore, there is no evidence to support the contention that, with appropriate safeguards, anonymized, aggregate data can be readily and easily reverse engineered.

C. While companies may benefit from using "privacy by design" as a lens to evaluate and improve their internal processes, this concept should not become a regulatory requirement.

The principle of "privacy by design" can provide companies with a helpful tool to guide the development of corporate privacy and data security practices.[22] This principle balances innovation and privacy by encouraging businesses to develop new technologies in a manner that respects consumer interests. Indeed, many companies already incorporate data security, reasonable data collection limits, sound retention practices, and data accuracy into a company's everyday business practices. Such protections are also promoted by industry groups including the DMA. The DMA Guidelines direct our members to (1) only collect, exchange, and use marketing data, (2) limit the use of marketing data for only marketing purposes, (3) keep sensitive data confidential, (4) establish information security policies and practices, (5) create and implement staff policies, procedures, and training measures to protect personally identifiable information, and (6) employ and reassess protective physical safeguards and technological measures, including data retention, destruction, and deletion practices.[23]

However, we are concerned that the Report goes on to enumerate several substantive restrictions in its discussion of "privacy by design." DMA members constantly reevaluate their data collection and retention practices in light of continuing changes in technology and ongoing guidance from the Commission. However, we firmly believe that data collection and retention limits should not be regulatory requirements. In

[22] Staff Report at 44-52.
[23] The Direct Marketing Association, *Guidelines for Ethical Business Practice* (revised January 2010) 16-21, *available at*, http://www.dmaresponsibility.org/Guidelines/.

our view, the promulgation of rigid standards or the imposition of onerous obligations in these areas would diminish innovation and consumer benefits, without advancing consumer privacy.

Introducing prospective and across-the-board restrictions on data collection could thwart valuable current and future uses of information, impeding the delivery of countless services and products that consumers value. In the online world in particular, wholesale restriction on data collection would interfere with the functionality and operation of the Internet. The Commission has not identified a public policy basis that justifies such a shift in current practices, nor does the Report appear to consider the potential negative results of the proposed restrictions. The proposed data collection standard, which would require companies to limit the collection of data to "information needed to fulfill a specific, legitimate business need," does not reflect the operational realties of data collection.[24] A single piece of data can be used for multiple purposes in carrying out business operations and serving consumers. For instance, the same data point could be collected and used for fraud protection, authentication, and marketing purposes. Thus, the DMA believes that data protection standards should be focused on uses of data rather than the collection of data.

Similarly, while the DMA supports the principle that data should be retained only for as long as there is a legitimate business purpose, we believe that this principle should not be imposed as a regulatory requirement. Different uses, businesses and industries benefit from different data retention limits, and the Commission has not provided any evidence that shows a need for specific time durations for data retention. Of the more than 40 states that have enacted data security and maintenance laws, no state law imposes specific time limits. Given this complexity, mandatory regulation is not appropriate. Moreover, any new guidance on data retention should account for the wide differences between types of data and data uses. It is also critical for any new guidance to recognize that new and valuable uses for data frequently arise as companies offer new products and services in response to customer interest and demand. For example, evolving uses of data in the social media context and in the data analytics context are fueling innovation in the next generation of consumer applications.

D. In the area of consumer choice, the DMA believes that the Commission's approach of identifying "commonly accepted practices" is too narrow and will thwart innovation. Instead, the Commission should focus on identifying a limited number of practices that *should* require choice.

The Report calls for a "simplification" of consumer choice that reduces the burden on consumers and businesses, by streamlining the choice model into meaningful choice for certain practices, with no choice required for a limited set of "commonly accepted practices." The Commission's approach to identifying "commonly accepted practices," however, is too narrow and will thwart innovation. The proposed framework

[24] Staff Report at 45-46.

does not provide guidance or an apparent means for new or existing practices to become "commonly accepted" over time. This could inhibit the development of new products or services. Moreover, designating only certain practices as "commonly accepted practices" creates an expectation that this finite list includes the only legitimate practices, and stigmatizes practices that are not enumerated, for example, third-party marketing generating trillions of dollars, as *per se* suspect.

Instead, the Commission should focus on identifying a limited number of practices that should require choice, not because they are not "commonly accepted," but because providing choice is appropriate. As discussed, below, transfers of data for third-party marketing, which are commonly accepted, legitimate, and provide consumer value, are among the practices for which choice should be provided.

1. **The DMA agrees with the Commission that choice should not be required with first-party marketing.**

The DMA and its members applaud the inclusion of first party marketing as a commonly accepted practice that does not require choice. First party marketing is clearly an information practice that has become common and ubiquitous over time, and that consumers have come to expect.

First-party marketing should be given an expansive definition. All first-party marketing should not require choice, irrespective of the channel in which the marketing occurs. Business affiliates and service providers of the primary marketer should be included because reliance upon them is extremely common and necessary for the efficient functioning of websites. Data enhancement, which can be impacted by choices provided to the transfer of marketing data from third parties, is also a first-party use of data once the information is transferred to the first-party marketer.

2. **The DMA believes that third-party data use and sharing are commonly-accepted practices, but that choice is appropriate for such practices in the area of marketing.**

Like first-party marketing, third-party sharing of data provides substantial benefits to consumers, including allowing access to consumer data by small businesses and start-ups, which lack the ability to collect and maintain large databases of consumer data in-house. This data is used, much like first-party data, to deliver targeted and relevant advertisements to consumers. Even first-party marketers depend upon third-party data to enhance their own information and provide better services and more relevant marketing offers to their existing consumer base. Small businesses as well as non-profits and government agencies and political organizations and candidates rely on using third-party data to in order to identify relevant consumers for their messages, products, and services and keep their marketing costs down. This information also assists political candidates, who use this information to communicate campaign messages to interested citizens.

Although, as noted above, third-party sharing of data for marketing is common, legitimate, and provides consumer value, it is a practice for which consumers should be given choice. Indeed, the DMA has maintained for some thirty years a "mail preference service," now called www.dmachoice.org, that allows consumers to exercise their choice to start or stop receiving mail from individual companies within four different categories of direct mail—credit offers, catalogs, magazine offers, or other mail offers—or from an entire category at once. DMA members commit to respecting consumer mail preferences in order to maintain and honor healthy consumer relationships.

While not specifically mentioned in the Report, it is equally common and legitimate for companies to supplement their own website performance data with third-party analytics to better understand consumers' website usage. Such analytics employ aggregate data, such as the total number of visitors to a particular website, and are not designed to target individuals or to collect or store individual personal information.

Companies routinely rely on third-party analytics to decide whether and how to make investments in their websites and businesses. Analytics guide companies in numerous areas, including identifying promising new retail locations for businesses, what products to offer, and how to redesign website content or features to be more consumer-friendly. Similarly, regulators and government agencies rely on research to help understand policy challenges such as how the increased broadband access would impact the economy. Given that these significant benefits to understanding the Internet ecosystem can be provided with virtually no impact on consumers, we believe that third-party analytic services should be recognized as an information practice for which consumer choice is not required.

3. When choice is provided, opt-out choice remains the appropriate form of consent for advertising and marketing practices, by both first and third parties, which do not involve sensitive information.

The Commission has promoted the importance of consumer notice and choice, which historically has been construed to require allowing consumers the opportunity to opt out of unwanted practices. This approach takes the default position of allowing beneficial data flows to proceed unless the individual expresses a contrary preference. In the marketing context, there are benefits with little to no corresponding harm to consumers by having their information included in a database and, thus, allowing consumers the opportunity to opt out has always been deemed an appropriate form of choice.

The DMA is concerned that opt-in consent, even on a limited scale, would drastically alter the online experience. Given the collaborative architecture of the Internet, data-sharing interactions between website owners and other companies are commonly required for the orderly functioning of a website. These interactions are currently seamless, happen out of the sight of the consumer, and facilitate website features and online benefits that consumers value. A requirement for opt-in consent will

disrupt this architecture. The constant appearances of notice boxes will annoy and frustrate consumers, and will dilute the impact of such mechanisms. The result of this change in the *status quo* will be to create the illusion of a harm in the minds of consumers, unsupported by reality, where none currently exists.

To the extent that the Commission's interest in opt-in consent is related to a concern about the sufficiency of disclosures about data practices to enable consumers to make more informed decisions, the DMA submits that such a concern would be better addressed by focusing on methods to improve the provision of notice. There is no indication that most data flows harm consumers or should be discouraged. In particular, the Commission has not pointed to evidence of any concrete harm to consumers from the legitimate data practices that support online advertising. The Commission has not produced evidence of either a societal consensus against such data sharing or consumers' willingness to accept a changed Internet experience in exchange for reducing such sharing because his evidence does not exist. Such a drastic shift in policy should not be undertaken without overwhelming evidence of consumer harm necessitating such a fundamental change in policy and practice.

The results of a recent study conducted by TRUSTe on the effectiveness of an icon near advertisements on the Publishers Clearing House website found that more than half of the people who saw the icon and clicked through to the control panel said they found the information about interest-based ads and advertising networks to be helpful. This information included a three-step process to learn more about the ads, set preferences to opt-out of interest-based ads, and give feedback to TRUSTe about the process. Although the icon was accessed 56,000 times with 44,000 unique views, only 1.1% of the website's viewers chose to opt-out of all advertising networks.[25] The results of this study demonstrate that the majority of consumers, after learning more about online behavioral advertising, do not become alarmed about potential privacy concerns but instead will choose to continue receiving targeted advertisements.

4. Finally, the DMA believes that choice can and should be provided without interfering with the consumer experience.

The DMA believes that while choice should be readily available to the consumer, it should not interfere with the consumer experience. It does not have to be available at the point of information collection. For example, the Report states for an offline retailer, the disclosure and consumer control should take place at the point of sale by having the cashier ask the customer whether he would like to receive marketing offers from other companies.[26] This interaction at point of sale would interfere with the consumer experience and is likely to result in a hasty and uninformed decision by the consumer—precisely the opposite intended effect of the proposed framework which is supposed to encourage thoughtful, informed choice by the consumer. Similarly, in the online, social

[25] Tazina Vega, *Studies Find Success in Use of Privacy Icons*, N.Y. TIMES, Nov. 16, 2010.
[26] Report, p. 58.

media, and mobile environment, a consumer's ability to exercise choice should be made available in a way that makes sense within the context of the webpage and the technological medium being used. Many consumers are extremely comfortable with the online retail experience and do not need to be inundated with additional disclosures and information at the point where they are entering their personal information. Provided that the information is reasonably accessible to the consumer who wishes to seek additional information, it should not interfere with the experience of the consumer who is comfortable with the process.

E. The Report calls for a "Do Not Track" choice mechanism in the context of online behavioral advertising. The Self-Regulatory Principles for Online Behavioral Advertising, currently entering widespread cross-industry implementation, successfully address the Commission's call for a uniform and enforceable choice mechanism.

The Report calls for a "do-not-track" choice mechanism in the context of online behavioral advertising. Despite the headline-grabbing name, the specifics of the proposal seem instead to be calling for a uniform consumer choice mechanism which, the Report concedes, can be achieved through robust, enforceable self-regulation. The government should not be involved in the creation of a do-not-track mechanism. There is no empirical evidence supporting a harm to consumers resulting from online behavioral advertising. If the government builds and maintains a mechanism for controlling online behavioral advertising, the government will effectively create the misimpression of harm where none exists and will generate consumer mistrust. The DMA supports the concept of choice and the ability for uniform choice in the context of online behavioral advertising. Yet we strongly believe that industry self-regulation can achieve far more compliance and effectiveness than regulation in this context, by being responsive to changes in technology and flexible enough to handle new challenges as they arise. Although the Report acknowledges the developments in this area, it notes that "an effective mechanism has yet to be implemented on an industry-wide basis."[27] This assertion is incorrect.

The Self-Regulatory Program for Online Behavioral Advertising, described here, provides just this mechanism. This significant self-regulatory effort is already underway. It provides the uniform consumer choice for online behavioral advertising contemplated by the Commission. The Program began registering participating companies in October 2010 and the Advertising Option Icon that indicates a company's use of online behavioral advertising has already been featured in billions of ad impressions during its first month of use. We expect business participation to become even more robust in the coming months. This innovative solution will ensure that consumers can easily receive notice of the data practices of third parties. After the expense and effort that the industry has expended on the Program, it deserves the opportunity to attempt to fully launch the program and measure the results before replacing it with an untested regulatory

[27] Report, p. 64.

mechanism. The significant progress in this initiative is discussed in a separate set of comments.

In public statements, some members of the Commission have indicated that industry has been slow to implement self-regulatory solutions. These statements lack comparative contexts, appearing not to take into account the length of time it has taken the Commission to implement its own solutions to far simpler technological challenges. For example, it took the Commission seven years and five months after enactment of the Children's Online Privacy Protection Act to determine that the anticipated availability and affordability of secure electronic mechanisms for obtaining parental consent—upon which the sliding scale approach to verifiable parental consent was predicated—had not occurred.[28] It took the Commission four years and five months after enactment of the CAN-SPAM Act to issue the definitions that currently apply under the CAN-SPAM rule, which requires senders of commercial e-mails to include a link to an opt-out mechanism.[29] Furthermore, the obstacles to prompt implementation multiply when the task requires, coordination with other stakeholders, as the Commission knows from its far more modest experience of having to coordinate with only seven financial regulatory agencies to develop a short privacy notice to be issued by financial institutions under the Gramm-Leach-Bliley Act. That task spanned five years and 11 months from issuance of an advanced notice of proposed rulemaking to promulgation of final rule.[30] By comparison, industry moved consistently and diligently in coordinating dozens of trade associations and hundreds and thousands of companies as they developed and accepted standards in a very difficult area, developed technological specifications for them, and implemented and rolled out the a comprehensive self-regulatory mechanism in only 15 months.

The DMA worked with a coalition of other leading trade associations and companies to develop Self-Regulatory Principles. These Principles require advertisers and websites to inform consumers about data collection practices and enable them to exercise control over that information. The Self-Regulatory Principles 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."[31] The 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;

---

[28] *See* Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, P.L. 105-277 (Oct. 21, 1998); 71 Fed. Reg. 13247 (March 15, 2006).
[29] *See* P.L. 108-187 (Dec. 16, 2003); 73 Fed. Reg. 29654 (May 21, 2008).
[30] *See* 68 Fed. Reg. 75164 (Dec. 30, 2003) (ANPRM); 74 Fed. Reg. 62890 (final rule) (Dec. 1, 2009).
[31] 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.

In particular, the DMA believes that the promising Self-Regulatory Principles and the cross-industry Self-Regulatory Program for Online Behavioral Advertising, both of which were spurred by the Commission, should be given an adequate opportunity to continue and to be effective before additional regulation is considered in this area. The Principles are designed to apply to the diverse individual actors that work to deliver advertising intended to enrich the online consumer experience, and to foster consumer

In October 2010, the nation's largest media and marketing associations launched the Self-Regulatory Program for Online Behavioral Advertising (the "Program"), built on the Self-Regulatory Principles. Consumers now have 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). This choice is easily accessible to consumers and was designed to be consumer friendly. Upon visiting the AboutAds homepage, consumers are greeted with a large button leading them directly to the Consumer Opt-Out page. *See* Screenshots from AboutAds.info, Attachment A.

The icon has already appeared in billions of ad impressions across the Internet. More than a trillion impressions are expected to have been placed by the end of the year. Since November 2010, consumers have been able to visit the AboutAds Consumer Opt-Out Page to easily opt-out of some or all of the interest-based ads they receive, if they choose to do so. This choice page is linked to through the Advertising Option Icon. The choice to opt-out is persistent to a consumer's browser as long as the consumer does not

delete the cookie through which opt-out is obtained. Close to 60 companies are currently participating in this choice mechanism, providing consumers with control over whether their data is collected or used for online behavioral advertising. Dozens of additional companies are in the process of joining the Program.

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. DMA will continue the complaint-based program that it has run for more than forty years, supplementing that long-standing program with the use of monitoring technology that enables DMA to look proactively for compliance issues across the Internet. This technology will also be used to gather evidence to inform investigation of the complaints received.

Set forth below are answers to specific questions posed by the Commission on this issue.

- *How should a universal choice mechanism be designed for consumers to control online behavioral advertising?*

The Commission encouraged the development of a universal self-regulatory program. The Advertising Option Icon, already featured in billions of ad impression, is an interactive solution for consumers who wish to learn more about targeted advertising and to control their preferences in this area. Unlike a browser based solution, which discourages consumer transparency by requiring consumers to take the initiative to learn how to change their browser controls and preferences, the Advertising Option Icon is attached to the advertisement itself, and offers choice to the consumer directly through the advertisement. This solution is easily scalable to the entire Internet ecosystem. A copy of real ads featuring the Icon are included as Attachment B to show how transparent to consumers the Icon is.

The Icon is a universal choice mechanism. The AboutAds Consumer Opt-Out Page currently allows consumers to opt-out of online behavioral advertising from nearly 60 companies which, combined, place over 90% of all behavioral advertisements on the Internet. Dozens of additional companies are currently in the process of being integrated into the tool and we expect the choice to be ubiquitous at that time.

- *How can such a mechanism be offered to consumers and publicized?*

The DMA is not clear why the Commission would favor a browser-based solution after its calls for transparency in its self-regulatory report. A browser based solution has not been vetted by a broad cross-section of the online advertising industry, it is not transparent to consumers, and it is not scalable across the Internet ecosystem. Such a

system is not the simplest, consumer friendly way to inform consumers of their choices. Some of the browser based "solutions" that have been suggested require that consumers themselves create a so-called black list. We are at a loss to understand how a large cross-section of average consumers would (a) know how to do this; and (b) have the time to do this. This is difficult and labor-intensive, unlike the Advertising Option Icon, which appears ubiquitously, and hence, is transparent, and is easy to use.

- *How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers?*

The Advertising Option Icon is placed within the advertisement itself. This provides consumers with the most clear and easy-to-find means to learn additional information about the actual advertisement that the consumer is viewing in real time. The Advertising Option Icon gives consumers real choice that uses a persistent cookie, and, therefore, sustainable across the web and across sites.

- *How can such a mechanism be designed so that it is clear to consumers what they are choosing and what the limitations of the choice are?*

The goal of a successful self-regulatory program should not be measured by the number of consumers who choose to opt-out of targeted advertising. By using the number of consumers who choose to opt-out as the metric for success, the risk arises of unfairly and unnecessarily stigmatizing targeted advertising as a practice that causes consumer harm. There is no evidence that it does so. Widespread deployment of the Advertising Option Icon, which provides instant information to consumers, combined with consumer education, is the best means for making the scope and limitations of the choices clear to consumers.

- *What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?*

One of the risks of a government mandated Do-Not-Track mechanism is that consumers may come to perceive targeted advertising as a practice that causes consumer harm. In that scenario, if large numbers of consumers choose to opt-out of targeted advertising, the result will not be less advertising. Instead, consumers will receive a higher volume of non-targeted advertising and advertisements that do not interest the consumer, resulting in a less efficient Internet and fewer choices for consumers in terms of free online content and services.

- *How many consumers would likely choose to avoid receiving targeted advertising?*

The DMA is confident that the consumers who understand how targeted advertising works would not opt-out of this type of advertising. The Commission has been promoting an expectation to consumers that a Do-Not-Track mechanism would

result in little or no advertisements. This is not true. The real result to consumers who choose to avoid receiving targeted advertising is likely to be a higher volume of advertising, most of which will be of no interest to the consumer.

Consumers who understand that targeted advertising causes no harm to consumers and significant benefits will not opt-out of targeted advertising. After years of championing less but more targeted advertising, the Commission appears to be moving the goal post right as industry has developed a solution that provides easy-to-use universal choice to consumers.

- *How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided?*

The Advertising Option Icon has only been in effect for a few months, and numbers regarding the number of consumers who have utilized the opt-out mechanism are not yet available. Measuring success in terms of a high percentage of consumers who opt-out is the wrong metric. Instead, success should be measured by the barometer of how widespread the choice has been offered. By this measure, the Advertising Option Icon promises to be an overwhelming success. It has already been featured in billions of ad impressions and is expected to be featured in more than a trillion ads by the end of the calendar year.

- *What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?*

If large numbers of consumers elect to opt-out, the result will be an increase in advertisements of little interest to consumers, and a greater increase in spam advertisements. The overall result will be a less efficient Internet, with fewer choices in content and services for consumers. This, in turn, will result in less innovation and fewer jobs. We also anticipate that more sites will have to charge for content because without targeted advertising, they are no longer economically sustainable. Finally, we anticipate a significant economic downturn for small business and retailers because they no longer will have the ability to reach a likely/targeted consumer with an ad for a product or service when it is relevant and timely.

- *In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them?*

It has never been the case that consumers would be able to opt-out of receiving ads completely as asserted in this question. Consumers would only be opting out of

receiving targeted advertisements, and in exercising this option, would be signing up to receive a greater amount of irrelevant advertising.

The use of advertising to subsidize online content and services has long been recognized as a unique comparative advantage for driving online commerce in the United States. Some advertisers, such as Google and BlueKai, are working on novel solutions to give consumers more granular options regarding the targeted advertising they receive. The market will determine whether these experiments are effective. Advertising will remain a fact of the online experience, but its overall relevance and volume remain to be determined.

A system that allows consumers to make so-called granular choices does not recognize that consumers' interests evolve and change over time. Consumers develop new interests, hobbies and concerns, and consumer-provided information about getting information about "travel" or "cooking" may no longer be relevant. Imposing the burden on consumers to update "preferences" seems to be a step backward when we now have the technology to ensure that consumers get information and ads about things that interest them precisely when that information is relevant and timely.

- *Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications?*

The mobile market is rapidly changing. The industry continues to evaluate the mobile market, and will develop a response when the needs of the mobile market can clearly be determined. In the meantime, the Commission should not interfere with this dynamic, fast-changing market platform, which is outside of its jurisdiction anyway.

- *If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?*

No, the Commission should not recommend legislation requiring such a mechanism. The Commission called for industry self-regulation and in response, the industry built and deployed an effective, ubiquitous choice mechanism. This mechanism should be given time to take effect and work. Without evidence of harm to consumers, and the detrimental effect such legislation would have on the online economy, legislation in this area is not warranted.

F. The DMA generally supports transparency in data practices but has concerns about the Commission's proposals for new and burdensome obligations.

1. The Report does not provide evidence to support any need for new data access, correction, and accuracy standards beyond the consumer rights already provided by key sector-specific laws.

The DMA does not agree with the Report's call for a standardized means for providing consumer access and correction to data. The Report proposes a sliding scale approach whereby the extent of access would depend on the sensitivity of the data and its intended uses. For example, the Report states that companies that maintain data for marketing services "might disclose the categories of consumer data they possess and provide a suppression right that allows consumers the ability to have their name removed from marketing lists."[32] It also states that "companies should take reasonable steps to ensure the accuracy of the data they collect, particularly if such data could be used to deny consumers benefits or cause significant harm" and suggests that one way to help consumers learn that data had been used to deny them a benefit would be "to require that entities that deny benefits to consumers based upon information obtained from information brokers provide notice to the affected consumer, similar to an adverse action notice under the Fair Credit Reporting Act ("FCRA"). This would allow the consumer to contact the information broker and access and potentially correct the data upon which the denial was based."[33] Despite these assertions, which are unsubstantiated, the DMA believes that the Report does not actually identify a new need for data access, correction and accuracy standards.

The Report does not provide any evidence that consumers are denied some benefit from authentication services, since requesting additional documentation from consumers is the result of the failure to be authenticated. Consumers do not need expanded access rights for marketing data that is predicated on inferences. They already have rights to access data used to make decisions of substance, including the FCRA, the Fair Billing Act, the Fair Debt Collection Practices Act, and the Health Insurance Portability and Accountability Act. For example, under the FCRA, consumers are already entitled to receive notices for the most important adverse actions that may involve the use of personal information, such as denials of employment, credit, insurance, or housing. The FCRA also provides the affected consumer with a copy of the information that was used in making the adverse decision. Applying an access right more broadly than in the FCRA context would impose burdensome compliance costs on a huge number of businesses, without any evidence of harm, and with little or no additional benefit to consumers.

In contrast to the purposes of data governed by statutes like the FCRA, marketing data sets are largely benign and do not require access and correction. Currently, there is

[32] Report, p. 74.
[33] Report, p. 76.

no public policy basis that supports accuracy for marketing and advertising data. In general, marketing causes no identifiable harm to consumers. 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 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 correct 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. Expanded access 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 to accompany them. When viewed as a whole, the enormous expenditures and burdens are not warranted by data that does not cause any identifiable harm to consumers.

2. **The DMA would welcome additional guidance from the Commission regarding how complex data practices can best be communicated in privacy policies; however, the DMA notes that current policies are partly shaped by the Commission's enforcement focus on this area.**

As noted above, further Commission guidance on how privacy policies can be made more friendly to consumers would be welcome. In order to encourage adoption of such guidance, it would also be helpful to provide a safe harbor mechanism so that companies that follow the Commission's guidance are shielded from liability. For example, the Commission and other agencies issued a new model privacy notice for financial information, based on consumer testing. The use of this model notice affords financial institutions a safe harbor from liability, which provides a strong incentive to adopt the notice. A similar effort for website privacy policies would assist companies in complying with the Commission's expectations.

Privacy policies tend to be complex because online data practices often defy easy characterization. The Commission should also recognize that company privacy policies are shaped, in part, by efforts to respond to past enforcement actions by the Commission, which has repeatedly used its Section 5 authority in past years to pursue enforcement actions based on misstatements or nondisclosures in privacy policies. The Commission should not be surprised that companies seek to avoid such liability by "cataloging" their

information practices with precisely worded language in an effort to make sure that a complete list of their practices is disclosed to consumers.

The Commission's enforcement pattern has created incentives for the continued expansion of privacy policies, both in terms of length and complexity, in an effort to capture all behaviors that may subject the company to future liability. A number of Commission investigations that have looked closely at website privacy policies also encourage the continued expansion of privacy policies. The current regime provides no comfort to companies that choose to rollback and simplify their privacy policies that they will not be subject to liability for nondisclosure of certain data practices. In the face of these risks, it is commendable that commercial websites almost universally post privacy policies that are exceptionally transparent about the company's operations.

* * *

The DMA thanks the Commission for the opportunity to submit these Comments, and we look forward to working with the Commission as it continues to evaluate these important issues. The DMA also urges the Commission to strongly consider the joint comments of the American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Direct Marketing Association, and Interactive Advertising Bureau, and the comments filed by the coalition of self-regulatory groups that includes DMA. Further, the DMA includes for the Commission's consideration, as Attachment C, the comments it filed with the Department of Commerce in response to their request for public comments on "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," submitted on January 28, 2010.

Please contact Linda Woolley at 202-861-2444 or lwoolley@the-dma.org with any questions.