August 5, 2014

Submitted Via Email: privacyrfc2014@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Attn: Privacy RFC 2014
Washington, DC 20230

RE: Request for Comment on "Big Data and Consumer Privacy in the Internet Economy"

To Whom It May Concern:

On behalf of the Direct Marketing Association ("DMA"), we provide comments in response to the National Telecommunications and Information Administration's ("NTIA") request for public comment on "big data" and consumer privacy published on June 6, 2014.[1]

DMA is the world's largest trade association dedicated to advancing and protecting responsible data-driven marketing in the United States and globally.[2] Founded in 1917, DMA represents thousands of companies and nonprofit organizations that use and support responsible data-driven marketing practices and techniques. DMA provides data-driven marketers the voice to shape policy and public opinion, the connections to grow members' businesses, and the tools to ensure full compliance with responsible and best practices as well as professional development.

Marketers have engaged in the responsible collection and use of data for marketing purposes for more than 100 years. The recent advent of large data sets or "big data" (and the computing power to make use of them) has enhanced, but not changed, the basic role that marketing plays in the United States ("U.S.") economy. Namely, the analysis of big data by marketers has made it easier and more efficient to connect consumers with the products and services they desire. According to a recent study, the resulting Data-Driven Marketing Economy ("DDME") added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in 2012 alone.[3]

The remarkable growth of the DDME is due in part to the flexible regulatory framework applied to the use of data for marketing purposes. This framework combines specific, harm-based legal restrictions, with enforceable industry self-regulation that responds to a rapidly changing business landscape. It is this flexible framework of protections governing the

[1] Big Data and Consumer Privacy in the Internet Economy, 79 Fed. Reg. 109, 32714-32716 (June. 6, 2014).
[2] www.thedma.org
[3] Deighton and Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy* (2013), *available at* http://ddminstitute.thedma.org/#valueofdata (hereinafter "*The Value of Data*").

responsible use of data for marketing purposes that has helped drive innovation and fuel the U.S. economy.

I. Benefits of Big Data

DMA encourages the NTIA to consider, from the outset, the benefits of big data and the successful track record of the current U.S. approach to privacy regulation. The collection and use of data for marketing purposes has been supporting our nation's economy for more than 100 years. The goal of marketing has always been to connect consumers with the products and services they desire, when they desire them. The analysis and use of big data by marketers has not altered this goal, but has made this task more efficient.

While studies of big data have cited speculative warnings about the abuse of data, research has been able to show the concrete economic benefits of data. A recent study commissioned by DMA's Data-Driven Marketing Institute ("DDMI") and conducted independently by Professors John Deighton of Harvard Business School and Peter Johnson of Columbia University, entitled, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy* ("*Value of Data*"), quantifies this fact.[4] As noted above, the *Value of Data* study found that the DDME added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in 2012 alone. The study also found that an additional 1,038,000 jobs owe part of their existence to these DDME jobs. The study estimated that 70% of the value of the DDME – $110 billion in revenue and 475,000 jobs nationwide – depends on the ability of firms to share data across the DDME.

The billions of dollars and hundreds of thousands of jobs that the DDME has provided to the U.S. economy can be linked to the responsible use of data by marketers. Responsible data use benefits consumers and our society. For nearly a century now, DMA members have been collecting and analyzing consumer data to make it easier and more efficient to connect consumers with the products and services they desire. Such techniques have expanded to the online environment, helping businesses provide customized offerings to an even broader consumer audience. This growth has occurred in the context of a robust self-regulatory environment that continues to focus on expanding transparency and limiting harms to consumers.

Innovative applications of marketing analytics to big data provide benefits to society every day by making it more likely that an offer will be valuable to the consumer who receives it. For example, a retailer might look at what a customer has purchased at a particular store, through its website, and from its mobile site, and then analyze those purchases in comparison to others who have bought those items. Using analytics, the retailer will predict whether a customer is more likely to want a coupon for jewelry or for kitchen appliances and use the same data to identify and improve the channels where consumers are more likely to purchase and engage with the retailer's products. When successful, these techniques give consumers more information as they navigate the commercial marketplace and help consumers to obtain the goods and services they desire at competitive prices.

[4] Deighton and Johnson, *The Value of Data*, at 3.

Marketing data analytics also offer broader social benefits, outside the realm of commercial marketing. For example, charities and other nonprofit organizations use big data analytics to support their missions. They use the same analytic techniques as marketers to help reach audiences more likely to support their cause and to more efficiently reach those in greatest need of assistance. Such analytics help lower fundraising costs, freeing up donated funds to work on achieving the organization's societal mission.

Today, the goal of marketers remains the same—to use data and analytics to connect with customers and consumers in meaningful ways. While modern techniques are more sophisticated, the fundamental approach remains the same as well—predicting consumer propensity for the purpose of delivering relevant and meaningful marketing offers and advertisements to consumers.

The practice of data-driven marketing was begun in the U.S. more than a century ago, and the burgeoning DDME is a uniquely American creation as well. Just as the United States created digital market-making media by commercializing the Internet browser in the 1990s, so it created postal market-making media when Montgomery Ward developed the mail order catalog in 1872. Today, the U.S. leads the world in data science applied to the marketplace. Ideas developed in the U.S. by American statisticians and econometricians, running on U.S.-designed hardware, and coded in algorithms developed and tested in the research offices of U.S. firms, are used to generate revenues throughout the world. This has established the data-driven marketing industry as a major export industry, and the *Value of Data* study confirmed that the DDME is a net export contributor to U.S. economic well-being. DDME firms derive a considerable portion of their revenue abroad (sometimes upwards of 15%) while employing nearly all their workers in the United States.[5]

The framework of existing sectoral laws and self-regulatory protections that govern the use of big data for marketing purposes—which has been successful for consumers and businesses alike—stands in contrast to the more prescriptive data protection regimes that have been adopted elsewhere in the world. The U.S. framework combines specific legal restrictions, focusing on misuse of data that can cause identifiable harms, with enforceable industry self-regulation that nimbly responds to an ever-changing marketplace. It is this agile, flexible framework of protections that has helped drive innovation and fuel the U.S. economy.

In Question 12 of the Request for Public Comment ("RFC"), NTIA references the White House Big Data Report's discussion of how data can be used improperly to cause certain societal harms, and asks whether new legislation is needed to address such improper use in the big data context.[6] DMA believes that the current U.S. legal framework provides ample protections for consumers by focusing on particular areas where the nature of the data, if misused or misappropriated, could cause discernible harm to consumers. For example, the Health Information Portability and Accountability Act ("HIPAA") regulates certain health data; the Fair Credit Reporting Act ("FCRA") regulates the use of consumer data for eligibility purposes; the

[5] Deighton and Johnson, *The Value of Data*. See summary of study, at 2, *available at* http://ddminstitute.thedma.org/files/2013/10/DDMI-Summary-Analysis-Value-of-Data-Study.pdf.
[6] 79 Fed. Reg. at 32716.

Children's Online Privacy Protection Act ("COPPA") addresses personal information collected online from children; and the Gramm–Leach–Bliley Act ("GLB") focuses on consumers' financial privacy. This harm-based approach to regulation has allows the private sector to continue to use data responsibly including, in most cases, to enable the delivery of more relevant marketing. These sectoral laws are supplemented by industry self-regulatory principles and this combination has proven to be a successful means of advancing innovation, while also providing consumers with transparency and control over their data choices as appropriate.

Big data has not created new concerns regarding the private sector's responsible use of marketing data for marketing purposes. Regardless of quantity, data is data – it may be used for good or for harm. The scope of data has not made existing protections less valuable or less effective, and the focus of policy frameworks should continue to be on uses of data shown to be harmful to consumers, rather than on restricting the responsible use of data for marketing purposes. Indeed, the White House Big Data Report ("White House Report") recognized this, and focused its discussion of big data on potential misuses of data, not on the collection of data for legitimate uses.[7] Instead of focusing on the potential, speculative harms discussed in the White House Report,[8] the U.S. privacy framework should continue to focus on concrete consumer harm.

The robust and successful framework has already led to the thriving DDME, and to a marketplace of innovative digital goods and services that consumers embrace. DMA encourages NTIA to see the value in the U.S. tradition of focusing on discernible, concrete harms to consumers and to exercise caution in considering any new restrictions on the free flow of data that could impact the United Sates' well-functioning and data-driven economy.

II. Value of Self-Regulation

Questions 13 and 16 of the RFC discuss the value of self-regulation and accountability mechanisms. Consumers have enjoyed both meaningful privacy protections and the benefits of data-driven marketing under the existing U.S. approach in which enforceable industry self-regulatory principles (or codes of conduct) supplement certain sector-specific laws. Industry self-regulation is more flexible and adaptable than legislation, and therefore self-regulation can adapt quickly to changes in consumer expectations or available technologies. This is especially necessary in the rapidly evolving online and technology marketplaces. In contrast, legislation tends to be prescriptive and is difficult to update.

The *DMA Guidelines for Ethical Business Practice* ("*DMA Guidelines*") are one example of longstanding and successful self-regulatory principles that provide meaningful controls and accountability to ensure that marketing data is used responsibly for marketing purposes.[9] The Guidelines include, among other items, standards for offline and online data practices that

---

[7] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President (May 1, 2014) at 55, *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[8] *Id*. at 51.
[9] Direct Marketing Association, *Guidelines for Ethical Business Practice* (Jan. 2014), *available at* http://thedma.org/wp-content/uploads/DMA_Guidelines_January_2014.pdf.

incorporate key Fair Information Practice Principles ("FIPPs") (*e.g.*, providing notice of online information practices including marketing practices, providing consumers with choice about receiving marketing offers). Specifically, the *Guidelines* require choice and transparency regarding responsible collection and use of marketing data. For example, article 31 of the *Guidelines* provides for consumer choice with respect to the collection, use, and transfer of personally identifiable data.[10] The *Guidelines* are updated regularly by DMA's Ethics Policy Committee to account for changes in the way consumers and marketers create and engage with data.

For more than four decades, DMA has helped ensure that data is used responsibly through the robust and proactive enforcement of the *Guidelines* against both DMA members and non-member companies across the DDME. The *DMA Guidelines* have been enforced in hundreds of direct marketing cases concerning deception, unfair business practices, personal information protection, and other ethics issues. In addition, companies that represent to the public that they are DMA members but fail to comply with the *DMA Guidelines* could be subject to enforcement under Section 5 of the Federal Trade Commission Act and comparable state laws.

DMA receives matters for review in a number of ways: from consumers, member companies, non-members, and consumer protection agencies. Complaints referred to DMA's Ethics Operating Committee are reviewed against the *DMA Guidelines* and if a potential violation is found to exist, the offending organization is contacted, investigated, and advised as to how it can come into full compliance. Most companies work with the Ethics Operating Committee voluntarily to cease or change the questioned practice.

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. However, if a company does not cooperate and the Ethics Operating Committee believes there are ongoing violations of the Guidelines, it can recommend that action be taken by the Board of Directors and can make case results public. For example, in the period spanning February 2012 through June 2013, DMA's Corporate & Social Responsibility Committee reviewed 55 cases and 12 of these were made public. Additional Board actions could include public censure, suspension or expulsion from DMA membership. DMA also refers cases to federal and state law enforcement authorities for review when appropriate.

With the rise of the online advertising ecosystem, DMA joined with other leading advertising and marketing trade associations to spearhead the establishment of the Digital Advertising Alliance ("DAA") in 2009. The DAA administers *Self-Regulatory Principles for Online Behavioral Advertising*, *Self-Regulatory Principles for Multi-Site Data*, and *Application of Self-Regulatory Principles to the Mobile Environment* (collectively, "Self-Regulatory Principles") in order to provide consumers with effective transparency and choice regarding the collection and use of web viewing information and data gathered from mobile devices including precise location data and personal directory data.[5] DMA is one of two accountability programs enforcing the DAA program. The DAA program also prohibits the use of marketing data for credit eligibility, employment eligibility, healthcare eligibility, or insurance eligibility or

[10] See *Guidelines* at p. 20.

underwriting purposes. In 2012, the DAA was commended by the White House, the Secretary of Commerce, and the Chairman of the Federal Trade Commission for its work.[11]

DMA and DAA self-regulatory programs are examples of how the data-driven marketing industry effectively regulates its marketing data practices, delivering enhanced transparency and control to consumers. Informed by our experience with these self-regulatory programs, DMA strongly supports industry self-regulation as the most efficient and effective means of addressing both online and offline marketing and advertising information practices in a manner that takes into account consumer privacy considerations while allowing data-driven innovation to flourish. Unlike legislation, which is static and runs the risk of codifying practices that may become out-of-date even before a bill turns into law, industry self-regulation is nimble by its very nature and thus better suited to provide protections in cutting-edge areas such as the information economy.

Any potential legislation that would touch on consumer privacy should respect the successful and longstanding U.S. framework of sectoral laws complemented by self-regulatory programs. One valuable addition to this framework would be nationwide federal data breach notification legislation that would preempt the current patchwork of 49 state breach notification laws with which industry must comply currently. A single federal standard would reduce the cost of compliance, as well as increase the quality and consistency of consumer notice nationwide.

III. Applicability of the "Consumer Privacy Bill of Rights" to Big Data

Questions 1, 2, and 3 of the RFC address the applicability of the Consumer Privacy Bill of Rights to big data, and the development of a "responsible use framework." The Consumer Privacy Bill of Rights was articulated by the White House in its February 2012 Report entitled "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy."[12]

With respect to whether the advent of big data requires a new framework or a formal codification of the Consumer Privacy Bill of Rights, DMA believes that the existing sectoral approach should be maintained. The existing framework sufficiently balances innovation and privacy considerations in the era of big data.

As a historical analogy, during the rapid expansion of the Internet in the 1990s, the federal government considered comprehensively regulating the Internet and related connectivity through formal legislation, but ultimately adopted the approach we have today—namely, a "sectoral" framework that addresses particular areas of concern, such as children's online privacy or specific sectors perceived as handling sensitive information (*e.g.*, healthcare and financial services). These sectoral laws are supplemented by industry self-regulatory principles

---

[11] Speech by Danny Weitzner, *We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age* (February 23, 2012), available at http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age (last visited June 3, 2014).

[12] White House (Feb. 2012), at 1, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

to successfully promote the responsible online and offline collection and use of data. As a direct result of the decision to adopt this approach, the Internet continues to foster unprecedented growth in the data-driven economy.

According to the 2012 White House report, the Consumer Privacy Bill of Rights "applies comprehensive, globally recognized Fair Information Practice Principles (FIPPs) to the interactive and highly interconnected environment in which we live and work today."[13] We believe that the FIPPs remain a useful tool for companies to use in analyzing their practices, and the spirit of FIPPs has been incorporated for decades into successful industry self-regulatory principles that have the flexibility to keep pace with new technology and market offerings. For instance, the DAA *Self-Regulatory Principles* discussed above provide enforceable standards that incorporate key features of the FIPPs, implemented through innovative technical mechanisms that reflect how consumers interact with online advertising.

Other successful frameworks further highlight the success of the existing approach to data governance and its continued viability in the big data context. In the case of facilitating the responsible use of data across jurisdictions and borders, the "safe harbor" programs negotiated by the United States play a critical role in addressing online and offline information practices. The United States – European Union ("E.U.") Safe Harbor allows companies to self-certify that they comply with certain principles consistent with the E.U. Data Protection Directive, allowing cross-border data transfers to take place and promoting the success of U.S. companies in overseas markets. The DMA Safe Harbor Program provides a participating member with assistance in preparing to self-certify to Safe Harbor (e.g. developing a privacy policy based on the Safe Harbor Privacy Principles), a third-party dispute resolution mechanism, and a distinctive mark for use on the member's website.[14] As of mid-2013, the DMA Safe Harbor Program was serving 62 participating member companies. These programs offer efficient and enforceable protection for the international flow of data into the U.S. from the E.U.

In the context of this RFC and the suggestion that legislation based on the Consumer Privacy Bill of Rights is being considered, DMA believes that the Administration should opt for continuing existing self-regulation and programs like the "safe harbors" as accepted means of providing transparency, choice, individual participation, security, and enforcement for consumers, among other goals embodied in FIPPs. Maintaining this approach would help ensure that the U.S. remains an innovative leader in the information economy, while also providing consumers with meaningful protections.

IV. Notice and Choice

In this section, responding primarily to Question 4, DMA addresses: (1) the continued viability of the notice and choice model and (2) concerns about using "respect for context" as a basis for data restrictions.

---

[13] *Id.*

[14] *See* The DMA Safe Harbor Program: A Guide for Businesses, *available at* http://www.dmaresponsibility.org/SafeHarbor/.

A. Continued Viability of the Notice and Choice Model

The existing combination of sectoral laws designed to address specific, concrete harms complemented with enforceable self-regulatory codes of conduct has proven to be a successful means of advancing innovation while also providing consumers with transparency and control over their data choices. The RFC alludes to what the President's Council of Advisors on Science and Technology Big Data Report ("PCAST Report") describes as the "limitations of the notice and consent framework" in the big data environment.[15] This characterization appears to imply that notice procedures are somehow insufficient, outdated, or otherwise unavailable to consumers in the big data context.

DMA believes that the notice and choice model remains a successful and effective mechanism to provide consumer privacy in an age of big data. As big data has evolved, so too have notice and choice. Through industry efforts including both self-regulation and innovation by individual companies, consumers now are provided with an array of notice and choice mechanisms. For example, the DAA Program advanced the provision of transparency through the development of an actionable icon. This icon provides notice outside of the privacy policy where data is collected and used for advertising purposes. The DAA icon is served globally more than one trillion times each month on ads and websites. In addition, the DAA makes available a centralized choice mechanism—a single website that unites the opt-out mechanisms provided by the more than 100 third-party advertisers participating in the program. The choice mechanism website offers consumers a "one-click" option to request opt-outs from all participating third-parties or allows a user to make choices about opting-out of interest-based advertising from specific companies. Consumers are directed to AboutAds.info not only from DAA icon-based disclosures on or around ads, but from other forms of website disclosure. Industry continues to advance transparency tools through prominent in-ad notice on desktop and mobile devices, meaningful disclosures about the collection and use of data, app settings, and industry opt-outs available through self-regulatory program. The emergence of such new and robust vehicles for providing notice demonstrates that notice and choice remain a necessary – and sufficient – tool for empowering consumers in big data settings.

Contrary to assertions made in the PCAST Report, notice and choice has not devolved into a "fantasy world", but rather has transformed into just the opposite—a critical, real-world framework used by hundreds of millions of Americans to exercise choice about the use of their data across the marketplace.[16] The mechanisms in place to effectuate these choices have evolved from privacy policies to display ad icons and have now expanded to the mobile environment. In the marketing context, industry has led the evolution of notice and choice through self-regulation. For example, the *DMA Guidelines* require mobile marketers to provide notice and choice about mobile marketing practices.[17] Specifically, Article 56 states that "every mobile

---

[15] President's Council of Advisors on Science & Technology, *Big Data and Privacy: A Technological Perspective* (May 1, 2014) at 21, *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

[16] *Id*. at 38.

[17] Article 55 of the *DMA Guidelines* states:

marketing message sent must include a simple and easy-to-use mechanism through which the individual can opt out of receiving future mobile marketing messages" and that "where possible, the opt-out mechanism provided should allow the recipient to opt out via reply text message."[18] With respect to location-based information, such information "must not be shared with third-party marketers unless the individual has given prior express consent for the disclosure."[19]

This evolution of notice and choice has occurred alongside innovation in the DDME. The notice and choice model remains the best way to effectuate consumer preferences while safeguarding the societal and economic benefits of big data. Policymakers should continue to embrace a model that has helped unleash the power of data while giving consumers meaningful choice about the use of their personal data.

B. Limitations with Respect for Context

Question 4 also asks whether the notion of "respect for context"—articulated in the Consumer Privacy Bill of Rights—should be engrafted upon the existing privacy framework in light of big data developments. According to this principle, companies' collection, use, and disclosure of personal data should occur in a manner limited to the context in which the data was provided. This approach, however, presupposes that data used for purposes beyond the immediate transaction for which it was collected does not benefit consumers. The experience of data innovation proves just the opposite. For instance, a household-goods manufacturer may gather data about household use of an appliance for the purpose of maintaining and servicing the appliance. The same data, however, could be used by the manufacturer to develop new and improved appliances, make current product lines more energy efficient, or, for the eco-friendly consumer, provide information to them about the availability of other energy efficient appliance. Attempting to implement a narrowly drawn "respect for context" principle would cause severe disruption to the economy and to consumers. Instead, the concept of "respect for context" should be expanded to reflect the way that the DDME actually functions today.

The success of the DDME is dependent on responsible data flows through the data-driven marketing ecosystem. The natural consequence of a restrictive "respect for context" principle

---

> Marketers that send or intend to send mobile messages should publish an easily accessible notice of their information practices (which includes but is not limited to a notice in their respective privacy policies) with regards to mobile marketing. The notice must include sufficient information to allow individuals to make an informed choice about their interaction with the marketer. This should include, at minimum, any applicable terms and conditions, details of the marketer's information handling practices and clear directions about how to unsubscribe from future solicitations.
>
> The mobile marketing notice should be easy to find, read and understand on mobile screens, and should comply with existing *DMA Guidelines*.

See Direct Marketing Association, *Guidelines for Ethical Business Practice* (Jan. 2014), *available at* http://thedma.org/wp-content/uploads/DMA_Guidelines_January_2014.pdf. See also Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment*, available at http://www.aboutads.info/DAA_Mobile_Guidance.pdf.

[18] *Guidelines* at p. 46.

[19] *Id*.

would be the diminution or elimination of data exchange across the DDME. The *Value of Data* study found that stopping the exchange of data across the DDME would impact at least $110 billion in revenue to the U.S. economy and 478,000 American jobs. Even within a single entity that has collected data, a narrowly-drawn "respect for context" concept restricts that entity's use of its own data for research or other purposes, constituting a system where businesses must seek permission to innovate.

The narrow view of "respect for context" envisioned in the Consumer Privacy Bill of Rights would harm the economy, job creation, and consumers—and is unnecessary given the options already available to consumers. In the marketing context specifically, the DMA has long required companies to provide an opt-out choice for data transfers for marketing purposes. In addition, the *DMA Guidelines* impose requirements on companies making material change to their data practices. Moreover, advances in the provision of transparency mitigate significantly concerns about the movement of data across the DDME.

V. Data Retention Benefits Consumers and Businesses

Question 7 of the RFC calls for comments on data deletion practices. While individual companies often institute data deletion policies according to their specific business models, DMA has concerns with government-mandated data deletion requirements, and believes that such requirements would cause significant harm to consumers, including by undermining fraud prevention services and other consumer-friendly programs for which organizations retain data. Fraud prevention services rely on timely access to accurate data to prevent identity theft and other concrete consumer harms. Deletion mandates could also hamper statutory obligations and other compliance efforts, or create difficulties with companies involved in internal investigations. The impact of this provision on the common practice of creating backup tapes for servers is also unclear.

Requiring deletion of data also is not practicable. As the PCAST Report noted, it is "practically impossible" to assure that all data relating to an individual has been deleted from a particular data holder's databases.[20] Moreover, as a practical matter, requiring companies to purge all copies of data and to inform third parties to purge their copies of data, may not be technically feasible, especially in situations where information has gone "viral." Even in ordinary business situations, the ability for digital media to be reproduced instantly and at no cost to most individuals means that 100% deletion could potentially only be achieved at great expense.

In light of these significant problems with mandated deletion, and the fact that current sectoral laws combined with robust and enforceable self-regulation already address the potential for data misuse that risks consumer harm, DMA believes that it would be both unwise and unnecessary to impose data deletion requirements on the DDME.

Instead of giving credence to speculation about harms that could possibly arise from the collection and retention of data, the NTIA's focus should be on concrete harms that may result

[20] PCAST Report at 39.

from the misuse or unauthorized use of data. This approach has been the bedrock of U.S. privacy regulation, and it has served to create the dynamic DDME that is fueling the U.S. economy.

VI. Data Services Sector

Questions 8 and 10 of the RFC discuss the practices of the data services sector, which includes companies commonly referred to as "data brokers." DMA addresses these questions from the perspective of data services that facilitate the collection and use of marketing data.

The data services sector has been examined several times recently by the FTC, Congress, the Government Accountability Office, and other government entities, and in no case has any concrete harm or wrongdoing been identified.

The data services sector facilitates legitimate commercial data practices that are essential to America's job creation, economic growth, and global leadership. Marketing benefits consumers individually by informing their buying decisions and collectively by fueling competition. It is critical to understand that marketing databases are not individual "look up" services. Such databases are merely high-tech ways for companies to pursue the same goal that marketers have always had – namely, reaching a group of consumers likely to enjoy their products and services. No company wants to send a lawnmower discount to an apartment dweller, and no apartment dweller is interested in such a coupon. Moreover, no company wants to "look up" a single homeowner in order to send a lawnmower discount; rather, companies are seeking to communicate with a group of likely buyers.

The RFC also references the notions of access, correction, and deletion in relation to the data services sector. The FTC examined this issue in its report on *Protecting Consumer Privacy in an Era of Rapid Change*, and concluded that "companies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain."[21] DMA agrees with the FTC on this point. As the Commission notes, the only "harm" consumers might experience from inaccurate marketing data is an irrelevant advertisement, and heightened accuracy standards for marketing data would actually require the addition of more personally identifiable information to marketing databases in order to increase accuracy and permit authentication of individuals who request access or changes to records.[22]

Congress has repeatedly considered legislation that would regulate third-party providers of consumer marketing data. Following extensive deliberation, Congress has repeatedly decided not to enact such legislation. In fact, as discussed above, many commercial data practices, including marketing practices involving certain types of data, are already regulated in the U.S. under existing laws and self-regulatory regimes including FCRA, GLB, COPPA, HIPAA, and

[21] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at 30 (March 2012).
[22] *Id*. at 29.

implementing regulations. These legal regimes are policed through both government oversight and longstanding self-regulatory standard-setting bodies like DMA's Ethics Policy Committee.

Additionally, as noted above, the DAA principles restrict the use of Multi-Site Data, Cross-App Data, Precise Location Data, and Personal Directory Data for eligibility purposes such as employment; credit; healthcare treatment; and insurance underwriting and pricing.[23]

There are also practical considerations counseling against expanded consumer access to marketing databases. Individual companies that have direct relationships with consumers often provide review and correction mechanisms for their customers. This enhances the accuracy of any data that they provide to third parties. Database compilers, in turn, invest in significant efforts to ensure that their data is correct, and have strong market incentives to maintain the quality and accuracy of their data. With respect to marketing data such as "segments" assigned based on statistical algorithms that are predicted and may or may not reflect actual consumer characteristics, consumer access would not be meaningful even if it were provided.

Moreover, the cost of implementing access and correction for marketing databases is prohibitive for most companies and would outweigh any benefits.[24] Mandating additional or redundant access would add significant costs likely to be passed on to consumers. 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, expansion of access rights would require the implementation of appropriate authentication and verification systems. These types of controls are not only costly to implement, but in many cases would require the collection and maintenance of additional personal information in order to authenticate individuals. When viewed as a whole, the enormous expenditures and burdens are not warranted by data that does not cause any identifiable harm to consumers.

Policymakers should not disrupt the well-functioning self-regulatory programs that currently protect consumers. The existing regulatory framework, designed to address concrete harms associated with the misuse of data, complemented by self-regulatory codes of conduct backed by enforcement mechanisms, appropriately fosters market innovation while protecting consumers.

VII. Role of De-identification Practices

The RFC in Question 11 refers to the proposition advanced by some that de-identification of personal data has limited efficacy, or is inherently susceptible to "re-identification."

At the very least, the "re-identification" proposition has been seriously challenged. A 2011 study entitled *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy* noted that de-identification prevents third parties from

[23] Article 38, *Guidelines*, at p. 28-29; Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment*, available at http://www.aboutads.info/DAA_Mobile_Guidance.pdf.
[24] Protecting Consumer Privacy, FTC, supra note 21 at 65.

knowing information about identifiable individuals, and that regardless, the vast majority of third parties with access to de-identified information have "neither the motivation, nor the technical expertise, nor the resources necessary to re-identify individuals."[25] The report concluded that "the claim that the de-identification of personal data has no value and does not protect privacy due to the ease of re-identification is a myth."

De-identification procedures are common in the data-driven marketing industry, and the *DMA Guidelines* and DAA principles provide guidance to help ensure that data is not re-identified after any transfer of data. The DAA *Self-Regulatory Principles* define de-identification as taking reasonable steps to ensure that data cannot reasonably be re-associated to an individual or a particular computer or device. These methods assure that data is not connected to individuals after it has been de-identified. The *DMA Guidelines* require that members take steps to protect the de-identification process where necessary. Article 38 requires members to:

> Take reasonable steps to protect the non-identifiable nature of information if and when it is distributed to non-affiliates, including not disclosing the algorithm or other mechanism used for anonymizing or randomizing the information, and obtaining satisfactory written assurance that such non-affiliates will not attempt to re-construct the information and will use or disclose the anonymized information only for purposes of online behavioral advertising or other uses as specified to users. This assurance will be considered satisfied if a non-affiliate does not have any independent right to use the information for its own purposes under a written contract.

As a basic matter, there has been no identifiable harm rooted in the combination of multiple, anonymous, data sets. To the extent that data does become re-identified, the potential for concrete harms to consumers is addressed under the existing sectoral privacy laws.

VIII. Robust Laws to Protect Against Improper Uses of Data

Question 12 of the RFC speculates that big data could be used to harm consumers through discrimination against certain individuals or groups or predatory practices. The expanding scope of data and advancing technology have not made existing anti-discrimination and consumer protections less valuable or less effective, and the focus of policy frameworks should continue to be on uses of data shown to be harmful to consumers, rather than on restricting the responsible use of data for marketing purposes.

One such important marketing use of data is in predictive analytics, which is the process of applying statistical techniques, such as modeling, to current and historical data for the purpose of tailoring marketing materials to meet the preferences of consumers. The use of predictive analytics is the means by which retailers, non-profits, and other organizations can tailor their product or service offerings to consumers so that the interaction is more relevant and useful to

[25] Cavoukian and El Emam, *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy, Information*, Information and Privacy Commissioner, Ontario, Canada, at 5, *available at* http://www.ipc.on.ca/images/Resources/anonymization.pdf.

consumers. Predictive analytics can be used to boost engagement with existing customers. In this sense, predictive analytics can serve as a customer relationship management tool, allowing businesses to leverage internal customer data, data provided by a marketing information service provider, or both, to accomplish these goals. Even more, predictive analytics can react to the dynamic evolution of consumers' preferences, making the analysis more valuable over time than a static snapshot. These processes help businesses serve their customers better.

Predictive analytics are also used to protect the safety and security of consumers. Data can be modeled to detect patterns of fraud across a business or industry and solutions can be crafted to prevent future fraud. Technological platforms can analyze data in real time to detect irregularities or abnormalities in transactions, and other techniques can evaluate historical data to predict future fraud attempts, and to enhance authentication and verification measures. For example, the application of predictive modeling of fraudulent claims in the insurance industry—a significant and ever-present problem—has reduced overall claims costs by five percent.[26] The use of predictive analytics for fraud prevention has yielded tangible, positive results for business and consumers in all areas of the economy. Such success is due to advances in technology that permit the analysis of multiple sources of large and diverse data sets.

The RFC references the use of data to engage in discriminatory or predatory practices. As the White House Report recognized, such conduct is restricted under existing law. With respect to discrimination in lending in particular, existing law addresses "scores" that may be used to establish an individual's eligibility to receive a product or benefit. The FCRA regulates the use of scores to make eligibility decisions for credit, employment, housing, and other areas in which a consumer faces material consequences based on a decision. In these contexts, the law imposes obligations on the user of the information, such as notifying the consumer of an adverse decision and providing other information relating to the use of a credit report in making the decision. In contrast, the use of predictive analytics in marketing has no such impact and accordingly Congress has chosen not to regulate such marketing uses.

IX. Privacy Enhancing Technologies

Questions 14, 15 and 17 of the RFC request comment on the availability of technology and other tools for promoting privacy. DMA appreciates efforts to improve competition around consumer privacy protections, such as "privacy preference profiles," but believes that such competition should come from within the private sector. Innovative privacy practices can best be developed by the private sector, as they are better able to respond to consumer preferences. As such, any guidance from the government regarding privacy practices should be technology neutral. This will allow data-driven marketers and other responsible users of data the flexibility to continue to innovate and create improved privacy methodologies.

DMA, however, would welcome government investment in and support of research regarding how data may continue to improve outcomes and productivity in the private sector,

[26] Steve Culp, *Insurers Help Themselves and Their Customers by Fighting Fraud More Effectively*, Forbes Feb. 3, 2014, *available at* http://www.forbes.com/sites/steveculp/2014/02/03/insurers-help-themselves-and-their-customers-by-fighting-fraud-more-effectively/.

while avoiding one-size-fits all rules in this developing area of the economy. Additionally, when appropriate, data maintained by the government should be made available to the private sector for use in creating technological advances, new products and services, and other as-yet-unknown benefits to society. The use of big data can measurably improve outcomes and productivity across the economy. DMA members constantly seek new ways to responsibly harness big data for the benefit of consumers and society, and we welcome the government's partnership in that effort.

* * *

DMA appreciates the opportunity to submit these comments, and we look forward to working with NTIA on these important matters. Please do not hesitate to contact me with any questions at (202) 861-2420.

Sincerely,

Peggy Hudson
Senior Vice President, Government Affairs
Direct Marketing Association

Cc: Stu Ingis, Venable LLP
Michael Signorelli, Venable LLP
Ariel Wolf, Venable LLP