Insights | Collaboration | Advocacy

Leading the Marketing Community

March 31, 2014

Big Data Study
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, DC 20502

SUBJECT: Request for Information on "Big Data"

Pursuant to the March 4, 2014 *Federal Register* Notice by the Science and Technology Policy Office, the Association of National Advertisers (ANA) appreciates the opportunity to provide these comments on the issue of "big data" involving consumers, businesses and our entire economy. These comments are addressed primarily to Question (1) in the Request for Information *"What are the public policy implications of the collection, storage, analysis, and use of big data? For example, do the current U.S. policy framework and privacy proposals for protecting consumer privacy and government use of data adequately address issues raised by big data analytics?"* We also include comments on other big data matters of interest and concern.

The ANA (Association of National Advertisers) provides leadership that advances marketing excellence and shapes the future of the industry. Founded in 1910, ANA's membership includes more than 575 companies with 10,000 brands that collectively spend over $250 billion annually in marketing and advertising. The ANA pursues "collaborative mastery" that advances the interests of marketers and promotes and protects the well-being of the marketing community. For more information, visit www.ana.net.

In General

ANA believes a number of points deserve emphasis at the outset:

- We agree with the *Federal Register's* Request for Comments definition of "big data:" "Big data' refers to datasets so large, diverse and/or complex, that conventional technologies cannot adequately capture, store or analyze them."

- This definition, however, focuses solely on the quantity and/or complexity of the data involved and the technological capacity to handle, store and analyze it. The definition, therefore, provides no guidance as to the policy implications of any dataset regardless of size.

- The amount of data in and of itself is not determinative of potential concern. Rather, the focus should be on the sensitivity and potential vulnerability to harm of any dataset.

- Various principles (e.g. transparency, accountability, consumer control) apply in both the big and smaller data contexts.

- While big and small data share these characteristics and concerns, they are not identical.

- All information is not created equal; some (health, financial) information is far more sensitive than other data and requires different treatment.

- Data security is, of course, a consistent fundamental interest that substantially impacts all data whether big or small.

- In the commercial arena, the use of data for advertising purposes is a driving force in the U.S. economy. It helps generate employment, sales and economic activity throughout various industrial and other sectors and in every geographical region in our nation.

- Increasingly, advertisers utilize data to provide greater and more relevant information to consumers. This information enables consumers to make informed choices in the marketplace, which helps to enhance economic efficiency, innovation and competition.

- For the purpose of effectively placing advertising, it is often not necessary to have or utilize personally identifiable data.

- Because of the critical role advertising plays in regard to our economy, it is essential that governmental decisions about commercial data collection and use be made carefully, correctly and judiciously.

- It is difficult to see how broad or comprehensive new privacy laws or regulations at the present time could keep pace with the revolutionary and extraordinarily rapid transformation of the Internet and other new media technologies.

- Advertisers have established various major self-regulatory mechanisms to address privacy and other issues related to data collection and use. Especially in a period of accelerating evolving technology, new data-related privacy laws and regulations should be initiated only where it is conclusively demonstrated that existing laws, regulations and industry efforts are clearly inadequate.

Data Provides Tremendous Value to the U.S. Economy

The appropriate collection and use of data provides increasing benefits for our nation's economy, the business sector and consumers. Every industry in America relies on data-driven marketing. One of our industry partners, the Direct Marketing Association (DMA), recently released a study that found that the data-driven marketing economy added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in 2012. The study also found that 70 percent of the value of the data-driven marketing economy depends on the ability of firms to exchange data across the marketplace. The DMA study is available at: http://www.the-dma.org

Advertising is a driving force in the U.S. economy, serving as a generator of job creation and sales. According to a 2013 landmark study conducted by IHS Global Insight, Inc., a highly regarded consulting firm, advertising is a remarkably powerful economic force. Nationally, it generated over $5.8 trillion in economic activity in 2012, or approximately 20 percent of total U.S. economic activity. Sales of products and services stimulated by advertising supported 19.8 million jobs, or 15 percent of the total jobs in the country. The study was based on an economic model developed by Dr. Lawrence R. Klein, recipient of the 1980 Nobel Prize in Economics. More information about the study is available at: www.ana.net/content/show/id/29212

Another Nobel Laureate in Economics, the late Dr. George Stigler, noted that advertising is a critical force in fostering economic efficiency and competition throughout the U.S. economy. In addition, the economic health of most of our country's media, including the online marketplace, rests primarily on the strong financial foundation provided by advertising.

As advertising fuels the Internet engine, advertisers have a great economic interest in the appropriate collection and use of data and are actively engaged in satisfying the privacy concerns of consumers in both the offline and online world. Advertising increasingly is a data-driven industry. It is extremely important, however, that marketers are able to obtain accurate anonymized consumer data, or Internet users will be besieged by unwanted and irrelevant advertisements, often labeled spam and in those circumstances, the Internet would be inundated with a profusion of unwanted and unnecessary traffic.

Not All Data is Created Equal

The United States has historically taken a sectoral approach to privacy regulation, adopting carefully defined rules to apply to specific categories of information. As a result, there are more than ten separate federal regulatory privacy regimes, including: the Children's Online Privacy Protection Act (COPPA), the Cable Communications Policy Act, the Telephone Consumer Protection Act, the Video Privacy Protection Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act.

This sectoral approach is based on the fact that not all information is created equal. For example:

- Personally identifiable information clearly raises potentially far more serious privacy implications for consumers than non-personally identifiable information.

- Greater sensitivity concerning certain kinds of information, such as medical or financial information, is required. Consumers rightfully expect that this type of information should be more protected because the potential harm from disclosure is greater than for other kinds of information, such as the color of a shirt ordered online by a consumer.

- Information from and about children must also be treated differently. Marketers agree that children deserve greater privacy protection. ANA and others in the business community worked closely with the Congress and the Federal Trade Commission (FTC) to develop COPPA, which provides parents substantial control over this type of data collection.

A majority of the data collected for marketing purposes is anonymous or anonymized and is not sensitive information. Any consideration of government restrictions on the collection and use of this data must include a serious analysis and delineation of any harm that might occur if this information were inappropriately released. Would there be real, rather than theoretical, harms, and what steps could be taken to address them?

We cannot assume that the mere collection and use of data is harmful or will encroach on individual privacy. Major steps have been taken by industry to address specific privacy concerns. The Digital Advertising Alliance (DAA), formed by ANA and four other industry groups, for example, has set forth seven guiding principles designed to address consumer concerns about the use of information, 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. These principles apply in both the big and small data contexts, and address the following:

- Education: educate individuals and businesses about the collection and use of data.

- Transparency: provide clear and easily accessible disclosures to consumers about data collection and use practices.

- Consumer control: ensure the ability for consumers to choose whether data is collected and used for specified purposes, including the obtaining of consumer consent in certain circumstances.

- Data security: provide appropriate security for, and limited retention of, data collected and used.

- Material changes: obtain consumer consent before a material change is made in certain collection and use policies, where such change would result in more collection or use of data.

- Sensitive data: recognize that data obtained from children merits heightened protection, and require parental consent for data collection under 13.

- Accountability: develop programs to advance these principles, including programs to monitor and report instances of non-compliance with these principles.

These principles are available at: http://www.aboutads.info

In addition, in the area of Web viewing data, the DAA has set forth a clear framework governing the collection of online Multi-Site Data that also provides consumer choice for the collection of such data. These Principles clearly and explicitly prohibit the collection or use of Multi-Site Data for the purpose of any adverse determination concerning employment, credit, health treatment or insurance eligibility. Additionally, the Multi-Site Data Principles provide specific protections for sensitive data concerning children, health and financial data. These and other industry efforts are directed to very specific potential harms. The principles are available at: http://www.aboutads.info/msdprinciples

The private sector has made substantial progress over the past several years to enhance the level of privacy protection for consumers. At the urging of ANA and other industry groups, almost every major commercial website has adopted and posted privacy policies to tell consumers how information is collected and used. Companies are innovating in the area of privacy and offering consumers new privacy features and tools such as sophisticated preference managers, persistent opt-outs, universal choice mechanisms and shortened data-retention policies. These developments demonstrate that companies are pro-active as well as responsive to consumers, and focusing on privacy as a way to distinguish themselves in the marketplace.

Even in the sensitive area of health information, there are examples of the effective and appropriate use of large scale databases to achieve very positive results while protecting the privacy of consumers. Dr. Michael Nguyen, the Acting Director of the Division of Epidemiology in the Food and Drug Administration's Center for Biologics Evaluation and Research, recently wrote a blog entry describing the use of extensive medical databases to evaluate the safety and effectiveness of prescription medications: "FDA scientists have partnered with the Harvard Pilgrim Healthcare Institute to create such a surveillance system, called Sentinel. Within Sentinel, FDA has supported the development of software that analyzes information from health insurance and health record databases to search for evidence that certain products are linked to specific adverse effects. Although these data are protected behind tight firewalls and remain under the control of the original health insurance plans that created them, the software makes it possible to analyze the information without disclosing identifying information in order to strictly maintain patient privacy." http://blogs.fda.gov/fdavoice/index.php/2014/03/sentinel-harnessing-the-power-of-databases-to-evaluate-medical-products/

ANA does not believe there is a present need for broad new federal privacy legislation. Government regulation does not have the flexibility to adapt effectively to the exceptionally rapid changing technologies and new privacy issues that the Internet and other new media have generated. Rather, we believe that consumers can be best protected through a

combination of existing privacy laws and regulations, privacy enhancing technology, effective and muscular self-regulation and the ultimate backstop of the powers of the FTC to stop false, deceptive or unfair acts or practices.

The Internet of Things

It is clear that the discussion of data collection and use has expanded with the growth in data. For example, the ability of everyday devices, from cars to smart home appliances, to communicate with each other and with people is becoming more prevalent and raises new privacy and security concerns. This development is often referred to as "The Internet of Things."

The FTC held a public workshop last November to explore the consumer privacy and security issues posed by the growing connectivity of devices. In opening remarks, FTC Chairwoman Edith Ramirez stated: "As I see it, the expansion of the Internet of Things presents three main challenges to consumer privacy: first, it facilitates the collection of vastly greater amounts of consumer data; second, it opens that data to uses that may be unexpected by consumers; and third, it puts the security of that data at greater risk."

Chairwoman Ramirez concluded: "With big data comes big responsibility." ANA agrees with this comment, and notes that the advertising community has been actively addressing various issues related to the collection of vast amounts of data.

We believe that in the context of advertising that the DAA model provides the right template for action that can be modified and expanded to meet the privacy concerns of new media and new technologies.

Data Security is Essential

Big or small, data must be secure. Entities that collect and use data must make every effort to ensure that mechanisms are in place to guarantee the integrity of the data.

Larger amounts of data may make the challenge of securing such data more difficult. Larger data fields are available for trolling by unscrupulous entities, and those collecting and storing data will likely face greater challenges with large volumes of data than in the small data context.

The public and government have legitimate privacy concerns related to database hacking that could result in health, financial or other sensitive information ending up in the wrong hands. These are serious issues and there are several bills pending in the Congress and other Congressional activities related to data security issues. For example, on March 26th, the Senate Commerce Committee held the latest of numerous hearings on recent data breaches.

We believe Congress should pass data security legislation which establishes one uniform standard and preempts the 47 different state laws on data security and breach notification.

The Need for Accurate Data

Business in general and advertisers in particular are faced with a new and very dangerous challenge -- web traffic fraud – which does not discriminate based on the amount of data involved. The Internet Advertising Bureau (IAB) recently estimated that approximately 36% of all Internet activity is fraudulent, resulting from viruses and mechanisms that direct computers to particular sites. This "bot traffic" costs advertisers significant amounts, since advertisers pay for the placement of ads that are loaded in response to users visiting Web pages. Forty-six percent of online ads are served to websites and charged to marketers even though consumers never saw the ads. Additionally, advertising inadvertently supports rogue websites that deliberately pirate movies, music and other intellectual property.

The advertising community is responding to these and other measurement challenges through an initiative known as Making Measurement Make Sense (3MS). This initiative, launched in 2011 by the ANA, the IAB and the 4A's, is an industrywide effort to develop effective and accurate advertising metrics that will enhance evaluation of digital media and facilitate cross-platform measurement. More information about 3MS is available at: www.ana.net/content/show/id/d3ms

Data, whether it is "big" or "small," if it is inaccurate or corrupted, is of substantially diminished value both for industry and consumers. This is a growing challenge for the advertising community and for the Internet-based economy as a whole.

Commercial Privacy Issues Must Not be Conflated With Government Privacy Issues

Recent disclosures about surveillance of citizens by the National Security Agency (NSA) as well as several high-profile data breaches from major retailers and other companies have combined to substantially increase the focus of policymakers, the business community and consumers on data security and privacy issues.

In his January 17th speech on NSA reforms, President Obama stated: "The challenges to our privacy do not come from the government alone. Corporations of all shapes and sizes track what you buy, store and analyze our data and use it for commercial purposes. That's how those targeted ads pop up on your computer and your smart phone periodically."

Commercial privacy issues must not be allowed to be conflated with government surveillance and potential reforms at the NSA. These issues must not be confused with interest-based advertising or online behavioral advertising (OBA). The privacy issues in these two areas are very distinct and deserve careful separate consideration. In addition, government access to private sources of data must be considered carefully. Whoever holds collected data must have in place security mechanisms to ensure the safeguarding of data, and methods for

government obtaining such data must be clearly enumerated and subject to close supervision.

Interest-based advertising, which under the auspices of the DAA self-regulatory program primarily utilizes anonymous or anonymized data, is a critical tool to reach the right consumer at the right time with the right message and often at the right price. It provides enormous economic efficiency to the Internet marketplace; provides tremendous competitive benefits; and provides consumers with relevant marketing information rather than spam. Data fuels the engine of this online marketplace.

To address the privacy concerns that some have about interest-based advertising, the marketing community has built one of the most rapidly-growing and successful self-regulatory programs in history – the DAA. The DAA features an icon alerting consumers to the fact that they have been served an ad based on OBA. From this icon, consumers can access information about interest-based ads and learn how to exercise choice about how to opt-out of those interest-based targeted ads if they choose to do so.

Since its launch in 2010, the DAA has rapidly brought enhanced notice and choice to consumers:

- The AdChoices Icon is now served globally trillions of times each month
- 30 million unique visitors have visited our two program sites, www.aboutads.info and www.youradchoices.com
- 3 million unique users have exercised an opt-out choice on our Consumer Choice Page

These are compelling numbers which show that consumers are coming to rely on the DAA program for meaningful choice.

On February 23, 2012, at a White House event announcing President Obama's framework for privacy in the 21st century, the Chairman of the FTC, the Secretary of Commerce and White House officials publicly praised and endorsed the DAA's initiative.

Enforcement of the program is administered by the Council of Better Business Bureaus (CBBB) and the Direct Marketing Association. We believe that strong industry self-regulation is a superior alternative to restrictive new laws and regulations. One of the most important benefits of self-regulation is the flexibility to adapt to changing technologies, consumer behaviors and attitudes. In mid-2013, the DAA principles were extended to cover interest-based ads delivered across mobile applications and the mobile Web. The DAA guidance also addresses location-based data and personal directory data use.

The DAA's self-regulatory principles of choice and transparency for the collection and use of web-viewing data have been adopted by 31other countries, through the Digital Advertising Alliance of Canada and the European Interactive Digital Advertising Alliance.

Two public opinion surveys have found that Internet users recognize the value of online advertising and our industry's self-regulatory program. The first survey, commissioned by DAA and conducted by Zogby Analytics in early 2013, measured attitudes regarding online advertising with a specific focus on interest-based ads. Nearly 70 percent of respondents said they would like at least some ads tailored directly to their interests, compared to only 16 percent who preferred to see only generic ads. More than 90 percent of those surveyed said that free content was important to the overall value of the Internet. More than 75 percent said they prefer content like news, blogs and entertainment sites to remain free and supported by advertising, compared to fewer than 10 percent who said they would rather pay for ad-free content. The full results of the survey are available at: www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf

In the second poll, also conducted by Zogby Analytics last November, more than half of those surveyed (51.3 percent) said they would be more likely to click on an online ad that included an icon – like the AdChoices icon – that allowed them to opt out of ad-related information collection. Additionally, more than 73 percent of users polled said they would feel more comfortable with interest-based ads if they knew they had access to the protections that the DAA currently provides, such as the ability to opt out, limitations on data collection and third-party enforcement. The full results of the survey are available at: www.aboutads.info/ZogbyDAAOct13PollResults.pdf

It is clear, then, that consumers desire and benefit from interest-based advertising. It is also apparent that there are significant concerns and very serious issues related to governmental surveillance and potential NSA reforms. Any policies developed to respond to these issues should be tailored to address vulnerabilities and potential harms in the governmental sphere and avoid jeopardizing the many commercial benefits of interest-based advertising.

Conclusion

Ultimately, we believe that consumer privacy concerns must be balanced with consumers' desire for more innovative products and services. Because advertising is a major economic engine in the United States and throughout the global economy, great care must be taken not to stifle the many benefits provided by effective advertising. Industry self-regulation, coupled with consumer education, is the best way to strike this balance and to enable innovative technologies to continue to bring new and exciting opportunities to consumers. These objectives apply in both the big and small data environments.

All those who collect and use data must continue to work to ensure the security and proper use of that information. Advertisers will continue to focus on issues of harm that can flow from big data by working cooperatively with other industry participants, governmental policymakers and consumer-related organizations on greater data security, encryption and anonymization. Where relevant, lessons learned in the small data context can be applied to big data. Where necessary, for example, related to enhanced data collection involved with the Internet of Things, protocols may need to be developed to ensure that data remains reliable and secure.

Data and interest-based advertising are fundamental to the efficient use of the Internet, mobile and other emerging technologies. The DAA's self-regulatory program is the best end-to-end program to maximize consumer choice and provide consumer benefits in regard to online behavioral advertising served through any technology.

Any new laws or regulations should only be adopted to fill in where it has been shown clearly that existing requirements or mechanisms are not adequate to protect consumers from harm and that the new law or regulation will ameliorate that harm. Policies should not assume that data, big and small, is the same, but policymakers also should not ignore similarities between big and small data collection and use. Further, policymakers must recognize the rapidly evolving nature of technology and innovation and refrain from constraints that will impede additional benefits and opportunities for users and commercial entities alike.

Thank you for your consideration of our views.

Sincerely,

Daniel L. Jaffe
Group Executive Vice President, Government Relations