August 5, 2014

Angela M. Simpson
Deputy Asst. Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington DC 20230

Sent via email to privacyrfc2014@ntia.doc.gov

Re: Request for Public Comment, "Big Data and Consumer Privacy in the Internet Economy," Docket No. 140514424-4424-01

Dear Deputy Assistant Secretary Simpson:

The Interactive Advertising Bureau ("IAB") provides these comments in response to the Request for Public Comment on "Big Data and Consumer Privacy in the Internet Economy," issued by the National Telecommunications and Information Administration ("NTIA").[1] The IAB previously responded to the White House Office of Science and Technology request for information regarding big data, and incorporates those prior comments by reference in this submission. The IAB is pleased to have this additional opportunity to provide information to the Administration on big data and consumer privacy.

Founded in 1996 and headquartered in New York City, the IAB (www.iab.net) represents over 600 leading companies that actively engage in and support the sale of interactive advertising, including leading search engines and online publishers. Collectively, our members are responsible for selling over 86% of online advertising in the United States. The IAB educates policymakers, consumers, marketers, agencies, media companies and the wider business community about the value of interactive advertising. Working with its member companies, the IAB evaluates and recommends standards and practices and fields critical research on interactive advertising.

The IAB is committed to the continued growth of the interactive advertising ecosystem in tandem with ethical and consumer-friendly advertising practices. To that end, the IAB is one of the leading trade associations that released cross-industry self-regulatory privacy principles for the collection of web viewing data.[2] Launched in 2009, these Self-Regulatory Principles are administered by the Digital Advertising Alliance ("DAA"), have been widely implemented across the online advertising industry, and are vigorously enforced through longstanding and effective industry self-regulatory accountability programs. The Self-Regulatory Principles are reflected in IAB's Code of Conduct for its members.

[1] 79 Fed. Reg. 32714 (June 6, 2014).
[2] Press Release: *Key Trade Groups Release Comprehensive Privacy Principles for Use and Collection of Behavioral Data in Online Advertising*, July 2, 2009, *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209.

SUMMARY

NTIA's Request for Public Comment seeks views on numerous questions related to how the "Consumer Privacy Bill of Rights," as set forth in the 2012 White House Report on "Consumer Data Privacy in a Networked World" (the "Framework Report"),[3] should address "big data." The IAB's comments below focus on several themes responsive to the Commerce Department's Request for Public Comment, namely:

- The IAB supports collection and sharing of data, because such practices fuel innovation, provide tremendous benefits to consumers and our economy, and help to secure our nation's current competitive position globally.
- To that end, the IAB believes the current U.S. regulatory approach strikes the right balance by addressing the potential for concrete harms in specific areas, while otherwise enabling the free flow of data and fostering innovation in customer-friendly advertising. This sector-specific approach is complemented by robust self-regulatory enforcement efforts by industry. The Administration has not identified any new privacy issues presented by big data that cannot successfully be addressed under this existing approach.
- Accordingly, there is no need for new "one size fits all" consumer privacy legislation.
- In particular, there is no evidence of consumer harm that would justify new legal requirements related to data use, de-identification, or deletion.
- The IAB encourages the Administration to promote the success of the U.S. model in discussions with international partners to avoid the creation of unnecessary barriers to the free flow of data that would harm U.S. competitiveness.

Each of these themes is discussed below in more detail, with references to the relevant questions from the Request for Comment.

COMMENTS

- **The collection, use, and sharing of big data create many benefits. (Question 1)**

As the President's working group on big data recognized in its May 2014 report on "Big Data: Seizing Opportunities, Preserving Values" ("the White House Big Data Report"), the collection, use, and sharing of data have fueled economic growth and provided tremendous benefits for consumers and businesses alike. Big data, in particular, has unleashed exciting new innovations that increase consumer welfare in a myriad of ways. Consumers have only begun to benefit from big data's contributions to the development of new products and services and to job creation in a wide range of industry sectors.

Advertising and marketing uses of data, in particular, are hugely beneficial to consumers individually and to the economy as a whole. In the online advertising context, companies collect data for numerous operational purposes including ad delivery, ad reporting, site rendering, accounting, and network efficiencies and optimization, and site or application customization.

[3] White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (Feb. 2012).

These operations are necessary for a seamless cross-channel experience and a functioning digital economy.

In addition to these operational activities, companies in the online ad ecosystem use both small and big data to help them deliver more relevant and timely advertising messages. This data typically consists of Web viewing behaviors, which may be combined with offline data insights and used to predict the likely interests and needs of consumers. While this data may be "big" in the sense of including many different data types and data points, generally it is not sensitive. Interest-based advertising benefits consumers by providing them with more information to "comparison shop" and otherwise navigate the marketplace, and by providing access to products and special offers that are more likely to be desirable to consumers. While other business models exist, such as "pay walls," advertising has become the prevailing model for bringing online resources to the market across both Web and mobile applications. Because of advertising support, consumers can access a wealth of online resources at low or no cost. The decrease in the cost of online content and services made possible by advertising can have a particularly important effect on underprivileged individuals who might not be able to afford such resources otherwise. These ad-supported services for everything from business to entertainment have transformed our daily lives, and new innovation is continuing at a rapid pace.

Moreover, the data revolution has profoundly impacted citizen awareness by enabling the public release of information previously held by the government or otherwise made inaccessible to the public. Data also helps political and public interest information to reach interested consumers, which has transformed political advertising and public affairs reporting, as well as supporting a vibrant ecosystem of online information sources. These developments contribute to a more informed, active, and engaged citizenry.

From an economic standpoint, big data is central to the success of America's thriving technology industry, and is a growing feature of other industries as well. As discussed in greater detail in the IAB's previous comments submitted to the White House, a September 2012 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for IAB by Harvard Business School Professor John Deighton, found that the ad-supported digital industry directly employs 2 million Americans, and indirectly employs a further 3.1 million in other sectors. These figures resulted from strong job growth during a period when U.S. civilian employment had remained flat overall.

Data, and particularly responsible data sharing, is a boon to small companies. The Internet has allowed small publishers and businesses – the "long tail" of the online ecosystem – to thrive by lowering barriers to market entry and enabling them to reach niche audiences. This has supported the explosion of diverse online resources that consumers embrace.

- **The IAB believes the current U.S. regulatory approach strikes the right balance, and that big data issues can be successfully addressed under current privacy frameworks. (Questions 1, 2, 5)**

Because of the importance of big data for consumers and the economy, as well as the rapid pace of big data innovation, it is essential for the government to exercise caution when considering regulation of data practices. The first question in the Request for Comment asks

how the Consumer Privacy Bill of Rights can support the innovations of big data while also responding to its risks. The IAB believes that the current U.S. regulatory approach strikes the right balance in this regard.

The U.S. approach to regulating data practices is primarily "sector-specific." Targeted laws have been enacted (and continue to be considered by Congress) in areas where unauthorized or inappropriate use of data could cause concrete harms to consumers. These laws include the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act. These laws are rooted in the longstanding Fair Information Practice Principles, and focus on preventing identifiable harms to consumers that could occur through misuse of certain types of information. The Federal Trade Commission (FTC) also exercises its authority under the federal prohibition against unfair or deceptive acts or practices to address privacy and data security issues that it perceives as harmful to consumers. Additionally, there are state laws that prohibit unfair or deceptive practices against consumers, and authorize state attorneys general to enforce them. The FTC and other federal and state agencies vigorously enforce these important consumer protection laws.

Existing consumer protection laws are complemented by robust, enforceable industry self-regulatory programs. As one example of this type of program, the IAB, with other prominent trade associations, has led a successful effort to develop and implement the DAA Self-Regulatory Program governing the collection, use, and sharing of online data. The DAA Self-Regulatory Program applies to certain data collected online, and would include data that rises to the level of "big data." This program is enforced through accountability mechanisms run by the Direct Marketing Association and the Council of Better Business Bureaus. Industry stakeholders continue to adapt this self-regulatory program to respond to evolving technologies. Most recently, in 2013, the DAA issued guidance to inform companies about how the Self-Regulatory Principles apply to certain data practices in the mobile and other environments. For additional detail on how the DAA's groundbreaking program works, please see the IAB's comments submitted to the White House. There are numerous other self-regulatory programs that exist to guide privacy practices in relevant industries.

Both sector-specific laws and industry self-regulation in the United States generally follow the framework of the Fair Information Practice Principles (FIPPs). The Administration's Consumer Privacy Bill of Rights likewise is based on the FIPPs. The IAB believes that the FIPPs framework, in particular the notice and consumer control elements, has proven both flexible and enduring as implemented in the United States through law and self-regulation. The existing framework has provided meaningful protections for consumers while also allowing innovation to flourish.

In the IAB's view, it has not been demonstrated that big data presents new concerns that cannot be addressed through the existing framework and regulatory approach. With respect to advertising specifically, the practice of obtaining (or predicting) information about consumers' interests and providing tailored offers is longstanding. While this business model has now migrated online and draws on increasingly powerful technological resources, the data practices involved have not fundamentally changed and there is no new risk of harm to consumers. Furthermore, big data is playing in important role in helping security and privacy experts develop new tools to protect consumers' privacy and increase security. By analyzing large sets of

data, security experts are finding new ways to detect anomalies in their networks and prevent data theft.

- **There is no need for new "one size fits all" consumer privacy legislation. (Questions 1, 4, 6, 12-17)**

The White House Big Data Report asks the Commerce Department to draft legislation on a Consumer Privacy Bill of Rights. The IAB, as discussed above, believes that existing privacy frameworks, as implemented through the current combination of sector-specific laws and robust self-regulation, are sufficient to address privacy issues raised by big data. Accordingly, there is no need for new consumer privacy legislation that would apply "one size fits all" restrictions across industries and data practices. Legislation is, by its nature, inflexible and prescriptive. Imposing new legislative mandates that apply across industries would strike a severe blow to U.S. innovation and competitiveness. The adoption of monolithic restrictions would threaten both the economic benefits and consumer satisfaction that come from beneficial data uses.

In particular, the IAB is concerned that legislation should not establish prescriptive requirements for when or how consumer notice and control should be provided. While the IAB is committed to promoting consumer transparency and control related to data practices, specific legislative mandates in this area would thwart innovation and ultimately disadvantage consumers by reducing companies' ability to communicate effectively with their customers. For example, the explosive growth of the "Internet of Things" sector illustrates how quickly prescriptive notice and control requirements can become obsolete and meaningless as technology evolves at a rapid pace. Notice and control issues can be most effectively addressed through industry self-regulation, which can more easily adapt and respond to changes in technology and consumer expectations.

The DAA's Self-Regulatory Program provides an example of how industry self-regulation can drive the adoption of groundbreaking new mechanisms for consumer notice and control, while maintaining sufficient flexibility for businesses to communicate with their customers. As discussed at length in the IAB's previous comments, the DAA's Self-Regulatory Principles are implemented through an icon that is delivered as a part of relevant online advertising and provides easy access to an online consumer control mechanism. This approach has been praised by officials at the White House and FTC.[4][5] A new DAA solution for mobile notice and control, expected to launch later this year, demonstrates how industry solutions can adapt nimbly over time as technology evolves. The IAB supports efforts to improve transparency and consumer control through self-regulation.

The IAB further believes that additional broad restrictions on data collection, storage or sharing would be harmful to consumers and the economy. To date, privacy statutes have focused on regulating areas where data misuse presents a significant risk of concrete, identifiable harms to consumers. The DAA Self-Regulatory Principles similarly prohibit the use of "Multi-Site Data" for employment eligibility, credit eligibility, health care treatment eligibility, or insurance

[4] Kaye, K. (Feb. 2012). Ad Industry Joins FTC, White House in Do Not Track for Browsers. ClickZ. Retrieved from http://www.clickz.com/clickz/news/2154461/industry-joins-ftc-white-house-track-browsers

[5] Digital Advertising Alliance, FTC's Jessica Rich Applauds DAA's Newly Previewed Mobile Choice Tools (July 2014), Retrieved from http://www.digitaladvertisingalliance.org/blog.aspx?id=07-04-2014

eligibility or underwriting.[6] Although such practices were not occurring in the marketplace, the DAA issued these prohibitions out of an abundance of caution to ensure that such practices would not occur.

Aside from areas where a risk of concrete harm was identified, the government generally has refrained from regulating data for advertising and marketing purposes, because the only risk that consumers face from inaccurate advertising data is irrelevant marketing offers. Where concerns have been raised about misuse of marketing data, industry has responded through self-regulation. As a result of this harm-based approach, the free flow of data, including flows across industry sectors, has fueled tremendous consumer benefits such as more relevant and affordable content on the Internet, and promises to drive additional rapid innovation beneficial to consumers in the future. Consumers will not benefit from restrictions that cut off the flow of advertising and marketing data in response to vague or theoretical privacy concerns.

Regarding Question 4, IAB believes that the concept of "respect for context," where "context" is understood to include consumers' reasonable expectations, commonly accepted practices, and a balancing of the benefits and harms that may result from any expansion of the definition of "context," can be a useful principal to apply to the use of big data. According to this principal, data collected for one purpose should be considered as "respecting context" if it's used for another purpose that will optimize products and services for consumers. Such use would be consistent with consumers' expectations and would permit industry to continue to provide innovative services, creating net gains for consumers, industry and the economy.

The Request for Comment also includes questions related to sections of the White House Big Data Report on potential discrimination (Question 12). As discussed in the White House Big Data Report, existing laws address the possibility of discrimination against certain individuals or groups and can be vigorously enforced by the government. While the IAB condemns unlawful discrimination, the IAB believes that the existing legal and self-regulatory frameworks are sufficient to address discrimination that might be linked to data use, as well as other forms of discrimination. Notably, there is no evidence of a pervasive problem with discriminatory practices among companies that adhere to these self-regulatory frameworks. The IAB does not perceive a need for additional legislation or mandates to address discrimination concerns related specifically to big data. In particular, it would not be helpful to adopt new restrictions on automated decisionmaking or to require impact assessments for big data analytics. It is also important to note that market segmentation for advertising and marketing purposes does not equate to discrimination and that, to the extent that marketing data could be misused for discriminatory activities, this would be addressed by existing law. Market segmentation is a fundamental concept in public and private sector strategy that is employed to help increase marketing efficiency. It would be a mistake to restrain beneficial data practices, such as advertising practices, based on largely theoretical concerns about discrimination.

Finally, with respect to Questions 14-17 of the Request for Comment, the IAB submits that the government should remain technology-neutral in its efforts to advance consumer privacy. It is important that the government should not "pick winners and losers" among the

[6] Digital Advertising Alliance, "Self-Regulatory Principles for Multi-Site Data" 4-5 (Nov. 2011), available at http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

various technologies that may, depending on circumstances, enhance consumer privacy protections. The advancement of such technologies should be determined by the market. In particular, the promotion of specific technologies through legislation would not be appropriate and could actually stymie future innovation.

As policymakers confront the technological breakthroughs that are driving the collection, storage, analysis, and use of large data sets, the IAB believes the appropriate path forward is clear: industry self-regulation should remain harm-based and is generally the preferred approach to addressing privacy concerns associated with data collection and use. The Administration's Framework Report recognized the important role that industry codes of conduct can play in applying the FIPPs. Industry's successful DAA Self-Regulatory Program for the collection and use of Web viewing and mobile data demonstrates how self-regulation can effectively tackle new data practices as they arise, by applying the FIPPs framework in creative ways to new situations. Relevant to Question 13 in the Request for Comment, the IAB private accountability mechanisms can play a useful and important role in effectuating self-regulation. However, their role should focus on enforcing standards that have been established through cooperative processes that include industry stakeholders.

- **In particular, there is no evidence of consumer harm that would justify new legal requirements related to data use, de-identification, or deletion. (Questions 3, 7-10, and 11)**

Sections of the Request for Comment ask specifically about data usage, de-identification, and deletion. The IAB provides its views on these important questions below.

First, the Request for Comment asks about applying a responsible use framework to the regulation of big data (Question 3) and about the merits of regulating certain uses of data by information services companies (Question 8). IAB agrees with the President's Council of Advisors on Science and Technology report entitled "Big Data and Privacy," which recommends that policy attention be driven by a harm-based model that seeks to address actual use, rather than the collection and analysis of data. However, existing laws already address targeted areas where misuse of data could cause identifiable harms to consumers. The IAB is concerned that legislating new use limitations based on vague concepts or theoretical potential harms would create uncertainty and compliance costs for businesses and would unnecessarily restrict the free flow of data. In particular, the use and sharing of data for advertising purposes is beneficial for consumers and the economy, and is consistent with consumers' reasonable expectations regarding the use of their data. As discussed above, there is no evidence supporting a need for additional government restrictions on data use and sharing for such purposes.

The Request for Comments also includes questions related to de-identification of data (see Question 11). De-identified and other non-personal data is widely used in the online advertising industry in order to enable interest-based advertising, whether because personally identifiable information is not available or because companies choose to avoid using personal identifiers. The use of de-identified data is an essential part of industry's privacy "toolkit" today, especially for product development and market research purposes. De-identification enables companies to realize many of the benefits of big data while also limiting unnecessary use or sharing of personal identifiers. The DAA Self-Regulatory Principles accordingly recognize that

data that has undergone a reasonable de-identification process does not require the same notice or consumer control.[7] In the DAA framework, de-identification includes technical steps coupled with additional safeguards – namely, satisfactory written assurance from downstream data recipients that they will not attempt to re-identify the data.[8]

The IAB recognizes that some concerns have been raised about whether de-identification is effective. The relevant question, when assessing these concerns for regulatory purposes, is whether data is actually likely to be used to identify and cause harm to specific persons. Contrary to what critics suggest, de-identified data – even big data – simply is not equivalent to personally identifiable information. Effective de-identification techniques exist and can be applied even to large datasets. Re-identification of de-identified data, while theoretically possible according to critics, does not pose a meaningful risk of harm to consumers where the data involved is non-sensitive. Moreover, as noted, data for advertising purposes is frequently based on predictions rather than individual information, making re-identification even more difficult.

Other questions in the Request for Comment address data deletion or other methods of rendering data irretrievable (see Questions 7, 9, and 10). Simply put, data that cannot be easily retrieved does not pose meaningful or significant privacy risks to individuals. As discussed elsewhere in these comments, the IAB cautions against adopting new restrictions on the free flow of data based on theoretical or vague concerns. As suggested in Question 7 of the Request for Comment, the IAB therefore believes that a "reasonableness" standard for data deletion or for obfuscating data is the appropriate approach for companies to apply. This type of standard is consistent with the prevailing approach to data security concerns and can be advanced through industry self-regulation as appropriate.

- **The IAB encourages the Administration to promote the U.S. model in discussions with international partners.**

The IAB recognizes that some critics have unfavorably compared the U.S. approach to privacy regulation against jurisdictions that have taken a more prescriptive approach to consumer privacy. Rather than responding to such critiques by adopting similarly prescriptive legislation, the IAB encourages NTIA and the Commerce Department to champion the U.S. approach in international forums. Wider recognition of the merits – and effectiveness – of the U.S. approach would greatly benefit U.S. companies by reducing barriers to cross-border data flows and lowering compliance costs. It would also help to make the consumer experience consistent across borders.

The benefits of the U.S. approach are many. The U.S. approach to privacy regulation has fostered the development of a dynamic technology industry that is highly successful in international markets. It has also benefited consumers worldwide through the development of exciting new products and services for consumers, and the creation of a vibrant information economy. Finally, the U.S. approach effectively safeguards consumer privacy through the combination of targeted legislation, robust self-regulation, and meaningful enforcement

[7] *Id.* at 8.
[8] *Id.*

described above. No other country has balanced the goals of innovation and privacy as effectively.

The IAB, along with other trade associations, is accordingly investing significant resources in promoting adoption of the DAA Self-Regulatory Principles in over 30 countries. Consistent programs are already underway in Canada and Europe, and the IAB is engaging in discussions with Chinese stakeholders toward adoption in China. Further support from the Administration and recognition of the merits of self-regulation would provide valuable momentum for these efforts.

Inconsistent privacy regimes create barriers to free trade and competition. By promoting the U.S. approach abroad, the Administration would contribute to the success of American businesses. In contrast, critiques of the current privacy approach provide ammunition to critics overseas who seek to limit data flows across borders. While frank discussion of policy concerns is a hallmark of our democracy, the IAB encourages the Administration to avoid positions or statements that could undermine the ability of U.S. companies to compete globally.

CONCLUSION

The IAB appreciates the opportunity to provide these comments to NTIA as it continues its consideration of the Consumer Privacy Bill of Rights concepts laid out in the Framework Report. The IAB urges the Administration to maintain the current and successful approach of addressing privacy questions through targeted legislation coupled with industry self-regulation, avoiding new restrictions on the free flow of data. Enacting new legislative mandates related to complex issues such as notice and consumer control, data use limits, de-identification, deletion, or privacy-enhancing technologies would be going in the wrong direction. Rather than moving toward a prescriptive model of privacy regulation, which has limited companies' ability to innovate in other countries, the United States should support American businesses and lower trade barriers by promoting the U.S. model of privacy regulation in international forums.

* * *