April 4, 2014

Nicole Wong, Esq.
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue NW
Washington, DC 20502

RE: Big Data Study - Notice of Request for Information 79 FR 12251

Dear Ms. Wong:

Thank you for providing the Online Trust Alliance (OTA) the opportunity to submit comments in response to the White House Office of Science and Technology Policy (OSTP)’s Request for Information. As a 501c3 non-profit organization, OTA’s mission is to enhance online trust and empower users while promoting innovation and the vitality of the Internet. OTA works to educate businesses, policy makers and stakeholders about best practices and tools that enhance the protection of users’ security, privacy and identity. OTA supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.

OTA applauds the Administration’s leadership and commitment in facilitating this multi-stakeholder discussion. We share the mutual goal of maximizing big data’s benefits and the free flow of information while minimizing the privacy and related data security risks. This goal requires government and business entities to become stewards of data, moving from a minimal compliance perspective to one that takes full account of consumer context and societal expectations.

With big data, we have witnessed an unparalleled transformation of how information is collected, analyzed and used. We have also seen the impact of U.S. policy and businesses practices reaching far beyond our physical boarders. Big data brings many benefits and implications to the global economy. There is significant economic potential in fraud detection, security and threat modeling technologies. However, we are simultaneously grappling with the balkanization of the Internet, proposed trade barriers and challenges to the existing US-EU Safe Harbor. Therefore we must establish policies facilitating collection and sharing that have controls and processes preventing abuse.

Big data involves the collection of vast amounts of information from a growing number and variety of sources. These powerful analytic tools include both on and off-line data collection. These tools foster useful insights applicable to a range of business, medical and social issues. In the right context, consumers can realize significant benefits in services and offers tailored for their needs and lifestyles. In
the wrong context real harm can occur, ranging from public embarrassment to denial of benefits, manipulated costs of products and lost employment opportunities.\(^1\)

Today’s digital reality goes beyond the “reasonable expectation of privacy,” compromising the very foundation we have built the Internet upon. If left unchecked, consumer trust will continue to decline, the adoption of anti-tracking technologies will continue to increase and the long-term health of the internet will be undermined.

OTA looks forward to continued dialog on these issues and provides the following responses:

\((1)\) **What are the public policy implications of the collection, storage, analysis, and use of big data?**

Data collected about individuals and businesses is growing through new and innovative means, spanning both the online and offline world. The “Internet of Things” has brought an era of dependence and connectivity to our mobile devices, homes, automobiles and applications. With the blurring of work and personal boundaries, there are significant policy implications. Controls must be established for both the public and privacy sector. Otherwise, we risk finding ourselves in the dystopian world such as “Minority Report”.\(^2\)

Big data collection is occurring in multiple dimensions. Analytic capabilities and data mining tools are transforming what appears to be benign and individual data elements into a comprehensive picture of one’s life and lifestyle. For example, medical data, financial information and social relationships are often collected and analyzed to better understand a consumer’s personal interests. Yet in the wrong hands and wrong context, this usage could violate an individual’s basic right of privacy.\(^3\)

Unintended consequences such as accidental exposure, internal misuse or data loss incidents are real and present dangers and can cause disastrous effects. Unencumbered access to sensitive information could further drive fraud and identity theft. When a determined criminal tries to compromise a company, no matter what level of security protection is in place, both the company and their customers become victims. Recent data loss incidents and rouge employee access demonstrates how sensitive information can become accessible to third parties and result in harm to consumers, both U.S. Citizens and consumers abroad.

In order to demonstrate their commitment to proactive privacy ethics and practices, entities engaged in big data analytics should detail the purposes for which they collect and use information. From a policy perspective, user expectations are a good indication of whether purpose of collection relates to its intended use. Similar to credit reports, individuals should have the right to, access, examine and

---


challenge collected individualized data. Access by the consumer to data collected on that individual is essential to long term consumer trust in the data ecosystem.

Additionally to protect consumer privacy, governments and businesses alike must be transparent and inform individuals about the collection and use of their personal data. These entities must take steps to protect the data from abuse and their infrastructure from compromise. Just like first responders to a fire, entities should have data managers and cyber responders trained, equipped and empowered to deal with an incident. OTA recommends related entities adopt leading security practices, including comprehensive end-to-end encryption as well as developing a data breach readiness and incident response plan.

(2) What types of uses of big data could measurably improve outcomes or productivity with further government action, funding or research? What types of uses of big data raise the most public policy concerns? Are there specific sectors or types of uses that should receive more government and/or public attention?

Society has experienced tremendous benefits in predictive analysis for environmental and medical research. Individual health care professionals may see what may appear to be one or two unrelated patients. Aggregated data, however, can provide insights into potential epidemics and identify trends before they publicly spread. The pharmaceutical industry, aggregating years of research, has expedited the availability of new treatments and medicines and the Center for Disease Control (CDC) has used big data to create flu-tracking systems. The benefits will only increase as these tools and data collection practices become more sophisticated and dynamic. As our dependence on these systems and big data increase, OTA recommends that the government increase funding and research for cyber security measures that will protect these systems vitality and promote innovation.

Recognizing that these tools and specific technologies will evolve, OTA recommends the OSTP should focus the discussion on fundamental consumer concerns of data collection, usage/sharing and obligations. The OSTP should consider how to leverage its unique role as a convening authority for both private and public participants. Learning the lessons from past multistakeholder processes, a working group should be formed with equal numbers of representatives from each constituency in order to promote a collaborative and balanced view and meaningful self-regulatory best practices.

Balancing privacy with security is another fundamental concern when forming public policy. As new technologies such as location trackers and persistent identifiers are integrated into devices and applications, safeguards must be put in place to help prevent or detect fraud and abuse. However it is

4 One example is Acxiom’s "About the Data," a tool that gives individuals control over categories of information collected and allows consumers to correct this information, suppress any data they see, or opt-out of Acxiom’s system. https://www.aboutthedata.com/#education
important that these safeguards do not impede data collection and sharing. Such technologies may be used for marketing and other purposes that can provide enhanced online experience or other consumer benefits. When this data is being collected, the user should be provided a clear understanding of the use of data, including any third party sharing, with an ability to opt-out.

OTA believes anonymous web analytics for research or operational purposes should be exempt from proposed legislation. Web analytics is generally performed by third party service providers for the purpose of providing insight into industry trends. This research helps inform industry investments, website feature developments and facilitates efficient e-commerce and innovation. Such processed data is not used to target any individual or device via on or off line advertising or alter content viewed by the individual based on his/her individualized behavior and activities. Providers of such analytic services that aggregate, weigh, anonymize and otherwise process the collected data are in accordance with industry best practices.

(3) **How should the policy frameworks or regulations for handling big data differ between the government and the private sector?**

With the limited exception of national security, government entities should follow the same policies as the private sector. The government and private sector struggle to keep up with ever increasing sophisticated attack methods. This challenge is in part due to the lack of automated real-time information sharing. The sharing of threat intelligence information is a key arena for the government and private sector. Major players in both sectors must work diligently to usher in cooperation with the objective of improving protection against threats.

Threat intelligence sharing must move from individual silos of data to being shared cross sector to help identify trends. This shared data will help mitigate threats and aid in the prevention of cybercriminal activities. To better facilitate communication among and between members of the private and public sectors, OTA believes we must universalize incongruent standards, procedures, data formats and abuse reporting.

(4) **What issues are raised by the use of big data across jurisdictions, such as the adequacy of current international laws, regulations, or norms?**

Multinational companies must comply with often contradictory regulations due to disparate international laws and regulations. This engenders excessive technical investments, legal and consulting fees. OTA supports the White House commitment to pursuing international interoperability though the mutual recognition of commercial data privacy frameworks that incorporate effective enforcement and

---

8 Examples include, but are not limited to, data used to optimize site operations, site traffic analysis and frequency capping.


10 For example, the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) is a private information sharing community that improves timely local protection against cyber security threats by sharing security-event data, in near-real time, within a trusted federation. http://www.ren-isac.net/ses/
accountability mechanisms.\textsuperscript{11} However, the United States lacks a comprehensive privacy framework, making it harder for U.S. companies and officials to argue credibly against overbroad and unworkable privacy regulations.

Data localization regulations that are currently being proposed in the European Union would contribute to the balkanization of the internet.\textsuperscript{12} This would also negatively affect American businesses by increasing global operating costs or leading users to migrate towards non-US based services. Synchronization of data regimes will allow businesses to adopt more privacy protective schemes. Clear direction from the OSTP, accompanied with incentives and safe harbors, will support businesses in fulfilling and exceeding privacy requirements.

**Conclusion**

In summary, OTA looks forward to continued collaboration with all stakeholders in the ecosystem including online brands, technology providers, trade organizations, government agencies and advocacy groups who recognize the benefits and risks of big data. OTA recognizes that business accountability, data stewardship and data protection are all important privacy issues when considering implications of data collection. The goal of this discussion should be to maximize the potential benefits of data collection and the free flow of information while minimizing the privacy and related data security risks. The Online Trust Alliance thanks the White House Office of Science and Technology Policy for considering these comments.

Sincerely,

Craig D. Spiezle  
Executive Director and President  
Online Trust Alliance  
Craigs@otalliance.org  
https://otalliance.org  
+1 425-455-7400