Big Data RFI
Comments to the White House
From the Marketing Research Association
Submitted to: bigdata@ostp.gov
March 31, 2014

…………………...

The Marketing Research Association (MRA) applauds the White House for launching a public consultation on the issue of Big Data and privacy and how federal policy can best grapple with the topic. However, we do worry that it is far too broad to be tackled in such a short period of time, especially since the investigation appears to be shoe-horning multiple concepts into one big bucket.

Background

On January 17, 2014, the president addressed concerns about NSA surveillance, but turned the conversation to a much broader range of issues: "Challenges to our privacy do not come from government alone. Corporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes."[1] He launched a 90-day review of Big Data and privacy, led by White House Counselor John Podesta, which Podesta said aimed "to deliver to the president a report that anticipates future technological trends and frames the key questions that the collection, availability, and use of Big Data raise – both for our government, and the nation as a whole. It will help identify technological changes to watch, whether those technological changes are addressed by the U.S.'s current policy framework and highlight where further government action, funding, research and consideration may be required."[2] The White House asked for public comment,[3] and even launched a crude online survey to collect public opinion,[4] although we have sincere concerns about the effort's execution and effectiveness.[5]

Whether considered as the interconnected data-sharing nature of everyday consumer devices, from refrigerators and thermostats to mobile phones and medical devices, or the much maligned brokers of consumer-related data, or the ever-advancing realm of large data sets and predictive

[1] http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence
[2] http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy
[3] https://www.federalregister.gov/articles/2014/03/04/2014-04660/government-big-data-request-for-information
[4] http://www.whitehouse.gov/issues/technology/big-data-review
[5] "White House survey on Big Data and privacy is a good idea, poorly executed." March 24, 2014. http://www.marketingresearch.org/news/2014/03/24/white-house-survey-on-big-data-and-privacy-is-a-good-idea-poorly-executed

analytics, Big Data serves as sort of a cypher. The term is widely-referenced but poorly understood, and people in the public policy community see in it a variety of hopes and fears, particularly as they relate to data privacy and data security.

White House Counselor John Podesta outlined on March 3 how he was approaching the term: "data sets that are so large, so diverse, or so complex that the conventional tools that would ordinarily be used to manage data simply don't work. Instead, deriving value from these data sets require a series of more sophisticated techniques, such as Hadoop , NoSQL, MapReduce and machine learning. These techniques enable the discovery of insights from big data sets that were not previously possible."[6]

The White House seeks to look at Big Data from many standpoints:[7] data collection, sharing and use by government entities and private sector companies; government or law enforcement surveillance, as well as public health; what privacy protections exist or should exist, and how to apply them in all these different circumstances; and how the federal government could or should be encouraging or subsidizing Big Data innovation in the public and private sectors.

Each sub-category would be worthy of its own thorough investigation.

However, MRA is generally agnostic on government collection, sharing and use, except as it regards the decennial Census and the American Community Survey,[8] so we will focus our comments on private-sector data collection, sharing and use.

Survey, opinion and marketing research

MRA is a non-profit national membership association representing the survey, opinion and marketing research profession.[9] MRA promotes, advocates for, and protects the integrity of the research profession, and works to improve research participation and quality.

[6] http://www.whitehouse.gov/sites/default/files/docs/030414_remarks_john_podesta_big_data.pdf

[7] The White House asked 5 questions to help guide comments in this review: "(1) 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? (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? (3) What technological trends or key technologies will affect the collection, storage, analysis and use of big data? Are there particularly promising technologies or new practices for safeguarding privacy while enabling effective uses of big data? (4) How should the policy frameworks or regulations for handling big data differ between the government and the private sector? Please be specific as to the type of entity and type of use (e.g., law enforcement, government services, commercial, academic research, etc.). (5) What issues are raised by the use of big data across jurisdictions, such as the adequacy of current international laws, regulations, or norms?"

[8] "The Census Bureau's American Community Survey (ACS)." http://www.marketingresearch.org/the-census-bureau%E2%80%99s-american-community-survey-acs

[9] The research profession is a multi-billion dollar worldwide industry, comprised of pollsters and government, public opinion, academic and goods and services researchers, whose members range from large multinational corporations and small businesses to academic institutes, non-profit organizations and government agencies.

Survey and opinion research is the scientific process of gathering, measuring and analyzing public opinion and behavior. On behalf of their clients – including the government (the world's largest purchaser), media, political campaigns, and commercial and non-profit entities – researchers design studies and collect and analyze data from small but statistically-balanced samples of the public.[10] Researchers seek to determine the public's opinion and behavior regarding products, services, issues, candidates and other topics. Such information is used to develop new products, improve services, and inform policy.

Analysis of massive data sets is playing a growing role in the research business, both on its own and in conjunction with more traditional research methodologies. While Big Data analysis can and is done for research purposes, analysis in and of itself is not necessarily a research activity.

MRA, in consultation with the broader research profession, has developed a legal definition of bona fide survey, opinion and marketing research, which implicitly includes Big Data analytical research: "the collection and analysis of data regarding opinions, needs, awareness, knowledge, views, experiences and behaviors of a population, through the development and administration of surveys, interviews, focus groups, polls, observation, or other research methodologies, in which no sales, promotional or marketing efforts are involved and through which there is no attempt to influence a participant's attitudes or behavior."

Survey, opinion and marketing research is thus sharply distinguished from commercial activities, like marketing, advertising and sales. In fact, MRA and other research associations prohibit and attempt to combat sales or fundraising under the guise of research (referred to as "sugging" and "frugging"), "push polls,"[11] and any attempts to influence or alter the attitudes or behavior of research participants as a part of the research process.[12] Quite to the contrary, professional research has as its mission the true and accurate assessment of public sentiment in order to help individuals, companies and organizations design products, services and policies that meet the needs of and appeal to the public.

Data's use and purpose matter

Question #2 asks, among other things, "*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?*"

[10] A "sample" is a subset of a population from which data is collected to be used in estimating parameters of the total population.

[11] "'Push polls' - Deceptive Advocacy/Persuasion Under the Guise of Legitimate Polling." http://www.marketingresearch.org/push-polls-deceptive-advocacypersuasion-under-the-guise-of-legitimate-polling

[12] For instance, in the *MRA Code of Marketing Research Standards:* "7. Ensure that respondent information collected during any study will not be used for sales, solicitations, push polling or any other non-research purpose. Commingling research with sales or advocacy undermines the integrity of the research process and deters respondent cooperation. In addition, the possibility of harm from data sharing – such as health insurance companies adjusting an individual's costs based on information disclosed about their health behaviors or financial companies denying someone credit based on their propensity for online shopping – are the focus of growing public debate about Big Data and data brokers. Respondents should be assured that information shared in a study will only be used for research." http://www.marketingresearch.org/code

Question #4 also asks: "*How should the policy frameworks or regulations for handling big data differ between the government and the private sector?*"

Consumer concerns, such as they exist, rightly focus more on data use than its mere existence or collection. Certain types of data may be considered more sensitive than others, but even those are dependent both on an individual's subjective judgment and the context in which those data are used.

MRA generally supports a privacy model based on intended use – different protections and requirements for data privacy, depending on the uses to which that data will be put. Data to be collected, used and transferred strictly for bona fide survey, opinion and marketing research should be held to a different standard than ordinary commercial use, which will differ from purely transactional use. Those uses should all be treated differently than data used for determining a consumer's eligibility for things like health insurance, credit or a mortgage, or data used to prosecute crimes or prevent terrorism. Research purposes, unlike most of the other purposes, involve data collection, sharing and use of information about individuals only to understand broader population segments and demographic groups.

As noted, we appreciate the president's interest in Big Data and privacy. However, we are also extremely concerned that, by lumping NSA spying and private-sector data collection into the same bucket in his January 17 speech and in this review, the president has inadvertently minimized the importance of public concern about the NSA and Edward Snowden's revelations (whether or not they are legitimate) and redirected that concern to a completely unrelated target. We sincerely hope that, through the course of this review, the White House is able to properly separate these spheres of activity, since such data uses are so extremely different.

While Big Data should be approached with common privacy principles, the application of those principles must differ depending on the purpose and use of the data in question, in both the public and privacy sectors. Even in the public sector, those purposes and uses will vary dramatically. The purposes of IRS data collection – normally, for help in collecting taxes owed by individuals – are extremely different from the Census Bureau, which needs to collect individuals' data in order to learn about diverse groups of Americans. Neither sort may be deemed as intrusive by some Americans as data surveillance by law enforcement and espionage agencies, and thus may be held to different standards. Alternatively, Americans may wish to give even greater leeway to such agencies, since their purposes are so important.

Public policy implications of Big Data

Question #1 asks: "*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?*"

Among the concerns raised about the policy implications of Big Data are: (1) notice and consent for data sharing, access and correction; (2) data minimization; (3) deidentification; and (4) eligibility decision-making.

(1) Notice and consent for data sharing, access and correction

Many concerns about massive data sets center on how to apply consumer notice and consent to the workings of massive data sets.

MRA already requires that researchers seek tailor-made approaches to transparency with regard to clients, research participants, and the public at large that are appropriate to different modes and methods of research. Research best practices require disclosure of what data is being collected and used, and for what purpose, that research organizations designate a chief privacy officer to take responsibility for the privacy of respondents and their data,[13] and that participants have the opportunity to opt out.

But should consumers be required to be notified when their data is shared and be able to either opt out of such sharing, or be required to opt into it?

While some survey, opinion and marketing research indicates that consumers, on average, are concerned about their privacy, notifying consumers of every minute thing happening with their data could work counter to the interest of actually keeping consumers well informed, since over-notification and excessively lengthy privacy policies already may be causing consumers to stop paying close attention to their own privacy needs and wants and growing more careless in how they handle their own data.

Moreover, turning to opt in to any great extent for data sharing could severely tilt the competition in the data business towards the largest companies (like Google and Facebook), who have so much internal data that they don't need to share.

The question of whether or not consumers should be given access and control over data regarding them appears to be more complicated.

The demand of access to consumer data may make sense in contexts of eligibility, where such data (particularly if inaccurate) could adversely impact a consumer's credit rating, personal or professional reputation, or in the likelihood of becoming a victim of identity theft or fraud. However, none of these conditions should reasonably be assumed to apply to survey, opinion and marketing research data. Participation in survey, opinion and marketing research is voluntary.

The cost of access and correction could potentially be quite onerous, especially for smaller research companies and organizations, given a potential deluge of frivolous or pointless inquiries. Since the research process is interested in broad groups, not individuals, compiling and tracking individual consumer data, by the individual, would require complex and expensive procedures and infrastructure not currently in use. Moreover, such tracking could lead to a much greater threat of harm from data leakage and empower the kind of consumer tracking that causes privacy concerns.

[13] "Designating a Privacy Officer." http://www.marketingresearch.org/designating-a-privacy-officer

The ability of companies to authenticate the identity of consumers requesting access is another potential problem. That kind of authentication would require collecting and checking even more data, which runs counter to our interest in data minimization and limited data retention. Plus, necessary authentication procedures and processes would add to the cost in money and time on the part of research organizations.

MRA supports the concept of a "sliding scale" for access and correction responsibilities in order to reconcile the vague benefits with the expected costs. We propose that the availability and extent of access should depend on the data actually being susceptible to use for criminal or fraudulent purposes. As pointed out earlier, purpose and use matter.

(2) Data minimization

As a broad principle, data minimization – not collecting or maintaining more data than necessary to fulfill a certain purpose – makes sense. However, within various modes and methods of research, the need to retain data will vary, and should be properly subject to those needs, not an arbitrary decision by fiat of law, or by the decision of a regulatory body unfamiliar with the processes and practices of research. Additionally, a major objective of research is to understand attitudes, behaviors and opinions over time. The collection and analysis of this information often leads to new theories over time, requiring the re-visiting of older data. Prescribed retention periods would thus diminish the long-term value of data collected for research purposes.

MRA would thus be concerned about a law or a regulatory agency setting time constraints without being familiar with the processes and practices of all businesses that would be impacted by their implementation, including the many processes and practices of survey and opinion research.

(3) Deidenification

Anonymizing or de-identifying personal information whenever possible, by aggregating or pseduonymizing it, is a sensible principle, and one that MRA and the research profession support. In fact, carving out a safe harbor from many privacy regulations for data that has been protected in this way makes a lot of sense. We are concerned with the specific definition of how and to what extent to do it.

There is an ongoing debate in the academic and policy arenas on whether or not data can ever be fully de-identified or anonymized. If it cannot, then any piece of data could ultimately be personally identifiable.

Speakers at a conference in Washington, DC in December 2011 clashed extensively over this very question.[14] Several researchers, like Latanya Sweeney, director of the Data Privacy Lab at Harvard University, contended that most any data could be re-identified, based on a pair of her

[14] "Personal Information: The Benefits and Risks of De-Identification." A conference held by the Future of Privacy Forum (FPF) on December 5, 2011. http://www.futureofprivacy.org/2011/10/19/upcoming-fpf-event-one-day-conference-dec-5/

studies. Several other researchers responded that the two biggest re-identification studies were very limited cases and not generalizable.[15]

To illustrate the debate, consider a data point such as date of birth, which could be considered personally identifiable because it splits the population into 25,000 cells and can enable re-identification. If you combine such data with a zip code containing only a handful of people in a certain age range, it may be very easy to re-identify. Professor Peter Swire of Ohio State University made an analogy at the conference to a cop collecting clues. A suspect is male, tall, with red hair. That would not be enough to re-identify, but it would certainly make it easier. It is more a matter of how much legwork, analysis and extra data is available and accurate. That is what weighs against the public being able to re-identify de-identified data, according to Professor Swire.[16]

Khaled El Eman, a researcher at the University of Ottawa, felt that the data re-identification efforts by Sweeney and company were the exceptions that proved the rule. Most attacks fail miserably, he said. According to Eman, the studies that succeeded are too small, too few, too ambiguous, too heterogeneous and with confidence intervals that are way too large. Eman concluded that, “Re-identification is hard.” He suggested that there would need to be 40-50 replicable studies to start to change such a conclusion.[17]

It is also important to remember that de-identification carries costs as well as benefits. Daniel Barth-Jones, epidemiology professor at Columbia University, warned at that conference that excessive de-identification of data can yield huge statistical errors and inaccurate research results: the greater the level of de-identification, the less statistically useful the data becomes.[18] Blanket de-identification could grind statistical research and number-crunching to a standstill. Ultimately, is there a point in de-identification to a level where there are significantly easier and cheaper ways of getting the data? Professor Barth-Jones ended his presentation with a warning about trade-offs, that the real harm is not the ephemeral threat to privacy but the real threat of “not catching the next HIV epidemic”.[19]

There may be benefit to engaging the government agencies in the broader public debate over de-identification, but they should not be encouraged to arbitrarily end that debate.

(4) Eligibility decision-making

Identifying (and especially, quantifying) the harm arising in data privacy often proves elusive for both privacy activists and regulatory authorities. Aside from legitimate concerns about identity theft, fraud and other criminal abuse, the only potential harm agreed upon to date from Big Data is negative impact on eligibility decisions, such as whether or not consumers should receive health insurance, what kind of credit or mortgage rate they should be offered, or discounts or premiums they should be offered or charged when shopping for products and services.

[15] FPF Conference.
[16] FPF Conference.
[17] FPF Conference.
[18] FPF Conference.
[19] FPF Conference.

A recent Senate hearing on data brokers[20] provides useful illustrations.

Professor Joseph Turow from the Annenberg School for Communication expressed fears at the hearing about the power of advanced computing and statistics "blending your information into complex algorithms" to "better understand you," which he thinks is "turning into an actuarial activity." He touched throughout the discussion on the unfairness of Big Data predictive analytics, from the more well-known algorithmic decision-making for mortgage loans to the dramatically variable pricing of airline tickets. He even suggested that lawmakers should consider "how many data points companies should be allowed to buy about us at a time, and how they can be merged with other data points."

Senator Ed Markey touched on similar concerns at the hearing, decrying the attachment of "propensity scores" to American consumers, without their knowledge and consent, which then become the basis for targeting offers or benefits. High value prospects get good offers, he said, but many others end up getting shut out.

As a recent *Forbes* article described such price discrimination, "In a traditional bazaar a seller might charge a well-dressed buyer twice as much as another based on visual clues or accents. Big data allows for a far more scientific approach to selling at different prices, depending on an individual's willingness to pay."[21]

A more recent workshop hosted by the Federal Trade Commission (FTC) on "Alternative Scoring Products"[22] discussed many similar concerns. Edmund Mierzwinski, consumer program director with the U.S. Public Interest Research Group, pointed out that his organization is not concerned about Big Data, but that they are "concerned about its use and its impact on financial opportunity." However, as pointed out by Stuart Pratt, president and CEO for the Consumer Data Industry Association, the reward and reinforcement of customer loyalty is nothing new, and more than a few participants pointed out that the use or abuse of Big Data for credit and other financial services determinations are already covered by other federal laws, such as the Fair Credit Reporting Act.

MRA happens to think that eligibility decisions are an issue worthy of potential regulatory action regarding Big Data, but crafting the right response has so far proven elusive. Instead of precisely and objectively defining the eligibility decisions that require regulatory oversight and action, the privacy debate has, so far, run a wide and subjective gamut. Meanwhile, some private sector

[20] "What Information Do Data Brokers Have on Consumers, and How Do They Use It?" Senate Commerce Committee. December 18, 2013. http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a

[21] "Different Customers, Different Prices, Thanks To Big Data." by Adam Tammer. Forbes. April 14, 2014. http://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/

[22] FTC workshop. March 19, 2014. http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products

companies are innovating on their own to try to bring transparency to some of that decision-making, such as Acxiom's AboutTheData website.[23]

Harmonization of international data privacy protection

Question #5 asks: "*What issues are raised by the use of big data across jurisdictions, such as the adequacy of current international laws, regulations, or norms?*"

The rise of Big Data is one of multiple issues driving the European Union (EU) to revamp and expand the 1998 European Commission's Directive on Data Protection, a regulation looked to as the model for privacy regulation by many countries around the world, whether they like it or not.

The Data Directive prohibits the transfer of "personal data" to non-EU nations that do not meet the European "adequacy" standard for privacy protection. The EU Data Directive places significant restrictions on the collection, use and disclosure of personal data that prove taxing for many researchers. Intentionally or not, the EU wields the Data Directive and its "adequacy" standard as an anti-competitive trade measure, discriminating against U.S. companies in digital trade because they do not deem the U.S. to have "adequate" data privacy protections. The main way a nation can be deemed "adequate" is by passing laws that closely imitate the Data Directive.

Fortunately, for now, in addition to adopting binding corporate rules, U.S. companies can self-certify to the U.S. Department of Commerce that they comply with the seven principles of the U.S.-EU Safe Harbor[24] and at least have some mechanism for data transfer. While it is a self-certification, the FTC enforces compliance with the Safe Harbor under its Section 5 authority to prosecute deceptive practices (not living up to one's public claims). As the EU tries to rewrite their Data Directive, it is essential that we maintain the Safe Harbor – our primary protection for the conduct of digital commerce and research. High level EU officials have made a habit recently of attacking the standing of the U.S.-EU Safe Harbor[25] and the EU Parliament recently voted to essentially get rid of it.

Comprehensive data privacy proposals have been advanced for the last few years by the FTC, the White House, and Members of Congress, all with the goal of better emulating the EU privacy regime so that the U.S. will be deemed "adequate" in its privacy protections by the EU.

MRA supports some form of baseline consumer data privacy law and we feel that is an important issue with which the White House must grapple as part of this Big Data and privacy review. However, the expansive measures envisioned by some parties go far beyond the baseline – with questionable promise of success. "Harmonization" of U.S. law to an EU standard may not make

[23] https://aboutthedata.com/

[24] Notice, Choice, Onward Transfer (to Third Parties), Access, Security, Data Integrity and Enforcement. http://export.gov/safeharbor/eu/index.asp

[25] "EU questions decade-old US data agreement." By Nikolaj Nielsen. EUObserver.com, July 22. http://euobserver.com/justice/120919 and "EU outlines improvements to US data agreement." By Kate Tummarello. *The Hill*, November 27. http://thehill.com/blogs/hillicon-valley/technology/191618-eu-outlines-improvements-to-us-data-agreement

the most sense economically. According to Congressman Lee Terry (R-NE-01), the U.S. has “flexibility” in its privacy regime, allowing for the “emergence of the data economy,” which he has identified as “a reason why we are the dominant innovators in this area and Europe is not.”[26] Similarly, as outlined by several large technology companies’ chief privacy officers at an Internet Association panel discussion in 2013, innovative data businesses generally develop and grow in the US, not in Europe, and our approach to data privacy may be a key factor in our competitive advantage.[27]

More importantly, over the course of many public and private engagements in the past couple of years, Members of the European Parliament and European Commission have indicated that none of the comprehensive proposals offered so far in the U.S. would, if enacted, win the U.S. the coveted “adequacy” designation by the EU. It is possible that nothing short of a complete substitution of EU law for U.S. law would satisfy EU authorities.

Discussions of “harmonization” in trans-Atlantic privacy regulation, particularly given the swelling potential of Big Data, should focus on incorporating the U.S.’ strong enforcement mechanisms[28] and self-regulatory entrepreneurship to the EU’s more bureaucratic framework of privacy regulation.

What about the president’s multistakeholder process for privacy?

As part of this review, the White House strangely seems to have overlooked the president’s own multistakeholder privacy process, where the National Telecommunications and Information Administration brings together technology, policy, legal and other experts from innovation companies, trade associations, activist groups, academic institutions and other organizations to develop and agree upon enforceable privacy codes of conduct. While the first such effort, on mobile apps privacy,[29] ended somewhat ambiguously last year, the second effort, on facial recognition privacy, is already well underway.[30] MRA has been an active participant, including presenting a white paper[31] as part of a panel on February 5.

We would like to see the White House give this innovative approach more time to work before declaring where privacy regulation should go.

[26] "Rep. Terry: Data is the New Gold." October 29, 2013. http://www.marketingresearch.org/news/2013/10/29/rep-terry-data-is-the-new-gold

[27] “Corporate privacy officers discuss global compliance, trans-Atlantic competition, a comprehensive privacy law, and the US-EU Safe Harbor.” March 7, 2013. http://www.marketingresearch.org/news/2013/03/07/corporate-privacy-officers-discuss-global-compliance-trans-atlantic-competition-a-co

[28] “U.S. takes the gold in doling out privacy fines.“ by Jay Cline. *Computerworld*. February 17, 2014. http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=17

[29] “The NTIA Multistakeholder Process for Mobile Apps Privacy.” http://www.marketingresearch.org/the-ntia-multistakeholder-process-for-mobile-apps-privacy

[30] “Facial recognition privacy: Kicking off another NTIA multistakeholder process.” February 5, 2014. http://www.marketingresearch.org/news/2014/02/05/facial-recognition-privacy-kicking-off-another-ntia-multistakeholder-process-and-an-

[31] “The Marketing Research Applications of Facial Recognition Technology.“ MRA white paper. February 6, 2014. http://www.marketingresearch.org/sites/mra/files/pdfs/MRA_facial-recognition-MR-applications_2-6-14.pdf

Conclusion

Survey, opinion and marketing researchers already encounter significant public apathy with respect to research participation. Research "response" rates have been falling for the last couple of decades, driving up the cost of and time involved in achieving the required number and strata of participants to reach viable representative samples for most research studies. That always informs MRA's approach to any new regulatory impediments to research: that the issues identified above could make it harder to reach and involve research participants, increase non-response bias, make it more difficult to share and learn from data, and adversely impact the accuracy of research results.[32]

We've highlighted in these comments some areas of Big Data privacy regulation that may hold the most need and promise for consideration, such as notice and choice for consumer data sharing, access and correction, data minimization, deidentification, eligibility decision-making, and our digital trade relationship with the EU.

MRA looks forward to working with the White House on these and other important privacy issues.

However, the White House's review, as well-intended and necessary as it may be, spawned from a debate not about most of the issues we've discussed in these comments, but about the surveillance of citizens by American intelligence authorities. As observed recently by the *Washington Post*'s Catherine Rampell, "All the information the government collects in secret probably does little to cultivate trust in the collection that occurs more transparently."[33]

Privacy issues in the private sector, while certainly a concern, are already being tackled on multiple fronts. Between robust enforcement by the FTC and other agencies of unfair or deceptive practices, and the president's nudging towards more effective self-regulation through his multistakeholder process, there is plenty going on already. MRA urges the White House to strongly consider where its attention would best be focused and to not dictate direction too strongly to the independent authorities and processes already innovating in ways the White House would want.

[32] This wouldn't just impede bona fide survey and opinion research. It would ultimately result in higher costs for research – costs which would be passed on to all Americans, in the form of: higher prices for goods and services; lengthier time before new or better goods and services are brought to the marketplace; delayed introduction of new or better public policies; and a decreased amount of research ordered by companies, who might then bring less well-tested and researched products and services to market, harming consumers in the end because the goods and services did not fulfill consumer expectations or needs.

[33] "'Big data' needs a helping hand in Washington." By Catherine Rampell. *The Washington Post*. March 27, 2014. http://www.washingtonpost.com/opinions/catherine-rampell-big-data-needs-a-helping-hand-in-washington/2014/03/27/11b1f90e-b5bd-11e3-8cb6-284052554d74_story.html