Submitted 8/5/14 via privacyrfc2014@ntia.doc.gov

August 5, 2014

John Morris, Associate Administrator and Director of Internet Policy
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Attn: Privacy RFC2014
Washington, DC 20230

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

Dear Mr. Morris:

Thank you very much for the opportunity to comment on the White House's Big Data Report and the PCAST Report through NTIA's request for public feedback.

The undersigned organizations represent a broad coalition of leading privacy, consumer and civil liberties groups. This letter contains concrete recommendations for the Obama Administration on how to protect the privacy rights of American citizens with regard to big data, and attempts to answer some of the questions posed in the NTIA's request for comments.

Americans now face a formidable commercial surveillance infrastructure over which they have little control. Data collection and sharing is ubiquitous, invisible, intrusive and largely unregulated. Consumers have repeatedly made it clear that their confidence in the online ecosystem is eroding with every data breach, whistleblower report, media article and change in "Terms of Service."

The Administration has taken a positive leadership role in addressing the public's concern by drawing attention to the need for public policy change on privacy and big data, but it must take bold *action* now to begin to codify its recommendations. Enacting baseline privacy legislation that implements a strong and resonant Consumer Privacy Bill of Rights (CPBR) is the single most effective way to answer the public's call for basic online privacy rights, ensure trust in the online marketplace and create a level playing field for online businesses.

The following recommendations should be implemented to strengthen the CPBR:

1. **Make it consequential.** As the White House looks to its legacy, we believe that implementing a strong and comprehensive CPBR would be an iconic moment in American consumer protection. The privacy bill should be a benchmark for modern consumer protection that respects Americans' deep history of personal privacy in a technology context. We believe that it's preferable for the Administration to propose nothing rather than a weak bill that does little to advance privacy protections. Chiefly, the CPBR must

safeguard individual privacy rights and provide for meaningful enforcement, empowering relevant agencies such as the Federal Trade Commission (FTC) and Federal Communications Commission (FCC) to effectively and thoughtfully reign in data collection and use practices. Industry self-regulation is not enough, and has failed to inform or protect consumers. The Administration should empower the FTC to exercise oversight on any consumer privacy-related multi-stakeholder processes to give the necessary weight, accountability and enforcement to both the process and the resulting codes. *(Question 6)*

2. **Fill in the blanks of the FIPPs.** We support the FIPPs framework used by the White House in the CPBR but believe there exist key recommendations that need to be fleshed out. The first element of the CPBR, individual control, suggests that consumers only have rights with respect to personal data collected *from* them, effectively giving big data free reign to use consumer data they have from other sources. There should be no general distinction between personal data collected from consumers and personal data collected in some other manner. Even public records contain sensitive personal information, and when they are collected and indexed by private firms, individuals should retain control over their data. In addition, the framework endorses data limitation as a governing principle; we believe it should include specific restrictions on both data collection *and* use, including limitations on the uses of data downstream and a rubric that allows businesses to determine ahead of time whether any collection and use of data is appropriate in the transactional context. The CPBR framework makes clear the importance of transparency; a bill that implements the CBPR should require that industries provide comprehensive transparency to consumers on data practices and provide government entities with algorithmic transparency, so that efforts to regulate practices keep pace with reality. *(Questions 3, 6)*

3. **Recognize the real harms and significant risks.** According to a 2014 report by the Ponemon Institute[1], 432 million online accounts in the U.S. have been hacked in the last 12 months alone, impacting about 110 million Americans. The numbers are staggering: 70 million Target customers, 33 million Adobe users, 4.6 million Snapchat users, and potentially all 148 million eBay users have had their personal information exposed through database breaches. Despite these statistics, data breaches have continued unabated and mostly unchecked by the federal government. The recent PCAST report inexplicably determined there to be little risk to consumers in the collection of personal data, an assertion that is out of sync with reality. *The risk to consumers is significant and immediate.* Many other filers to this proceeding will provide additional details on these harms, and it's clear there is a need for preventative action. The FTC's recent report on data brokers[2] warned "…collecting and storing large amounts of data not only increases the

[1] Quantifying the cost of a data breach, Ponemon Institute, 2014.

[2] Data Brokers: A Call for Transparency and Accountability, Federal Trade Commission, 2014.

risk of a data breach or other unauthorized access but also increases the potential harm that could be caused." Data thieves can perpetrate bank, loan, benefits, employment and tax fraud, as well as identity theft. Studies show that consumers whose data is breached are more than four times as likely to become victims of identity theft[3], a crime that is both costly and time-consuming for consumers to resolve. The FTC report also lays out how the vast amount of personal information—such as race, religion, political affiliation, ethnicity, gender, age, household income, weight, health conditions, and guns and ammunitions purchases—allows data brokers to identify and categorize an individual. Companies' consumer profiling and scoring can obstruct access to quality financial assistance that is necessary to climb out of poverty.[4] Consumer scores in particular threaten privacy, fairness and due process because the scores are largely invisible to consumers and can easily evade the rules established to protect consumers.[5] The Administration must not be blinded by the hyperbolic arguments touting big data's benefits to the point that it neglects to see the current and potential impact on the finances and wellbeing of consumers. Nor, too, should it fail to understand the real harm experienced by businesses that lose the trust of their customers by default. A 2014 TRUSTe Consumer Confidence Privacy Report[6] found that this falling level of trust online negatively impacts businesses, with 83 percent of respondents less likely to click on online advertisements, 80 percent actively avoiding apps that they don't believe protect their privacy, and 74 percent less likely to enable location tracking on their smartphones. The Administration should not wait for an avalanche of big data victims (consumers or businesses) before taking action to enact strong legislation. *(Questions 2, 5, 10)*

4. **Carve out special protections for sensitive categories.** The Administration should establish special protections for sensitive data categories like financial information, health, race, ethnicity, geo-location, age and data collected in the education context. Data brokers and other information service providers, as shown by the FTC report, often pool their data on individuals in real time to generate profiles, unbeknownst to most consumers. As the White House Big Data report correctly warns, predictive data, data analytics and profiling offer ample opportunity for the existence of hidden proxies for illegal discrimination and other harmful differential treatment. The privacy bill must clearly delineate boundaries of acceptable and unacceptable data use for sensitive data, with special attention paid to the potential financial, educational and reputational impact of profiling,

---

[3] 2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters, Javelin Strategy and Research, 2013.

[4] Chester, Jeff and Mierzwinski, Ed. Selling Consumers Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act, Suffolk University Law Review, 2014.

[5] Dixon, Pam and Gellman, Robert. The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future, World Privacy Forum, 2014.

[6] TRUSTe 2014 Consumer Confidence Privacy Report.

particularly on underserved and disadvantaged and voiceless communities. The Administration should reinforce its statements on necessary extra protections for children, teens and students, and propose legislation that enhances regulators' policy tools to ensure consumer privacy in the marketplace. *(Questions 5, 8, 10, 12)*

5. **Implement practical solutions.** Solutions to protect individual privacy will not work unless they are backed up with individual rights. The "notice and consent" model in current practice provides an important illustration of this issue. Consumers are given a "take it or leave it" proposition—agree to terms of service or don't get access to a particular product or service—that is not an authentic choice. This model does not offer real control over data collection and usage, nor do consumers have redress or any way of knowing if their information is taken regardless of their consent. Regarding de-identification, we recognize that it has the potential to provide a middle ground that protects privacy while allowing for greater use of data. However, we also recognize that de-identification techniques are not a guarantee against re-identification or against the use of de-identified data in ways that discriminate against groups of people.[7] [8] Despite these shortcomings, we support greater use of de-identification techniques when coupled with policies that encourage the development of better technology, clearer standards and overall accountability. One way to allow for the sharing of data that has been partly de-identified while still protecting privacy is to require the transfer of the data under a chain of custody agreement. The agreement should bind the recipient (and any subsequent users) to use the data only in defined and appropriate ways; not to attempt to re-identify the data or to allow others to do so; to use the data in a broadly transparent way that disclaims discriminatory and other improper uses; and to transfer the data to others only when permitted and then only under the same terms and chain of custody agreement. Those who obtain and use de-identified data through a chain of custody agreement should be accountable for compliance. Accountability can be achieved through regulatory oversight and enforcement, through private rights of action, through liquidated damages, through future bans of access to data, and in other ways. *(Questions 4, 7)*

The proposal and enactment of strong consumer privacy legislation in the context of the CPBR is essential for achieving the complementary goals of protecting the privacy rights of consumers, maintaining consumer trust online and supporting business innovation.

---

[7] Sweeney, Latanya. k-anonymity: A Model for Protecting Privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10 (5), 2002; 557-570. The study, released by the FTC, illustrates how easy it is to re-identify Marylanders' health records using only ZIP code, birth date, and sex.

[8] Narayanan, Arvind and Felten, Edward. *No Silver Bullet: De-Identification Still Doesn't Work* (July 9, 2014). Narayan and Felten state in their study "there is no evidence that de-identification works either in theory or in practice..."

Sincerely,

American Civil Liberties Union
Center for Digital Democracy
Consumer Action
Consumer Federation of America
Consumer Watchdog
Common Sense Media
Privacy Rights Clearinghouse