The Internet Association

August 5, 2014

Submitted electronically via e-mail: privacyrfc2014@ntia.doc.gov

Attn: Privacy RFC 2014
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Washington, DC 20230

RE: Request for Comments Concerning Big Data and the Consumer Privacy Bill of Rights (Docket No. 140514424-4424-01)

The Internet Association is a trade association representing leading Internet companies, which engages policymakers to protect Internet freedom, foster innovation and economic growth, and empower users.[1] We appreciate the opportunity to submit comments in response to the Department of Commerce's June 4 Request for Comments.

After a 90-day review of how "big data" impacts American citizens as well as the public and private sector, the White House's Office of Science and Technology Policy (OSTP) released a report that detailed the findings from its review and proposed a set of recommendations to further guide exploration of this important issue. One recommendation resulting from this scoping exercise charged the Department of Commerce (Commerce) to pursue a public consultation period on "big data" and its impact on the Administration's 2012 Consumer Privacy Bill of Rights (CPBR).[2] The report indicates that Commerce will use the comments and feedback from this consultation as a basis for draft legislation, which will be submitted by the President to Congress and for consideration by stakeholders.[3]

---

[1] The Internet Association, the unified voice of the Internet economy, represents the interests of the leading Internet companies including Airbnb, Amazon, AOL, Auction.com, eBay, Etsy, Expedia, Facebook, Gilt, Google, Groupon, IAC, LinkedIn, Lyft, Monster Worldwide, Netflix, Practice Fusion, Rackspace, reddit, Salesforce.com, SurveyMonkey, TripAdvisor, Twitter, Uber Technologies, Inc., Yelp, Yahoo!, and Zynga.

[2] EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 60 (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [hereinafter *White House Big Data Report*].

[3] *Id.*

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

Building on this review, we encourage the Administration to evaluate the current legal landscape of consumer protections to understand what regulatory, self-regulatory, and other measures are in place today to improve consumer welfare. Also, we urge the Administration to work with stakeholders to identify the actual privacy and discrimination harms, if any, posed by "big data." Finally, the Administration can compare the actual harms identified to the protections offered by the existing legal regime, and determine whether any gaps exist.

Any effort to evaluate our nations' policies around "big data" must be premised on an effort to maintain consistency with existing policy and legal frameworks and to focus efforts on any areas where real gaps exist. We are concerned that any legislative proposal to address "big data" may create a "precautionary principle problem" that hinders the advancement of technologies and innovative services before they even develop.[4]

The Internet Association endorses a conversation shift towards a "responsible use framework" of data and away from data collection in order to take further advantage of the benefits afforded by data analytics and also to better assess risks and harms. This shift should be allowed to happen through self-regulation rather than by regulatory fiat. Readjusting the thinking towards responsible uses of data will promote innovation and future growth of the Internet industry, which is driven by data analytics. Consequently, we do not support preemptive legislative action, which could disrupt future growth of the innovation economy.

We also believe the Administration should devote additional resources to supporting research and development to identify new privacy-enhancing technologies and to supporting digital literacy efforts. Finally, The Internet Association recommends the Administration continue to stress interoperability with other jurisdictions' privacy systems, particularly as they look to follow the United States' lead in using data to spur their economies.

I. The Internet Association supports the Administration's recognition of the significant benefits afforded by "big data" and believes that the current landscape of protections afforded to users should be carefully documented and analyzed before turning to new legislative proposals.

OSTP's "big data" report entitled, "Big Data: Seizing Opportunities, Preserving Values," highlights the Administration's recognition of the important economic, social, and political benefits made possible through "big data." The Internet Association is encouraged by the report's detailed examples showcasing how big data analytics "boost[s] economic productivity,

[4] Adam D. Thierer, *Privacy Law's Precautionary Principle Problem*, 66 ME. L. REV. 468 (2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2449308.

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

drive[s] improved and government services, thwart[s] terrorists, and save[s] lives."[5] Additionally, the report notes that in today's innovation economy, "customers and companies are increasingly demanding that … data be analyzed to benefit them instantly."[6] These benefits span across multiple sectors from protecting critical infrastructure such as financial and energy systems to offering free, expansive content, products, and services for consumers to enjoy online.[7]

We are also pleased to see the Administration's continued efforts to explore new ways to reap the benefits from "big data." Our association looks forward to serving as a resource to the Department of Commerce as it hires its first-ever chief data officer responsible for "pull[ing] together a platform for all of [its] data sets."[8] We see significant promise in the chief data officer's charge with the help of a data advisory council comprised of private sector leaders to use government-held data sets to unlock $3.3 trillion in U.S. investments annually and activate new businesses, products, and services.[9]

As an industry on the forefront of leveraging data to innovate and spur technological advancements, we understand the great value that relevant, personalized content and services can bring to Internet users. Users choose to access our member companies' content and services because they trust that they will benefit from these services, and trust that member companies will use their data responsibly. Notably, this concept is highlighted in the Administration's 2012 report, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." The report's foreword begins with the sentence: "Trust is essential to maintaining the social and economic benefits that networked technologies bring to the United States and the rest of the world."[10] The report recognizes that this trust has permitted users to turn to Internet services to engage in social interactions, political movements, and commerce.[11] Self-regulation and agreements between industry and users are proven models for effectively and adequately protecting users, thus maintaining their trust for the continued growth and development of our industry and both the U.S. and global economies. Our member companies compete on privacy and understand that there are few barriers to switching among providers should consumers lose confidence in an online platform or service.

---

[5] *White House Big Data Report* at 5.
[6] *Id.*
[7] *Id.* at 39-41.
[8] Tony Romm, *Commerce to Hire Chief Data Officer,* POLITICO, (July 14, 2014). .
[9] *Id.*
[10] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY i (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter *White House Blue Print*].
[11] *Id.*

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

We urge the Administration to carefully consider the broad range of existing protections - both self-regulatory and government-regulated – that help ensure the robust and continually evolving suite of services our member companies and many others provide in a way that protects users' interests.

A. Many Internet companies adhere to self-regulatory codes, subject to enforcement by the Federal Trade Commission (FTC) and actively engage in multi-stakeholder processes to set sector-specific codes of conduct.

To ensure that our industry strikes the appropriate balance between offering innovative services and protecting users' privacy, many of our member companies voluntarily abide by self-regulatory codes such as the Interactive Advertising Bureau (IAB)'s Self-Regulatory Principles, Digital Advertising Alliance's (DAA) Self-Regulatory Program, and the Network Advertising Initiative (NAI) Code of Conduct, which are subject to enforcement by the FTC. Below is a description of each program:

- **Interactive Advertising Bureau (IAB)'s Self-Regulatory Principles:** Developed by leading industry associations, these principles also apply to a cross-sector of industry players that partake in the delivery of relevant advertisements to users online. This program consists of seven principles (based on the FTC's February 2009 "Self-Regulatory Principles for Online Behavioral Advertising" proposal): (1) education, (2) transparency, (3) consumer control, (4) data security, (5) material change, (6) sensitive data, and (7) accountability.[12]

- **Digital Advertising Alliance's (DAA) Self-Regulatory Program:** This program consists of three, separate principles that provide guidance for companies regarding online behavioral advertising (oba) and multi-site data, and application to the mobile environment.[13] As the FTC explains in its 2012 report, the DAA, which is a multi-sector coalition, created a mechanism to educate consumers about oba and allow them to opt out, if desired.[14] Additionally, the code puts restrictions on the use of consumers' data for certain secondary purposes,

---

[12] INTERACTIVE ADVERTISING BUREAU, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 4 (2012), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf.
[13] THE DAA SELF-REGULATORY PRINCIPLES, http://www.aboutads.info/principles/ (last visited Aug. 4, 2014).
[14] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES iii (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter *FTC Report*].

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

including use of multi-site data for eligibility for employment, credit, health care, or insurance.[15]

- **NAI Code of Conduct:** Since 2000, this Code imposes notice, transparency, choice, and data security requirements on NAI's 90+ members.[16] NAI has updated its code twice since its creation in 2008 and 2013 to ensure that it continues to be rigorously enforced through various programs such as annual reviews, technical monitoring, sanction procedures, etc. to ensure that its members adhere to the Code.[17]

In addition to these leading examples of self-regulatory programs, the Internet companies participate in various multi-stakeholder processes and fora, including the NTIA-led process established by the White House Privacy Blueprint.

B. Commerce should conduct a comprehensive review of the United States' existing privacy regime, which allows for effective federal and state enforcement.

In addition to self-regulatory codes and multi-stakeholder processes related to privacy, the United States' flexible and multi-layered privacy regime provides robust protections against privacy violations. This regime allows industry players who conduct business within these guidelines to freely innovate. At the federal level, the Federal Trade Commission Act (FTC Act), which provides comprehensive consumer protection, is bolstered by sectoral statutes including the Health Insurance Portability and Accountability Act, Gramm-Leach Bliley Act, Fair Credit Reporting Act, and the Children's Online Privacy Protection Act.

Additionally, at the state level, equivalent laws bar "unfair or deceptive" acts or practices, and authorize enforcement actions by regulators. The FTC and state attorneys general take action to protect consumers on important issues such as identity theft and data breaches. As discussed in our OSTP comments, U.S. regulators and law enforcement officials have a proven track record of protecting consumer privacy in a balanced and swift manner that focuses on actual harms while allowing industry to offer consumers innovative products and services.[18]

---

[15] *Id.*

[16] NETWORK ADVERTISING INITIATIVE, 2013 NAI CODE OF CONDUCT 1-2 (2013), *available at* http://www.networkadvertising.org/2013_Principles.pdf.

[17] *Id.*

[18] THE INTERNET ASSOCIATION WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY BIG DATA COMMENTS (Mar. 31, 2014), *available at* http://internetassociation.org/wp-content/uploads/2014/03/3_31_-2014_The-Internet-Association-Comments-Regarding-White-House-OSTP-Request-for-Information-on-Big-Data.pdf [hereinafter *The IA Comments*].

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

At this time, any legislative proposal, to address "big data" may result in a "precautionary principle problem" that hinders the advancement of technologies and innovative services before they even develop.[19] Given the breadth of existing protections for consumers, we encourage the Administration to carefully examine the existing regime to avoid negative, unintended consequences.

II. Actual harms posed by "big data" as well as methods to address these harms should be identified before taking steps to legislate. Otherwise, the Administration runs the risk of limiting the ability for data to create helpful innovation and services.

Throughout OSTP's 90-day review, the "big data" debate focused on highlighting its benefits while pinpointing its potential harms. It is also important to note that a majority of concerns raised by the report were largely speculative rather than actual harms.[20] This calls into question whether there is a need to engage policymakers and industry on this issue rather than focusing attention and resources to areas where users experience real harms, such as data security.[21] The report revealed the use of "big data" for discriminatory practices as the most salient harm deserving attention.[22] The most serious cases of discrimination focus on important aspects of people's lives such as employment, credit, and insurance.[23] This year marks the 50th anniversary of the Title VII Civil Rights Act of 1964, and the United States continues to grapple with civil rights issues. Leading civil rights organizations and advocates predict that "big data" could yield further systemic inequality and discrimination. In supporting these predictions, these advocates point to "digital redlining" and profiling as ways in which "big data" could be used to exclude certain groups of people.[24]

The Internet Association condemns acts that amount to unlawful discrimination in any form. It is a testament to the success of self-regulatory efforts that issues of discrimination are not widespread among Internet companies that adhere to them. Discrimination is not limited to technology or data but is a long-standing issue that should be addressed from a broader perspective. Conducting an exploratory review of our nation's existing, federal anti-discrimination laws will reveal that these laws already apply broadly to discriminatory practices regardless of technology. The current "big data" debate raises questions regarding whether

---

[19] Thierer, *supra* note 4, at 468.
[20] Daniel Castro and Travis Korte, *A Catalog of Every "Harm" in the White House Big Data Report,* CENTER FOR DATA INNOVATION (July 15, 2014), http://www.datainnovation.org/2014/07/a-catalog-of-every-harm-in-the-white-house-big-data-report/.
[21] *Id.*
[22] *White House Big Data Report* at 51.
[23] *Id.* at 53.
[24] *Id.*

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

discrimination laws as applied to mere data collection should have ex-ante prohibitions or should continue to be applied as ex-post enforcement to uses of data. Therefore, we urge the Administration to engage in a robust examination of discriminatory practices that are not currently covered by existing anti-discrimination laws. Once these harmful practices are identified, the Administration should consider appropriate policy mechanisms that will effectively address discrimination in a technology-neutral manner. We support policy considerations that prevent discriminatory practices against people. Reviewing this landscape will better inform this debate and identify potential gaps.

Additionally, we encourage the Administration to consider how the Internet and "big data" analysis supports inclusive ends. The Internet's great success is attributable to its decentralized, bottom-up model. Its very nature is based on the inclusion (rather than exclusion) and participation of all users for its continued success and development. Companies offer services that assist cities and law enforcement in tackling major issues such as transportation and communicating with residents, respectively.[25] Additionally, startup accelerators are backing new organizations to leverage "big data" for social good.

A. The Administration should distinguish between privacy harms and discrimination harms; and, further work should be done to determine how "big data" may identify unfair and discriminatory practices to empower underserved or oppressed groups.

At the White House and Georgetown University's June 19 Big Data Workshop, Nicole Wong, OSTP's Deputy Chief Technology Officer, stated that issues in this realm of "big data" go beyond protecting information and extend to considerations about fairness and autonomy. While privacy laws are generally intended to protect people from unauthorized or unwanted intrusions, anti-discrimination laws seek to stop the use of protected characteristics to make certain determinations to their disadvantage.[26] Anti-discrimination laws are also based on notions of fairness and equality rather than on the concept of autonomy. [27] Courts and legal scholars view privacy and anti-discrimination in separate realms. For decades, federal laws such as the Civil Rights Act of 1964, the Fair Housing Act of 1968, and the Genetic Information Nondiscrimination Act of 2008 provide meaningful protections to citizens and consumers against intentional and some unintentional forms of discrimination. Therefore, we urge the Administration to distinguish in its analysis between harms that relate to privacy and harms that relate to discrimination.

---

[25] Please see Section II, Part B for detailed examples.

[26] *See* Jessica L. Roberts, *Privacy Law As Anti-discrimination Law*, UNIVERSITY OF HOUSTON LAW CENTER 1 (Feb. 7, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263583.

[27] *Id.* at 16.

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

Though almost twenty, federal anti-discrimination laws exist, the interplay of technology, "big data," and civil rights raises a number of serious considerations. It also raises questions about whether and how to handle less consequential situations arising from value-added personalization benefitting consumers. The federal government's civil rights and consumer protection agencies along with academics, subject matter experts, and other qualified parties should investigate the landscape of existing anti-discrimination laws and explore the potential for new, harmful uses to determine how best to address them. Furthermore, outside of the civil rights context, it is unclear how data may be used to identify other types of discrimination. For instance, expert groups that specialize in identifying discrimination with data should collaborate with others and transfer their knowledge to third parties, such as technology companies, to replicate the necessary best practices.

B. Preemptive legislation to address potential discriminatory harms may limit data's ability to allow for innovation that protects privacy while preventing discriminatory practices.

Data analytics can spur the development and creation of helpful services that increase (rather than decrease) safety, opportunity, affordability, and convenience. Rather than aiming to negatively impact underserved communities, Internet and technology companies often leverage data to generate new applications and services that enrich users' experiences in terms of efficiency and effectiveness. For instance, consider Street Bump, an experimental mobile application between an organization and the Boston Mayor's Office of New Urban Mechanics.[28] This app sought to use smartphones' accelerometers and GPS fees to compile data and report back to the city on road conditions, including potholes.[29] The experiment led to the team's realization that because poor and elderly people are less likely to use smartphones, the data collected would direct city services to more affluent neighborhoods.[30] Ultimately, the team rectified the situation by first deploying the app to city-road inspectors and collecting additional data to ensure an equal outcome for all residents of the city.[31]

While this is just one example of how "big data" has been leveraged to prevent unfairness and inequality among categories of people, cities, companies, and others are constantly innovating for the betterment of the disadvantaged. Consider the following examples:

- New York City's Department of Transportation has leveraged big data and the cloud to build some sophisticated but user-friendly citizen-facing mobile and web applications to benefit residents. The Department's DOTMap Portal shows alternate-side parking

[28] *White House Big Data Report* at 51.
[29] *Id.*
[30] *Id.* at 52.
[31] *Id.*

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

schedules and other relevant parking rules on a map, which residents can use for things like avoiding towing during snowstorms and special events. And, the Department has developed iRideNYC, an app that shows residents how to use multiple modes of public transportation to get to their destinations, including buses, subways, bicycles, and even walking, and live data about each option. Because of big data and the cloud, New York City has helped improve transportation for millions of its residents.

- Google Translate is a free online service that provides users with instant translations among dozens of different languages, and it helps billions of people communicate and learn 80 languages.[32] This service operates based on patterns in documents previously translated by human translators and makes predictions on the most appropriate translation. It is used to facilitate communication in critical situations, especially for victimized or underserved communities. For instance, law enforcement in Texas used Google Translate to communicate with a non-English speaking assault victim who was often struck by her husband.[33] Additionally, Oregon State Police used a Google Translate app to with a foreign-speaking man who experienced a diabetic reaction while driving on a highway.[34] From communicating online to aiding law enforcement, Google Translate helps eliminate language barriers both on and offline.

- Facebook's Compassion Research team works to help over 3.9 million people resolve disputes as part of its social resolution tools,[35] which allow people to reach out to other users or trusted friends to help resolve conflicts or open a dialog about a photo, post, or other content that bothers them. Scientists are only just beginning to understand how the unspoken rules and mechanisms of human interaction apply to attitudes and behavior online; Facebook's Compassion Research team is leading the field by using aggregated, anonymized data to optimize the language it suggests people use to initiate discussions about online content they find offensive or bothersome. Facebook also tailors communications and reporting flows to be more sensitive to the countries in which people live and the cultures they represent.

- In addition to these existing services, investors are backing startup organizations to harness "big data" for the public good.[36] Y Combinator, a seed accelerator, is currently supporting Bayes Impact, a nonprofit intended to address important social issues such as

---

[32] GOOGLE TRANSLATE, http://translate.google.com/about/intl/en_ALL/ (last visited Aug. 4, 2014).

[33] EAGLE REPORT, *Owner of Dragon One restaurant accused of assaulting wife,* Jan 8. 2014, http://www.theeagle.com/news/crime/article_02055545-6416-5728-b0b8-7469ff356200.html.

[34] Frank Mungeam, *Policy use translation app to aid diabetic driver,* Feb. 13, 2012, http://www.kgw.com/news/Police-use-translation-app-to-aid-driver-139255188.html.

[35] FACEBOOK SAFETY, *Details on Social Reporting,* https://www.facebook.com/notes/facebook-safety/details-on-social-reporting/196124227075034 (last visited Aug. 4, 2014).

[36] Jonathan Shieber, *Harnessing Big Data for Social Good, YC Backed Nonprofit Bayes Impact Launched,* TECHCRUNCH, (July 15, 2014), http://techcrunch.com/2014/07/15/harnessing-big-data-for-social-good-yc-backed-nonprofit-bayes-impact-launches/?utm_campaign=fb&ncid=fb.

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

criminal justice reform to help determine recidivism, fraud detection, and improved and cost-effective research of the potential causes of Parkinson's disease.

Going forward, we look forward to sharing with the Administration additional examples of how Internet companies' products and services are employed for inclusive ends.

III. The Internet Association believes a flexible and balanced self-regulatory responsible use framework will enhance the benefits of "big data" for society, industry, and government.

Commerce seeks guidance on whether a shift towards a responsible use framework should occur in order to address some of big data's challenges and, if so, how should this shift be reconciled with the CPBR.[37] Additionally, Commerce inquires about the practical limits of notice and consent and "respect for context."[38] Both the OSTP report and the President's Council of Advisors on Science and Technology (PCAST) report on "big data" and privacy suggest that greater emphasis should be placed on a responsible use framework.[39] More specifically, PCAST recommends that policy considerations should favor actual uses of "big data" and focus less on data collection and analysis.[40] While PCAST supports the underlying principles of the CPBR, it calls into question the operationalization of these principles, which have largely focused on collection, storage, and data retention. PCAST suggests that this approach will prove inadequate in effectively protecting privacy but stops short of debunking the CPBR in favor of another framework.

"Big data" is not a new concept. Legal scholar Chris Jay Hoofnagle explains that consumer reporting information reached "big data" status dating back to the 1960s.[41] We previously advised the Administration that wholesale changes to the United States' existing privacy framework are unnecessary as existing regulations provide a strong yet flexible

---

[37] National Telecommunications and Information Administration, Department of Commerce Request for Comments on "Big Data and Consumer Privacy in the Internet Economy," 79 Fed. Reg. 32,714, 32,716 (June 6, 2014), *available at* http://www.ntia.doc.gov/files/ntia/publications/big_data_rfc.pdf [hereinafter *NTIA Request for Comments*].

[38] *Id.* at 32,715.

[39] *White House Big Data Report* at 56.

[40] EXECUTIVE OFFICE OF THE PRESIDENT, PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 49 (2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [hereinafter *PCAST Report*].

[41] Chris Jay Hoofnagle, *How the Fair Credit Reporting Act Regulates Big Data*, *in* BIG DATA AND PRIVACY: MAKING ENDS MEET 47 (2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf.

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

framework subject to enforcement by state and federal bodies.[42] We support a conversation shift towards responsible uses of data, which should be carried out through self-regulatory mechanisms. This framework must balance privacy protections with the flexibility to innovate and better identify harms, such as discrimination.

Analysis of large datasets can lead to the discovery of new opportunities, unanticipated insights, and unexpected services that bring value to society, businesses, and governments.[43] While PCAST and other commenters believe that the CPBR still provides flexibility in a "big data" world, they acknowledge that some of these principles, namely data minimization, respect for context, and notice and consent, are strained in today's innovation economy and suggest slight modifications to the existing principles.[44] For instance, the PCAST "big data" report notes that one important concern with "respect for context" is that it mainly focuses on consumers as sources for data.[45] It is of course appropriate to enable uses of data that consumers expect – either based on the context of their experiences or specific information provided to them – but we also believe that it may be prudent to consider additional factors, such as the benefits afforded and the lack of harm to consumers. For instance, in the era of the "Internet of Things," consumers may or may not think about whether a company will use their aggregated energy data from an interconnected light bulb to research ways to improve their in-house energy consumption life or better manage the energy grid. The FTC recognized in its 2012 report that some uses beyond mere service delivery are "commonly accepted" and therefore consistent with context[46], and we encourage the Administration to consider whether other uses, such as improving environmental efficiency in the connected light example, should similarly be included.

The in-house energy consumption example also illustrates how in a "big data" context, the "respect for context" principle is undermined by the current formulation of notice and consent and data minimization. The concept of notice and consent is a foundation of the United States' privacy framework spanning over a decade. However, in this "Internet of Things" age, requiring users to continuously process privacy disclosures from varying websites, applications, devices, etc. and consent to collection of data based on a specific purpose or context will prove unworkable and bar beneficial new uses of data. Continuously seeking user consent, even if done in a "just-in-time" way will ultimately lead to "notice fatigue" - a similar concept to "privacy fatigue," which the OSTP report describes as an effect of the "barrage of privacy

[42] *The IA Comments* at 7-8.
[43] *See generally White House Big Data Report*.
[44] *See generally PCAST Report*.
[45] *Id.* at 45.
[46] *See generally FTC Report.*

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

policies … [users] must wade through to simply use a service." [47] Furthermore, data minimization imposes limitations on data collection to the extent needed for a specific goal and requires deletion of information no longer needed to reach that goal.[48] Imposing these restrictions runs counter to the idea of using data to bring about valuable, unanticipated secondary uses.

Given these challenges, we must recalibrate our thinking towards responsible uses of data for continued innovation and future growth of the Internet industry, which is driven by data analytics.

IV. As the investigation of "big data" continues, The Internet Association suggests that the Administration consider important factors – education, transparency, cost-benefit analysis, and research and development – to ensure a flexible and balanced self-regulatory framework.

As the Administration rethinks the CPBR, additional factors should be considered to ensure a flexible and balanced self-regulatory approach in a "big data" environment; therefore, we encourage the Administration to consider the following factors:

- Education: To promote practical and effective privacy protections, bottom-up solutions like education will play an important role in ensuring users understand how, when, and why their data is being used. In the course of a decade, domestic and international online safety task forces determined that education has a lasting impact and should be the primary solution to online child safety concerns.[49] The OSTP report included a recommendation to educate "robustly and responsibly" users of all ages but particularly those in grades K-12 on digital literacy.[50] The Internet Association encourages the Administration to expand efforts to integrate digital literacy in the K-12 curriculum by launching similar task forces to further investigate the role of education and empowerment-based solutions for users of all ages. As the FTC plans to investigate "big data" as a tool for inclusion or exclusion, we urge the agency to investigate the most effective methods for educating users in navigating the "big data" world.

[47] *White House Big Data Report* at 42.
[48] Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics,* 11 NW. J. TECH. & INTELL. PROP. 239, 259 (2013), *available at* http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip.
[49] Thierer, *supra* note 4, at 479- 80.
[50] *White House Big Data Report* at 64.

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

- Transparency: The concept of allowing users to know and understand information about privacy and security practices is not novel. Our industry is a strong proponent of transparency in both commercial and government contexts. One way our member companies promote transparency on their platforms is via their privacy tools. Internet companies empower users with the ability to control account, privacy, and security settings based on their preferences. Our member companies offer a variety of tools that provide users with access to information about how they interact with services and content on the platforms of their choice. For instance, many of our member companies offer privacy dashboards that allow users to see and control how their data is used. Users can determine what information they want to share online and how they want to share it, which ultimately reduces the potential for harms and builds trust between users and online platforms.

- Cost-Benefit Analysis: A commenter in the White House OSTP process noted that successful accountability approaches should take into consideration both the costs and benefits of innovative uses of data.[51] The Department of Commerce's Internet Policy Task Force supports the use of privacy impact assessments to decide whether it is appropriate to engage in innovative data uses and identify alternative methods to reduce privacy risks.[52] But, we agree with another commenter in noting that this approach fails to fully consider the benefits, which have been well documented.[53] Hoofnagle points out that "use-based regulations of big data [provide] more transparency … [but do not] create adequate accountability."[54] Privacy scholars and technical experts continue to have robust discussions about accountability mechanisms for "big data." It is argued that implementing formal review mechanisms such as internal audits to promote institutional governance will discourage misuses of data. While we agree with this underlying notion, we understand that discussions around accountability also lead to further questions about the appropriate actors and methods to implement accountability systems. Therefore, The Internet Association supports additional efforts in this area to determine the necessary criteria needed to effectively conduct cost-benefit analyses for improved data stewardship.

---

[51] THE FUTURE OF PRIVACY FORUM WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY BIG DATA COMMENTS 10 (Mar. 31, 2014), *available at* http://www.futureofprivacy.org/wp-content/uploads/OSTP-Big-Data-Review-Comments.pdf.

[52] *Id.*

[53] *Id.*

[54] Hoofnagle, *supra* note 38, at 47.

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

- Research & Development: Commerce seeks input from stakeholders on bolstering the effectiveness of de-identification.[55] The Internet Association believes it is imperative for the Administration to support additional research and development into technical measures such as privacy-enhancing tools in order to move our innovation economy forward. In particular, we urge additional research into developing effective de-identification technologies. Despite some arguments to the contrary, many technical experts and regulators continue to see significant promise in the efficacy of de-identification techniques.[56] In its 2012 report on "Protecting Consumer Privacy in an Era of Rapid Change," the FTC supported companies and researchers' efforts to continuing innovating improved methods to de-identification.[57] Both the OSTP and PCAST reports explore current governmental and commercial efforts in developing privacy-enhancing technologies. Given these differing viewpoints, we support increased, federal research and efforts in improving these tools.

The Internet Association encourages the Administration to consider the factors outlined above to reach a flexible, balanced, and self-regulatory approach that takes into account both risks and benefits of "big data." Considering these factors and permitting a self-regulatory approach towards responsible use will ensure that the United States government and its citizens continue to enjoy the many societal benefits and economic value of "big data."

V. Other jurisdictions are considering how to leverage "big data" to spur economic growth, and the Administration should continue to promote the United States' existing privacy regime and ensure interoperability with other privacy regimes.

The Internet industry appreciates the Administration's continued commitment to ensuring that U.S. businesses remain globally competitive. In our OSTP comments, we urged the Administration to support the dynamic and flexible nature of the United States' privacy regime at a time where efforts to restrict the free flow of information through data localization proposals are increasing.[58] Post-NSA revelations, our companies continue to face a challenging global business environment. In addition to maintaining the United States' current approach to commercial privacy, one such way to demonstrate the robustness of our privacy regime is to reform the Electronic Communications Privacy Act and bring it in-line with users' digital

[55] *NTIA Request for Comments* at 32,716.
[56] ANN CAVOUKIAN AND DANIEL CASTRO, BIG DATA AND INNOVATION, SETTING THE RECORD STRAIGHT: DE-IDENTIFICATION *DOES* WORK 21 (2014), *available at* http://www2.itif.org/2014-big-data-deidentification.pdf.
[57] *FTC Report* at 21.
[58] *The IA Comments* at 7-9.

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org

privacy expectations. Despite the tough conversations concerning privacy and surveillance, other jurisdictions still look to the United States as a global leader in the innovation economy, which must not be compromised.

For instance, the European Commission (Commission) recently released its official communication on moving towards a thriving data-driven economy. In this communication, the Commission recognizes that Europe's digital economy has been slow to embrace data analytics compared to the United States and "also lacks comparable industrial capability."[59] The Commission suggests that in order to better leverage data to bolster its economy, the European Union must ensure a relevant legal framework and policies such as interoperability.[60] This initiative further validates a need to reinforce interoperability mechanisms like the US-EU Safe Harbor agreement, consistent with internationally accepted data protection principles, which must remain strong for Internet businesses.

VI. Conclusion

The Internet Association is pleased to provide further input in response to Commerce's request for comments on "big data" and its impact on the CPBR. Before taking steps to legislate, we encourage the Administration to conduct a comprehensive review of the United States' privacy regime, including self-regulatory codes of conduct that the Internet industry abides by to ensure that users are protected online. We are confident that this review will reveal the effectiveness of our current framework. Though we do not support wholesale changes to the United States' privacy regime, we do support a shift towards responsible uses of data that takes a balanced, self-regulatory approach to ensure that "big data" continues to benefit the innovation economy and U.S. economy as a whole.

Respectfully Submitted,

/s/Michael Beckerman
Michael Beckerman
President & CEO
The Internet Association

[59] *Communication from the Commission to the European Parliament, the Council, the European Commission and Social Committee, and the Committee of Regions, Towards a Thriving Data-Driven Economy,* at 2, COM (2014) 442 final (Feb. 7, 2014), *available* at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6210.
[60] *Id.* at 3.

1100 H Street NW, Washington, DC 20005
www.InternetAssociation.org