31 March 2014

John Podesta, Senior Counselor to the President
Nicole Wong, Deputy Chief Technology Officer, OSTP
Big Data Study
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Ave., NW
Washington, DC, 20502

Dear John and Nicole:

The Center for Digital Democracy (CDD) respectfully submits these comments for the Administration's review. While today's "Big Data"-driven landscape may appear to be a recent development, it is really the consequence of historical trends in data processing, the growth of digital platforms, and the evolution of the commercial online marketing business model. The overall dimensions of today's pervasive data collection complex were set in the middle 1990's. The principle commercial Internet business paradigm (i.e., the collection and analysis of individuals' information so they can be tracked and targeted) has long been based on what is called "one-to-one" marketing. Over the last two decades, such "1:1" marketing has expanded from tracking an individual on a single website to the vast data collection apparatus that operates in real-time today.[1] We are closely monitored and our behaviors analyzed across devices and applications (mobile, PC, gaming); our social media actions—as well as those of our "friends"—are scrutinized; and real-time location and geographic behaviors are gathered. Few Americans know that they are connected to a digital dossier—a so-called profile—that is filled to the brim through the contributions of dozens of increasingly allied data brokers. Or that their information is used to make assessments or predictions about them—such as their "Lifetime Value" for companies engaged in financial services. Nor are they informed that their profiles are increasingly auctioned off in milliseconds to the highest bidder, so they can be targeted wherever they are—including when using their mobile devices.

[1] See, for example, Jeff Chester, *Digital Destiny: New Media and the Future of Democracy* (New York: The New Press, 2008), chapter 7; and Jeff Chester, "Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the 'Big Data' Era," in Serge Gutwirth, et al, eds., *European Data Protection: In Good Health?* (New York: Springer, 2012): 53-77.

The inability to implement basic privacy rules in the United States to address Internet data collection practices has resulted in the ubiquitous commercial surveillance landscape that today threatens the privacy of Americans—as well as those in the European Union and other countries where U.S. companies collect and transport their information.[2] The absence of a clear legislative proposal from the Administration has contributed to the growing threat to privacy that Americans confront. The online data industry sees no credible challenge from the White House that would encourage it to stem the ever-increasing tide of personalized collection. It has now been more than two years since the White House announced a "Privacy Bill of Rights," explaining that the public "cannot wait" for much-needed consumer protection safeguards. CDD urges the Administration to release with its forthcoming Big Data report a specific legislative proposal to implement these privacy rights. Americans deserve to know where the Administration stands. Does it believe that individuals have the right to control how their data are collected and used? Will the Federal Trade Commission and other agencies responsible for privacy be empowered to engage in necessary rulemakings that protect the public?[3]

---

[2] A key exception to the failure to protect online privacy from the federal government was the enactment of the Children's Online Privacy Protection Act (COPPA) in 1998. The author of this comment, along with Professor Kathryn C. Montgomery of American University, played a key role in its passage. As COPPA demonstrates, a well-crafted policy that places individuals in control over their data collection can address changes in the data collection marketplace—putting to rest the purposefully disingenuous argument that the Internet is so dynamic that regulation is impossible. See Kathryn C. Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (Cambridge, MA: 2007); and Federal Trade Commission, "FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule,"19 Dec. 2012, http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over. The failure to enact both a fundamental policy law in the U.S. and an effective set of policies for Safe Harbor has placed data flows between the U.S. and EU as risk. See, for example, Jennifer Baker, "Safe Harbor: Reding Warns US that Progress is Needed Before Summer," viEUws, 26 Mar. 2014, http://www.vieuws.eu/ict/safe-harbor-reding-warns-us-that-progress-is-needed-before-summer / (both viewed 30 Mar. 2014).

[3] The White House, "We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online," 23 Feb. 2012, http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights. The Administration's approach to a "multistakeholder" process to develop industry "codes of conduct," part of its "We Can't Wait" announcement, is an inadequate approach to ensuring consumer protection and privacy. An industry-dominated convening, in which there is also no meaningful disclosure of actual data collection practices by leading companies and trade associations, has demonstrated that it cannot develop the appropriate safeguards. For a review of the first NTIA multi-stakeholder proceeding and its failings, see Center for Digital Democracy, "New Report Exposes Flaws in NTIA 'Multistakeholder' Effort to Establish Privacy Safeguards: White House Must Act to Fulfill its Vision for a 'Privacy Bill of Rights'/See Cross-platform Tracking/Users as $ 'whales,'" 29 Aug. 2013, http://www.centerfordigitaldemocracy.org/new-report-exposes-flaws-ntia-%E2%80%9Cmultistakeholder%E2%80%9D-effort-establish-privacy-safeguards-white-house-mus (both viewed 30 Mar. 2014).

As we expressed in a meeting the White House had with several privacy NGOs several weeks ago, CDD believes the Big Data report must address the *realties* of today's commercial data gathering and analysis landscape. While we acknowledge the many positive uses of Big Data, and its potential, the Administration should not gloss over the threats as well.[4] We fear that missing for the most part in the White House's review will be a fact-based assessment of actual commercial data practices conducted by Google, Facebook, Yahoo, data brokers, and many others. Such a review would reveal an out-of-control commercial data collection apparatus, with no restraints, and which is leading to a commercial surveillance complex that should be antithetical in a democratic society. The report should show the consequences of such information gathering on Americans, where the data can be immediately made "actionable." It should address the consequences when predictive analysis and other "insight" identification applications trigger real-time and future decisions about the products and services we are offered, the content we may receive, and even the online "experiences" with which we interact. The report should make clear how its Consumer Privacy Bill of Rights Principles should be interpreted when data collected from Americans are used to unfairly target them—and their families—for products and services that can be harmful to their well-being (such as the delivery of high-interest payday loans, promotion of questionable medical treatments, and the targeting of junk food ads to children, which contributes to the nation's obesity epidemic).[5]

CDD respectfully urges the White House to address in its report the following issues as raising privacy and consumer protection concerns, and requiring action by policymakers. For brevity, we will only briefly describe each issue and provide a few examples.[6]

- *The Growth of Ubiquitous Cross-Platform and Across-Application Tracking of Individuals Online:* Today, consumers are increasingly tracked across the devices they use, such as PC, mobile, gaming, and soon even TV. Companies are also expanding beyond cookies to create single identifiers on a person. The same person confronts a data collection environment that also captures their behavior and actions on social media, mobile apps, websites and more. As one online marketing publication recently explained about the implications of device identification, "Never before has digital tracking become so personal and never before has the argument for

[4] We note, however, that much of the commentary on the potential of Big Data is often akin to public relations. Recent critical analysis of the failure of Google's Flu Trends data to provide meaningful results is one example. Declan Butler, "When Google Got Flu Wrong," *Nature*, 13 Feb. 2013, http://www.nature.com/news/when-google-got-flu-wrong-1.12413 (viewed 30 Mar. 2014).

[5] In addition to CDD, there are other experts specializing in addressing the impact of today's commercial data apparatus on the public. See, for example, Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (New Haven, CT: Yale University Press, 2012).

[6] However, CDD follows this field very closely and is happy to provide further analysis and documentation of the problems we describe.

consumer privacy controls been so compelling."[7] Such all-encompassing data-gathering practices are at odds with long-standing Fair Information Privacy Practices requiring data minimization, as well as the Administration's "Focused Collection" rights principle.[8]

- *The Emergence of Big-Data-derived Comprehensive Data Profiles on Individuals (Data Management Platforms)*: Evolving from the one-to-one marketing paradigm described earlier, companies are focused on collecting and making actionable as much of a person's information as possible. The data broker company Merkle has called this process "Connected Recognition"; others describe similar "360 degree," "Master" profiles, and "multi-channel" approaches. Few consumers know that all their information is increasingly stored in one central repository such as a data management platform (DMP)—that can include their financial data, social media usage, location, demographics, ethnicity, and much more. These data profiles can be connected to "Experience Managers" and other applications used by marketers and others to make determinations—and take action—concerning the products and services to offer an individual. The continuous gathering and use of a person's information should be challenged as posing a fundamental threat to privacy in America today. The unfettered growth of commercial data profiles is at odds with many of the Administration's

---

[7] Gavin Dunaway, "ID Is Key: Unlocking Mobile Tracking & Cross-Device Measurement, Part I," AdMonsters, 2 Aug. 2013, http://www.admonsters.com/blog/id-key-unlocking-mobile-tracking-cross-device-measurement-part-I; Gavin Dunaway, "ID Is Key: Unlocking Mobile Tracking & Cross-Device Measurement, Part 2," AdMonsters, 3 Aug. 2013, http://www.admonsters.com/blog/id-key-unlocking-mobile-tracking-cross-device-measurement-part-2 (both viewed 5 Feb. 2014).

[8] See, for example, Google, "The New Multi-Screen World Study," Think Insights, Aug. 2012, http://www.thinkwithgoogle.com/research-studies/the-new-multi-screen-world-study.html. See also Google, "The Customer Journey to Online Purchase," Think Insights, http://www.thinkwithgoogle.com/tools/customer-journey-to-online-purchase.html (both viewed 5 Feb. 2014); Steve Schuler, "How to Reach Consumers Across Devices with Sequential Messages," Yahoo Advertising, 16 Sept. 2013, http://hispanicad.com/agency/digital/how-reach-consumers-across-devices-sequential-messages; "Marketing for Cross-screen Sequencing," ANA Magazine, Issue 8, 2012, p. 7, http://www.ana-thoughtleadership.net/ana-thoughtleadership/2013_issue_8#pg7 (both viewed 5 Feb. 2014); Nielsen, "Unleashing Cross-Platform: The Tip of the Spear," 13 Nov. 2013, http://www.nielsen.com/us/en/newswire/2013/unleashing-cross-platform-the-tip-of-the-spear.html. See also Becky Chappell, "Making Mobile Work Across the Advertising Industry," DoubleClick Advertiser Blog, 1 Nov. 2013, http://doubleclickadvertisers.blogspot.com/2013/11/making-mobile-work-across-advertising.html. "What The Google AdID Means For Ad Tech," Ad Exchanger, 19 Sept. 2013, http://www.adexchanger.com/data-driven-thinking/what-the-google-adid-means-for-ad-tech/. For examples from Facebook, examine the relationship between what a consumer does outside of the social network who can then be targeted while there. See, for example, "Datalogix Announces Facebook Partner Categories for CPG, Retail and Automotive Brands," Datalogix, Apr. 2013, http://www.datalogix.com/2013/04/datalogix-announces-facebook-partner-categories-for-cpg-retail-and-automotive-brands/ (all viewed 30 Mar. 2014).

Privacy Principles, including Transparency, Individual Control, Focused Collection, and Accountability.[9]

- *The Digital Data Collection Apparatus, Including the Use of Multiple Data Sources and the Real-time Buying and Selling of American Internet Users:* Americans do not know—nor can they effectively control—the myriad of data that is collected and used on them. Data brokers and other similar providers increasingly work together to pool and sell their information on a single person or to create a highly refined segment. This information is made available for sale, and is combined with the data resources on individuals that e-commerce and Internet marketing companies routinely capture. Our data profiles feed a far-ranging automated system of online auctions on individual Americans—a dehumanizing process in which we are sold to the highest bidder through ad exchanges, regardless of whether we are online or using a mobile device (and soon even in front of a TV). Without our awareness or consent, our information (including behaviors, ethnicity, race, financial interests, etc.) is treated as a mere commodity for sale. Both the role of data broker alliances and the use of super-fast computers to track and sell Americans raise concerns related to a number of the Administration's Privacy Rights, including Transparency, Individual Control, Respect for Context, Focused Collection, and Accountability.[10]

---

[9] Security is also implicated, of course, as the recent explosion of major data breaches illustrates. Nor is there any meaningful access or methods to ensure accuracy. For background on the growth and use of these comprehensive Big Data dossiers on Americans, see, for example: Merkle, "Connected Recognition: Enabling a 360° View of the Customer," http://www.merkleinc.com/what-we-do/database-marketing-services/connected-recognition; Acxiom, "Macy's Focuses on the Customer; Builds Comprehensive View Across Touch Points," http://acxiom.com/macys-builds-comprehensive-view-customer/; Susan Bidel, "Boosting First-Party Data Effectiveness With DMPs," Forrester, 10 Jan. 2014, http://www.forrester.com/Boosting+FirstParty+Data+Effectiveness+With+DMPs/fulltext/-/E-RES108301; Acxiom, "Multichannel Marketing Solutions," http://www.acxiomdigital.com/services/multichannel-marketing.asp; eMarketer, "To Handle Big Data, Advertisers Turn to DMPs," 24 May 2013, http://www.emarketer.com/Article/Handle-Big-Data-Advertisers-Turn-DMPs/1009919; "Adobe Digital Marketing Summit Hits on Key Theme of Marketing Reinvention," 25 Mar. 2012, http://www.businesswire.com/news/home/20140324006499/en/Adobe-Digital-Marketing-Summit-Hits-Key-Theme#.UzgzI8dGJnY. See also Adobe's new "Master Marketing Profile" application that is integrated into its marketing cloud service. Adobe, "Profile Management," http://www.adobe.com/solutions/digital-marketing/profile-management.html (all viewed 30 Mar. 2014).

[10] Kevin Weil, "Driving Mobile Advertising Forward: Welcoming MoPub to the Flock," Twitter Blog, 9 Sept. 2013, https://blog.twitter.com/2013/driving-mobile-advertising-forward-welcoming-mopub-to-the-flock; Nexage, "Nexage Reaches Major Milestone with More than 50 Percent of Spend Now through RTB," 17 July 2013, http://www.nexage.com/resources/press-releases/nexage-more-than-50-percent-of-spend-now-through-real-time-bidding; Kelly Liyakasa, "Ads Across Amazon: O&O Sites Vary in RTB and Data Readiness," Ad Exchanger, 5 Dec. 2013, http://www.adexchanger.com/ecommerce-2/sizing-amazons-scope-the-owned-and-operated-opportunity/; DoubleClick, "Solutions for Publishers: Sell Across All Screens," http://www.google.com/doubleclick/publishers/solutions/mobile.html (all viewed 4 Feb. 2014);

- *The Growth of Commercial Digital Surveillance at the Community, Hyper-local Level:* Geo-location data are increasingly being gathered and made actionable, with capabilities permitting real-time responses to events and individual behaviors. The rapid adoption of mobile devices and mobile data-driven marketing practices enables companies both to collect data and to reach individual consumers at any time. Mobile analytics identify, track, measure, and help make actionable a wide array of user behaviors (including those that can be used to identify the spending behavior of individuals).

  Intrusive data collection practices increasingly monitor and assess the individuals, businesses, and institutions residing in a discrete "micro-neighborhood." For example, online data marketers have further sub-divided the country into so-called "tiles," which are used to identify unique characteristics of a community. The use of these "tiles" raises serious privacy and consumer concerns. As one hyper-local targeting company explained, "What we do is map data from multiple sources onto a grid of tiles that cover every square foot of the US. Each tile is 100 meters by 100 meters, and we inject third-party demographic information about that area into the tile, as well as data on what's physically located there—points of interest like parks and airports, tourist attractions, retailers, stadiums, and so forth. Then, we connect that data with where a mobile device is in real time, or where it has recently been, to build unique audience segments for brands to target."[11] The information derived from these "tiles" can help generate a "score" on an individual—or a neighborhood—that becomes part of a data profile and a decision point about their value (or lack thereof). Americans should not have to trade away their privacy—let alone make themselves or their neighbors vulnerable to ongoing and invisible scrutiny—in order to discover a gas station or drug store using an online map. The growth of commercial surveillance at the local level raises the specter of new forms of discrimination or unfair practices (and the continuation of historic practices related to redlining, for example). As

---

Natasha Singer, "Your Online Attention, Bought in an Instant," *New York Times*, 17 Nov. 2012, http://www.nytimes.com/2012/11/18/technology/your-online-attention-bought-in-an-instant-by-advertisers.html?pagewanted=all&_r=0. Programmatic buying is being applied to TV, which will eventually have similar data tracking and targeting capabilities now seen online. See, for example, AudienceXpress, "The Platform," http://www.audiencexpress.com/the-platform/. For an example of data partnerships and data coops, see Turn, "The Turn Partner Ecosystem," http://www.turn.com/en-gb/data-partners; Brilig, "Coop Members," http://www.brilig.com/coop-members.php (all viewed 30 Mar. 2014).

[10] Jeremy Lizt, "Data Onboarding System Overview," LiveBlog, 3 Oct. 2012, http://blog.liveramp.com/2012/10/03/data-onboarding-system-overview/; Fahim Zaman, "New LiveRamp Connect Allows Brands to Integrate Data into 70+ Marketing Platforms," LiveBlog, 21 Jan. 2014, http://blog.liveramp.com/2014/01/21/new-liveramp-connect-allows-brands-to-integrate-data-into-70-marketing-platforms/; Datalogix, "DLX OnRamp," http://www.datalogix.com/dlx-onramp; Michel Benjamin, "1st, 2nd, 3rd Party Data: What Does it All Mean?" Lotame, http://lotame.com/1st-2nd-3rd-party-data-what-does-it-all-mean (all viewed 30 Mar. 2014).

[11] Placed, "Placed Targeting," https://www.placed.com/targeting (viewed 5 Feb. 2014).

mobile payment data becomes increasingly merged with geo-location and other data, communities will confront an even more formidable system that can either help or harm their future. Mobile and hyper-local data practices raise each of the Administration's Privacy Rights principles.[12]

- *The Delivery of Financial, Health, and Other Products Linked to Sensitive Data and Uses that Raise Consumer Protection Concerns*: If all the data collected on an individual today were merely being stored, that alone would be a major privacy concern. But such data are analyzed and used to make decisions about us—including for the targeting of products and services tied to our livelihoods, well being, and families. Financial services companies, for example, are using data analytics and generating insights from our information to determine the products and services we are offered in the marketplace. The growing role of so-called "e-scores" can determine—invisibly and without accountability—our "lifetime value" and credit worthiness. CDD filed in this proceeding late last week, along with the U.S. PIRG Education Fund, a new report on Big Data and financial products and services that explores this issue in depth. CDD and a coalition of consumer, public health, and child advocacy groups are also filing today with OSTP a call for new safeguards related to Big Data and the obesity crisis linked to food and beverage marketing to youth online. The White House report should call for the strongest set of Consumer Privacy Bill of Rights safeguards covering sensitive information and their applications, especially when connected to a product or service that involves finance, health, race/ethnicity, young people and seniors.[13]

---

[12] Jesse Haines and Abigail Posner, "The Meaning of Mobile," Think with Google, Oct. 2012, http://ssl.gstatic.com/think/docs/the-meaning-of-mobile_research-studies.pdf; Verizon, "Unprecedented Insights, in Your Neighborhood," http://business.verizonwireless.com/content/dam/b2b/precision/Precision_Phoenix_Market_Infographic.pdf; "Measurement for Mobile App Ads," Facebook Developers, https://developers.facebook.com/docs/ads-for-apps/measurement/; eMarketer, "How to Use Location Data to Target Unique Mobile Audiences," personal copy; Stephen Milton and Duncan McCall, "Apparatus and Method for Profiling Users," United States Patent 8,489,596, 16 July 2013, http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8489596.PN.&OS=PN/8489596&RS=PN/8489596 (all viewed 4 Feb. 2014).

[13] Center for Digital Democracy, "Report Examines Both the Promise and the Potential Dangers of the New Financial Marketplace: Leading Reform Groups Call for New Regulations to Protect Consumers from Unfair and Discriminatory 'Big Data' Practices," 27 Mar. 2014, http://www.democraticmedia.org/report-examines-both-promise-and-potential-dangers-new-financial-marketplace-leading-reform-groups-c; Center for Digital Democracy, "Protecting Consumer Privacy and Welfare in the Era of 'E-Scores,' Real-time Big-Data 'Lead-Generation' Practices and other Scoring/Profile Applications [USPIRG/CDD FTC Filing]," 18 Mar. 2014, http://www.democraticmedia.org/protecting-consumer-privacy-and-welfare-era-%E2%80%9Ce-scores%E2%80%9D-real-time-big-data-%E2%80%9Clead-generation%E2%80%9D-practice; Federal Trade Commission, "#516: Request for Comments and Announcement of FTC Workshop on Spring Privacy Series," http://www.ftc.gov/policy/public-comments/initiative-516 (all viewed 30 Mar. 2014).

- *The Failure of Industry Self-regulation and the Limits of the Multi-stakeholder Process*: Finally, CDD urges the White House to look closely at the role and realities of so-called privacy self-regulation. As this comment illustrates, the growth of cross-platform and data broker-enhanced collected information on individuals continues—but without any corresponding ways to protect privacy. While online marketers, for example, declare that they are engaged in "anonymous" data gathering, even a cursory examination of their practices reveals disturbing expansion in the use of our personal data. Data companies, including Google and Facebook, publicly declare that they care about privacy—but actually engage in activities that constantly undermine our ability to make meaningful personal decisions about how and whether our information can be used. Scholarly research has demonstrated the inadequacies of the nearly invisible "icon" that is the most visible component of the marketing industry's self-regulatory program. News reports have revealed industry opposition to modest calls that would create a "Do-Not-Track" system. Industry lobbyists fight any regulatory proposal that would empower citizen and consumer choices for privacy. Self-regulation is designed to give the *appearance* of protecting privacy without actually doing anything to stem the powerful data collection tide. Technological solutions offer no magic digital bullet, either, although they can play a role. When the default is collection and use, which is how the online medium has been purposefully structured, it's not practical for consumers to try to "turn off" the data machine. There have to be regulatory rules that limit the collection of data and empower individuals to make their own privacy decisions.

The Department of Commerce's "multi-stakeholder" process, convened by the NTIA, isn't capable of developing a meaningful solution, either. It has failed to address how the contemporary data collection apparatus *actually works*, which is essential if one is to identify a framework that can better protect Americans. Beyond its unwillingness to focus on the integrated data environment that consumers confront, the NTIA hasn't demonstrated an interest ensuring a robust analysis of the two issues it has tried to address so far. Industry lobbyists also vastly outnumber consumer and privacy groups, and the process is rife with conflicts of interest. Leading companies refuse to discuss their actual practices or plans—even when connected to the issue being discussed. The belief by some in the Administration that the Internet is too dynamic to regulate is misplaced. So too is the focus on permitting so-called stakeholders to help set the rules of the data collection road. Such a process is akin to allowing lobbyists to draft legislation for their own industries. An examination of the role of stakeholders in addressing how to protect privacy will reveal their inability to rise above their own corporate imperatives in order to support pro-consumer policies. Rather than focusing on corporate "codes of conduct," the Administration should make it clear how it would like Congress to interpret its Privacy Bill of Rights.[14]

---

[14] Brad Stenger, "CHI 2012 Conference Q&A With Lorrie Cranor and Pedro Leon," *New York Times*, 17 July 2012, http://open.blogs.nytimes.com/2012/07/17/chi-2012-conference-qa-with-lorrie-cranor-and-pedro-leon/?_php=true&_type=blogs&_r=0; Kate Kaye, "Study: Consumers

Americans should not have to trade away their privacy or consumer protections in order to participate in the commercial arena—or in the marketplace of ideas in the Internet era. The Big Data report from the Obama Administration will be one of its key legacies—and historians and others will look back to see how willing the President and his advisors were to be candid with the American public and urge for the privacy safeguards and practices they deserve. Americans should no longer have to wait.

Respectfully submitted,

Jeff Chester
Executive Director
Center for Digital Democracy

Don't Know What AdChoices Privacy Icon Is," *Ad Age*, 29 Jan. 2014, http://adage.com/article/privacy-and-regulation/study-consumers-adchoices-privacy-icon/291374/; http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html; Natasha Singer, "Do Not Track? Advertisers Say 'Don't Tread on Us,'" *New York Times*, 13 Oct. 2012, http://www.centerfordigitaldemocracy.org/new-report-exposes-flaws-ntia-%E2%80%9Cmultistakeholder%E2%80%9D-effort-establish-privacy-safeguards-white-house-mus (all viewed 30 Mar. 2014).