Responses to Post-Hearing Questions for the Record from
Chairman Rockefeller, Senators Boxer, Klobachar, Lautenberg and Schatz

Senate Committee on Commerce, Science, and Transportation
“A Status Update on the Development of Voluntary Do-Not-Track Standards”
April 24, 2013

Submitted by Mr. Harvey Anderson,
Senior Vice President for Mozilla
May 31, 2013 (Updated June 5, 2013)

Post-Hearing Questions for the Record from Chairman John D. Rockefeller IV

Chairman Rockefeller Question #1:
Do you believe that the DAA’s self-regulatory program and choice mechanism, in their current form, are sufficient for consumers? Why or why not?

Mozilla Response to Chairman Rockefeller Question #1:
No, we do not believe the DAA’s program in its current form is sufficient for consumers. As we outlined in our written testimony, the efficacy of the Digital Advertising Alliance (DAA) Ad Choices program remains an open question. Last year, according to one study, the number of users who viewed the icon was low: 0.0035% of users clicked on the icon, and only 1 in 20 of those actually opted out. The DAA itself reported that more than a trillion ads per month include the Ad Choices icon – a blue triangular icon that when clicked, takes consumers to a page where they can learn about the ad, and opt out of receiving it. Only five million users have accessed the choice tool, and reportedly a total of two million of those have opted out of all interest-based advertising since the program began. Over a three-month period this equates to an effective rate less than .0000006%.

This low opt-out rate seems inconsistent with the 11 percent of Firefox users who have turned on Do Not Track without prompting or any conspicuous visual clues in the Firefox user interface (see https://dnt-dashboard.mozilla.org/). The argument that the current low participation rate means that consumers are “OK” with the current tracking and collection practices is contradicted by the ample survey research indicating otherwise.

The user experience for the opt-out and the user education could be substantially improved. The icon could be more visible, contain less text, and require fewer clicks – it could be more user-friendly. Still, even though we believe improvement is warranted, we recognize that the DAA scheme represents significant effort, coordination, and investment that overtime can improve through iteration and feedback.

Chairman Rockefeller Question No. 2:
Can the DAA's existing self-regulatory scheme be narrowed or changed in some way as to place reasonable, meaningful limits on the collection of consumer's information? How?

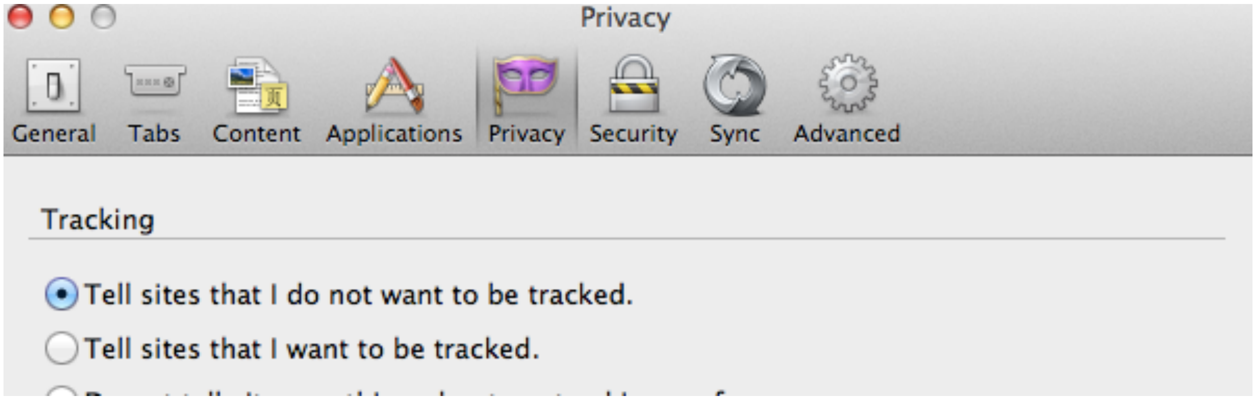
Mozilla Response to Chairman Rockefeller Question No. 2:
Mozilla only has access to the information that is publicly available concerning the DAA's program and, beyond our comments above, we do not have sufficient information to provide a detailed response to this question.

Post-Hearing Questions for the Record from Senator Barbara Boxer:

Senator Boxer Question No. 1:
How do Firefox users find out about the Do Not Track feature?

Mozilla Response to Senator Boxer Question No. 1:
Currently, we believe most Firefox users find out about the Do Not Track feature by exploring the Firefox preferences. Users may also learn about the feature through popular media, which has widely covered development of the feature, and from consumer advocacy groups. We have also provided users with some information about Do Not Track through our own blogs, marketing materials and support pages.

To enable Do Not Track in Firefox, a user must first select "Preferences" in the menu options, and then select the "Privacy" menu shown below to enable Do Not Track.



Tracking

● Tell sites that I do not want to be tracked.
○ Tell sites that I want to be tracked.

We do not promote the feature in the product or provide the user with visual prompts in the main user interface. This is primarily because Do Not Track is still under development and we need widespread industry adoption of the system and the signals for it to provide meaningful choice and control to users.

Senator Boxer Question No. 2:
To what do you attribute the growth in the number of Firefox users who have turned enabled Do Not Track?

Mozilla Response to Senator Boxer Question No. 2:
We attribute the growth in the number of Firefox users who have enabled Do Not Track to a broad user sentiment that they want more control in their digital transactions. There are very few easy options available, and users perceive they are tracked across their web browsing activities and don't understand how/whether they receive benefits or direct value from this tracking. Those users who don't want this to occur or don't understand what's happening with their data set their browsers to tell sites "not to track" them. We expect that adoption will stabilize over time and we don't necessarily believe the growth rates will organically continue if adoption remains consistent with historical patterns. We also believe that the adoption rate may be affected by how well industry recipients respect Do Not Track signals.

Senator Boxer Question No. 3:
Why did Mozilla make the decision to block third-party cookies by default?

Mozilla Response to Senator Boxer Question No. 3:
We continue to evaluate the "third party cookie patch" that is currently available in the Aurora build (a special testing build used by a small number of users) for Firefox. This patch would create a default setting that blocks third party cookies. Our primary motivation for considering the patch is to make enhancements to cookie policies that will help to create the Web experience users expect. The current feature set matches Apple Safari's third party cookie policy. We are still gathering feedback on the current proposal and iterating on other ideas and potential modifications. The new default cookie policy will remain in our test builds of Firefox until evaluation and development is complete.

Senator Boxer Question No. 4:
How do the expectations of Firefox users differ with respect to first-party and third-party cookies?

Mozilla Response to Senator Boxer Question No. 4:
We believe that Firefox users are more likely to expect tracking and collection from parties with whom they have intentionally engaged. This is because users have a better understanding of the value proposition and the benefits to them. This is often called a first-party. For example, when you log into

Amazon, users expect the service to remember your name, past history, and to offer experiences based on information they have collected about you through your interactions with the service. Conversely, users don't generally expect that parties with whom they do not have a relationship to collect or track information about them. The converse is also not necessarily true, all first parties are not necessarily "good" and all third parties are not necessarily "bad" or surprising to users. For example, some websites engage third parties by contract restricting their collection and tracking practices, others use third parties for analytics in ways that would be perfectly acceptable to users, and even other third parties operate and comply with the laws of the relevant jurisdictions with strict regulatory prohibitions on profiling without user consent.

Senator Boxer Question No. 5:
How does blocking third-party cookies change a user's browsing experience?

Mozilla Response to Senator Boxer Question No. 5:
Through our testing we continue to learn more about what happens when third party cookies are blocked, but we our review process is still ongoing. For the most part, blocking third party cookies will have little overall impact to a user's browsing experience. Users will still be able to consume content from those websites that have enabled third party cookies even though those cookies cannot be read – ads will continue to be displayed, but the user may not be shown targeted ads based on cookie data. It's also possible that a site may prevent a user from accessing some content or services without enabling the use of third party cookies for that site. It is worth pointing out that in mobile web browsing, fewer sites and apps rely on third party cookies, so disabling third party cookies by a mobile OS provider has even less impact on a user's browsing experience.

Senator Boxer Question No. 6:
How have users, advertisers, and other stakeholders responded to Mozilla's announcement regarding its new third-party cookie policy?

Mozilla Response to Senator Boxer Question No. 6:
The response to the proposal has differed widely depending on the respondent's role in the digital ecosystem. Users have largely been silent (maybe because the change and impact is not well understood outside of the ecosystem), yet comments posted to various social sites and media outlets demonstrate strong support coming from some segments of our user base. Publishers have expressed concerns about frequency capping and conversion management, functionality offered by cookies. Ad tech entities that don't have a direct relationship with the user or who provide re-targeting services have articulated concern that this may directly impact their current businesses. Some stakeholders in the ad tech industry have expressed concern that the proposed change gives first parties an unfair advantage that may make

their inventory more valuable over time. The brands have not articulated specific concerns, but generally tell us they don't want to be associated with non-transparent practices and are concerned about the extent to which third parties are tracking users outside their stated privacy policies. Consumer groups have been very supportive of the proposed change because it increases transparency and user control, reduces emergence of data inequalities, and the sale of secondary purposes outside of the user's control and benefit.

There also seems to be a general sentiment among stakeholders that the current practices of using cookies for collection and tracking are not long lived and new technological approaches are on the horizon. Thus, while stakeholders we've met with know change is inevitable with regard to cookies, there is inherent resistance until a better alternative is available.

Senator Boxer Question No. 7:
Do you anticipate other browser companies following suit in blocking third-party cookies by default?

Mozilla Response to Senator Boxer Question No. 7:
Apple's Safari browser already has implemented a third party cookie policy that blocks most third party cookies by default, including on its iOS platform devices like iPhones and iPads. We are unable to predict what Google and Microsoft will do relative to third party cookies.

Senator Boxer Question No. 8:
How prevalent is the use of digital fingerprinting and other non-cookie tracking among web sites encountered by Firefox users?

Mozilla Response to Senator Boxer Question No. 8:
We know various forms of digital fingerprinting are in practice today, however, we do not have sufficient information to quantify the extent of the current practices.

Senator Boxer Question No. 9:
What does Mozilla do to address the use of these alternative tracking methods?

Mozilla Response to Senator Boxer Question No. 9:
Our primary proposal to address all forms of tracking has been our work on Do Not Track. We still believe a simple, user-enabled Do Not Track signal is the best method for providing users and sites a simple, persistent, automated and effective signal to opt-out of tracking regardless of whether a site or app is using cookies, unique IDs, fingerprinting or other tracking methods. We also are continuing to work to minimize the Firefox user agent string fingerprint where possible.

Senator Boxer Question No. 10:

What role do alternative tracking methods play in the ongoing World Wide Web Consortium discussions regarding a Do Not Track standard?

Mozilla Response to Senator Boxer Question No. 10:

To date, the scope of the W3C discussions have been focused on a Do Not Track signal that would be technology-agnostic on the form of tracking method being deployed by a third party. Barring some change in the coming weeks, the W3C specification would apply to any type of third party tracking.

Post-Hearing Questions for the Record from Senator Frank R. Lautenberg:

Senator Lautenberg Question No. 1:

A 2010 *Wall Street Journal* series on online privacy illustrated the extent to which individuals are being tracked and how the invasive practice can cause real harm. A recent high-school graduate, who had been identified by advertisers as concerned about her weight, told the paper she sees weight-loss ads every time she goes on the Internet. She said, “I’m self-conscious about my weight. I try not to think about it…then [the ads] make me start thinking about it.” Do you believe this qualifies as a real harm?

Mozilla Response to Senator Lautenberg Question No. 1:

We cannot judge how the ad placements may have impacted the individual interviewed in the *WSJ* series. Traditionally, legal harm that results in remedies and legislative action requires a cognizable and quantifiable loss or injury. The *WSJ* series demonstrates the real need for education, transparency and greater trust in advertising data practices.

Senator Lautenberg Question No. 2:

Many believe the lack of transparency—particularly with regard to 3rd party cookies—and an individual’s inability to know what personal information is actually being collected can cause real harm because consumers don’t have the ability to understand how to protect themselves from invasive tracking. Do you agree that this is a harm?

Mozilla Response to Senator Lautenberg Question No. 2:

Harms in this case are difficult to quantify in a traditional sense because the real harm is a lost opportunity to accelerate commerce and more meaningful digital transactions. As stated in our written testimony before this Committee, we believe that more education, greater transparency and direct control around these advertising practices creates trust and demonstrates value to the user which would ultimately create a better, stronger ecosystem:

“If users do not understand what happens to their data, how it is used, or the trade-offs, they will inevitably seek more protective blocking options. Conversely, we may see the adoption of more invasive and even less transparent tracking methods. The impact is that efforts to protect the status quo further erode people’s trust in the ecosystem, thereby compromising future expansion of commerce and innovative growth of this ecosystem. Personalized content is good, however, the collective challenge we face is how to deliver that content transparently.

The future of a viable, innovative Web that continues to contribute jobs and drive social, educational and economic activity depends on consumer trust. To develop this trust, transparency, choice and control are essential. Real transparency of business and data sharing practices combined with meaningful user choice will engender the confidence users expect.”

Senator Lautenberg Question No. 3:
Do you believe that consumers have a basic right to privacy online?

Mozilla Response to Senator Lautenberg Question No. 3:
Certainly some states like California, and many countries around the world, have provided constitutional protections for privacy. To the extent these rights extend to digital environments, we act consistently with the applicable law. We also believe users have a right to make choices – that don’t punish them – about their information, habits, relationships, interests, activities, and preferences. This value is reflected in our product design in ways that users efficiently and easily navigate the web.

Post-Hearing Questions for the Record from Senator Amy Klobachar:

Senator Klobachar Question No. 1:
It now appears that Mozilla, Apple, and Microsoft are competing on consumer privacy. Both the FTC and White House reports on privacy released last year mention the possibility of privacy practices, including online tracking options, becoming a consideration for consumers deciding between devices and services.

Have you seen data suggesting consumers already chose services, particularly online, based on privacy practices? Is this impacting the competition between browsers and services?

Mozilla Response to Senator Klobachar Question No. 1:

Privacy practices by the major browser providers are emerging as a major factor but do not appear to be the driving factor in product selection. In most markets, privacy is important as a feature area for browsers, but our research indicates that it still ranks behind other factors like performance, stability and security.

Part of the challenge for browsers is that privacy is not a mature area of feature development. Most of the privacy tools and settings available in browsers are still in early phases of development and generally are not used by the mainstream user. If more browser technology existed that was privacy forward, intuitive, and added value to a user's online experience, more users would seek it out and avail themselves of it.

Post-Hearing Questions for the Record from Senator Brian Schatz:

Senator Schatz Question No. 1:

I agree with the point that you made in your testimony that it is important to protect the trust of consumers. I am concerned that, right now, consumers lack even the most basic tools to understand, let alone trust, the information collecting activities of advertisers on the websites they visit.

When a consumer is browsing on the internet, is there any way for that consumer to know on any given website (1) who is collecting information about that person, (2) for what purpose that data is being used, and (3) who else might have access to that data?

Mozilla Response to Senator Schatz Question No. 1:

For over a decade, the primary basis for consumers to learn about any given site’s data handling practices has been its posted privacy policy. Numerous studies have been done over the years showing that the vast majority of top commercial web sites have privacy policies (see TRUSTe Privacy Index 2011; http://tctechcrunch2011.files.wordpress.com/2011/11/truste-privacy-index-2011-websites.pdf). Some state governments, such as California, have legislated that websites are required to post a policy that covers the three points you outlined in your question. The Federal Trade Commission has also brought a number of deceptive/unfair practice actions against sites that have wavered from stated data practices.

While there is research showing that consumers don’t regularly read or make sense of these policies, privacy policies are noteworthy sign posts used to provide information about sites’ data practices (see “The Cost of Reading Privacy Policies,” A. McDonald & L. Faith Cranor, *I/S: A Journal Of Law And Policy*

For The Information Society, 2012; http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf).

As it relates to third party tracking, the current paradigm of relying on posted privacy policies creates challenges as it becomes more difficult to describe in detail within these policies how consumer web sites employ third party services, widgets and advertising. Moreover, because of the need for more transparency about the current practices in the digital ad tech sector, consumer expectations of what is occurring on these web sites are not being matched.

One of our stated objectives in developing a Do Not Track specification is to help evolve the notice and choice model to one where a user states his/her preference and the website is able to communicate back its relevant tracking practices all without the consumer needing to read the privacy policy.

Updated June 5, 2013:

Post-Hearing Questions for the Record from Senator Ron Johnson:

Senator Johnson Question No. 1:
What are the harms that are actually occurring to consumers through anonymous cookie-based “tracking?” As indicated in Mr. Mastria's testimony, the primary privacy concerns for most consumers online have to do with identity theft, viruses and malware, and government surveillance. So, what harms are occurring that the FTC doesn't currently already have the authority to address?

Mozilla Response to Senator Johnson Question No. 1:
The question of harms associated with online tracking is a complicated one to answer, as we stated above in our responses to Senator Lautenberg. We need to look beyond legal distinctions or classes of harms to look at the erosion of trust in the ecosystem resulting from non-transparent tracking of consumers online. Mr. Mastria’s testimony points to some of the privacy concerns of consumers today. However, we know consumers care about intrusions into their private lives, not just from hackers or governmental entities, but also from commercial entities.

To consumers, many types of personal information can be important to them, including elements that are uniquely identifiable or not, including de-identified data, that might be characterized as “anonymous” meaning not including a person’s name or SSN, for example.

Meaningful distinctions between personally identifiable information (PII) and non-PII are breaking down.

To a certain extent, much of the data collected from or about a consumer online could be reasonably considered “personal” by that person. In the context of cookies, calling data associated with a cookie “anonymous” because it doesn’t include a person’s name, home address or other PII doesn’t mean that there aren’t privacy considerations. Whether data is uniquely identifiable or becomes subsequently identifiable in combination with other data, or whether future, novel uses of that data create new contexts with privacy properties, people can have legitimate interests in wanting to understand and have a say in a company’s data handling practices. For example, a database generated by a third party company in the ad ecosystem that is able to associate a consumer’s online browsing history down to a specific product, interest or purchasing intent and then for that data to cross multiple companies’ systems to use that data across the web to personalize display ads, content or recommendations can feel personal to that user despite not including any PII.

On a technical level, there are many, real world examples of so-called anonymous data being later re-identified. In 2006, AOL released a large data set for research purposes of 650,000 users’ search queries that it anonymized before posting online. Using a phone book listing, the *New York Times* was able to identify individuals from the data. Since then, a number of researchers have demonstrated that by combining datasets from public sources with anonymized datasets, it is possible to re-identify actual individuals sometimes to dramatic effect in some cases where the once-anonymized dataset includes financial or health related data.

We shouldn’t accept comments made by those trying to minimize concerns associated with anonymized datasets about users’ online activities, purchases, communications and relationships because the business interest is only to personalize a display advertisement today. We have to think more broadly about the future of this data once its collected, whether it might be compromised by a hacker, resold to other businesses whose practices may not always be in the consumer’s interest (e.g., employment decisions) or swept up in a government subpoena. We believe all players in the industry need to recognize the long-term ramifications and implications of any data being collected online and establish best practices and technical measures to provide users greater transparency, choice and control.