Statement of Alex Fowler
Chief Privacy Officer, Mozilla
US Senate Committee on Commerce, Science and Transportation
"The Need for Privacy Protections: Is Self-Regulation Adequate?"

June 28, 2012

Chairman Rockefeller, Ranking Member Hutchison, and Members of the Committee, thank you for the opportunity to testify today on the need for privacy protections, the status of self-regulation, and Do Not Track.

I am Alex Fowler; I oversee privacy for Mozilla and lead our work on Internet-related policy issues. I've spent the last twenty years working on privacy as a technology policy analyst here in Washington, a consumer advocate, in a start-up developing privacy software tools and as a Big 4 consultant advising leading banks, healthcare and technology companies.

Mozilla is a global community of people who have been working together since 1998 to build a better Internet.[1] As an independent organization, we are dedicated to promoting openness, innovation, and opportunity online.[2] Mozilla does not own or operate a search or advertising business. Our mission is to pursue the interests of users, developers and the Web as a whole. Mozilla and its contributors advance our goals by making free, open source technologies for consumers and developers that reflect these values. Our most popular product is the Firefox Web browser used by more than 500 million people worldwide. As a core principle, we believe that the Internet, as the most significant social and technological development of our time, is a precious public resource that must be improved and protected.

We also believe that commerce is a vital and beneficial Internet activity. Enabling and maintaining economic ecosystems online is an important component of a robust and healthy Internet. However, we do not believe that the commercial imperative and user

[1] See http://www.mozilla.org for more information about Mozilla, its mission and many initiatives.
[2] The Mozilla Manifesto is available at http://www.mozilla.org/about/manifesto.en.html

choice/control are mutually exclusive. They can and must coexist through a combination of technical capabilities and user-centric business and data practices.

As a privacy professional, I see the Web ecosystem as increasingly relying on a *guesswork* economy. Many of our best and brightest engineering minds are hard at work on new technologies to predict and deliver what the user wants at just the right moment. They use content delivery networks, profiling, tracking, social graphs, and data analytics to grasp at tiny clues about us and piece them together to *guess* who we are, where we live, and what we like or want. Just recently it was reported that Orbitz presents higher priced hotels based in part on the operating system of the user. Apparently Mac users spend more on hotels, so Orbitz lists higher-priced rooms for them.[3] These results represent impressive feats of business and technological prowess, and the industry reports record growth,[4] yet they have not led to a Web ecosystem where the user is an active and informed participant.

The public is increasingly uneasy about the extent to which their online lives are invisibly profiled, analyzed, packaged, sold, and reused to personalize advertising, content and services.[5,6] This unease leads many users to want to understand and control the collection and use of data about them. We see new online privacy protecting services launching every month and privacy browser add-ons are growing in popularity. Many of the most popular approaches disrupt and are in direct conflict with common business models. Some of the tools block interactions between users and sites, third party advertising or data brokers.[7,8] This pattern has been likened to an "arms race," with industry and Web users locked in opposition to one another.

---

[3] Mattioli, Dana. On Orbitz, Mac Users Steered to Pricier Hotels. *The Wall Street Journal* (June 26, 2012). <http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html>

[4] Ha, Lyons. Internet Ad Revenue Reaches $31B In 2011, Mobile Up 149 Percent (IAB Report). *TechCrunch* (April 18, 2012). <http://techcrunch.com/2012/04/18/iab-revenue-report-2011/>

[5] TRUSTe. 2008 study: Consumer attitudes about behavioral targeting. (March 2008). <http://danskprivacynet.files/wordpress.com/2009/02/truste2008_tns_bt_study_summary1.pdf>

[6] Turow, J. et al., Americans Reject Tailored Advertising and Three Activities That Enable It (September 29, 2009). <http://ssrn.com/abstract =1478214>

[7] Lyons, Sean. Privacy Concerns Spark Innovations Among Companies, Startups. *International Association of Privacy Professionals* (May 11, 2012). <https://www.privacyassociation.org/publications/2012_05_10_privacy_concerns_spark_innovations_among_companies_startups>

We have an opportunity to break this cycle by working together with industry to develop innovative mechanisms that address real business and technical challenges and empower people to engage in an online ecosystem that's both sustainable and fair.

Mr. Chairman, the remainder of my statement focuses on the three areas you requested in your invitation on the current state of: industry self-regulation; our Do Not Track feature in Firefox; and the ability for industry to provide meaningful privacy tools.

I. The current state of industry self-regulation

It is unclear whether industry self-regulation, by itself, is a viable way to allow users to manage and control data collected and used about them by third parties. Any process that does not represent the users' interest is unlikely to be successful. Outside of the processes undertaken many years ago to develop fair information practices in the 1980s[9] and Web site privacy policies in the 1990s,[10] we have tried to address current privacy issues either through narrowly construed, industry-led efforts or a patchwork of state, federal and international privacy laws.

In particular, industry promoted the notice and choice model as a way to harness the power of the free market to provide the transparency needed for people to make individual decisions about which sites and services meet their privacy needs. This is an important goal: it is clear that different people have very different privacy preferences, so ideally they would have the tools they need to make informed choices for themselves and their families. Unfortunately, the notice and choice approach has some flaws, which have led to failure in the market. Under our current model, choice was supposed to be enabled

---

[8] Several of the most popular add-ons for Firefox are aimed at blocking advertising and tracking, including Adblock Plus, Ghostery and NoScript. Adblock Plus alone has been downloaded 160 million times, and has almost 14 million daily users.

[9] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *Organisation for Economic Co-operation and Development (OECD)* <http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html>

[10] Privacy Online: A Report to Congress. *Federal Trade Commission* (June 1998). <http://www.ftc.gov/reports/privacy3/toc.shtm>

by consumers using the sites, services and applications with the privacy notices that best reflect their values. Yet privacy notices are a mix of legal and technical jargon, impenetrable to all but the most sophisticated. Privacy policies are not going away, however. They are required under California law. We continue to see new best practices emerge, and the process of developing privacy notices for mobile may lead to some new innovations. But the original idea that people would read multiple privacy policies to decide which sites to visit or buy from has not happened. Today, the privacy practices are indistinguishable across sites. Privacy policies have not worked to inform or empower users.

Seals and trust marks are another form of notice that have only partially improved privacy online. The Better Business Bureau (BBB) offers a seal program.[11] TRUSTe, which does so, too, has weathered some rough years, with findings that the business practices of TRUSTe customers are less privacy protective than average.[12] BBB's and TRUSTe's work has been valuable in helping companies clarify their privacy practices. However, seals are an approach by business for business that has not measured up to the high hopes of empowering users' online privacy choices.

One of the more recent and visible industry self-regulation efforts has focused on online behavioral advertising.[13] We join many others in commending the Digital Advertising Alliance (DAA) for its work to bring together the online advertising industry, and the growth of its ad-based icon. While the icon program is a good step, it suffers from material implementation hurdles[14] and technological limitations that cause it to fall short.[15] Despite the advertising industry's extensive expertise on succinctly communicating

---

[11] BBB Accredited Business Seal for the Web <http://www.bbb.org/us/bbb-online-business/>

[12] Vila, T., Greenstadt, R., and Molnar, D. Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. In *ICEC '03 Proceedings of the 5th International Conference on Electronic Commerce* (2003) Pages 403 – 407.

[13] Kaye, Kate. Icon War? Two Behavioral Ad Notice Icons Could Confuse. *ClickZ* (January, 2010). <http://www.clickz.com/3636315>

[14] For example, "These results suggest that the icons and tagline are failing to effectively communicate their purpose to users" in Cranor, Lorrie F. Can Users Control Online Behavioral Advertising Effectively? *Security and Privacy Economics* (March/April 2012).

[15] Five technical hurdles described in Mayer, Jonathan R. and Mitchell, John C. Third-Party Web Tracking: Policy and Technology. In *IEEE Symposium on Security and Privacy* (2012), page 422.

complex messages, the advertising option icon is incredibly unclear to users.[16] Many believe that clicking on it will trigger pop-up ads or invite more advertising, and many more expect that it is related to purchasing advertising space.[17] According to the industry's own research, the number of users who use the icon is low: 0.0035% click, and only 1 in 20 of those actually opt out.[18]

Since the icon is just a gateway to the industry's current cookie-based opt-outs, it suffers from drawbacks and fragility. One significant challenge is that the mechanism is not persistent because it is cookie-based. Users who routinely clear their cookies for security or to limit tracking also inadvertently remove their opt-out cookies under the current industry self-regulatory program. The Ad Choice interface also does not work on all platforms, leaving Mac users without a way to opt-out. Opt-outs are also ambiguous: different companies interpret their opt-out cookies differently. Some stop collecting info about users, while others continue collecting info, but stop customizing content and advertising, making their data collection practices invisible to users. Finally, opt-out cookies are not a scalable option for users. Even if a user requests opt-out cookies for all advertisers today, that choice is not extended for new advertising companies tomorrow. With this mechanism, users have to keep a vigilant eye out for new companies.

My primary point here is that without input and commitments from stakeholders outside of the ad industry, industry efforts like seals and the one led by DAA will remain insufficient. They do not establish the public trust and engagement needed for success. Such options invite stronger measures like regulation and all the risks of unintended consequences that go with it.

We are seeing an important shift in self-regulation away from closed-door, industry-led efforts to multi-stakeholder approaches where industry, users, academics, service providers, browser providers and consumer advocates come together to develop holistic

---

[16] Leon, P. et al. What Do Online Behavioral Advertising Disclosures Communicate to Users? (April 13, 2012). <http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf>
[17] IBID.
[18] Consumer Interactions with Ad Notice. *Evidon* (2011). <http://cdn.betteradvertising.com/misc/consumer%20impact%20of%20ad%20notice%2011_11.pdf>

frameworks and standards for the protection of privacy.[19] This is different from what has happened in the past where a single industry adopted its own unilateral scheme. It is precisely this broadening of self-regulation to deliberately involve all relevant stakeholders, combined with FTC and Administration support, that will increase chances of success and potentially avoid the need for regulation.

Many of these new discussions are occurring in the World Wide Web Consortium (W3C) Tracking Protection Working Group.[20] Despite dialogue that could sometimes be characterized as atypically aggressive (for standards working groups) and even personal at times, the process has been open, transparent, and inclusive. The group consists of over 35 leading companies,[21] including advertisers, publishers, and Internet companies, together with consumer advocates, industry trade associations, academics from the US and Europe, and independent experts. The discussions have been productive so far. The group is committed to following a consensus-based approach to achieve a protocol that everyone can live with.

As a member of the W3C group, we remain optimistic that the process will produce a meaningful standard that ultimately provides people with more choice and control related to targeted ads and user tracking by 3rd parties. Together with the Administration's multi-stakeholder process to develop a code of conduct that promotes transparent disclosures to consumers concerning mobile apps' treatment of personal data,[22] we are hopeful that a more representative cadre of concerns will produce effective self-regulatory practices without the need for legislation. However in the event that an open, multi-stakeholder process is not successful it may be necessary to explore regulatory measures.

---

[19] See the NTIA's Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct <http://www.ntia.doc.gov/federal-register-notice/2012/multistakeholder-process-develop-consumer-data-privacy-codes-conduct>, as well as Mozilla's comments to the National Technology and Information Administration, <http://www.ntia.doc.gov/files/ntia/mozilla_comments_040212_final.pdf>

[20] See the Tracking Protection Working Group page <http://www.w3.org/2011/tracking-protection/>

[21] See the Tracking Protection Working Group participants list <http://www.w3.org/2000/09/dbwg/details?group=49311&public=1>

[22] United States Department of Commerce. First Privacy Multistakeholder Meeting: July 12, 2012. *National Telecommunications & Information Administration* (June 15, 2012). <http://www.ntia.doc.gov/headlines/2012/first-privacy-multistakeholder-meeting-july-12-2012>

II. The current state of the Do Not Track feature in Firefox

Mozilla was the first browser to implement Do Not Track in March 2011 inspired by innovations from privacy and security researchers Christopher Soghoian and Dan Kaminsky.[23] When we first announced it, the ad industry was critical and Microsoft publicly ridiculed the feature,[24] but the FTC strongly supported it and our users wanted it. Today 9% of our users have turned on DNT in the desktop version of Firefox and 18% have turned on DNT in the mobile version. Microsoft has announced it will ship IE with DNT turned on by default in Internet Explorer 10, and soon it will be possible for users to turn on DNT in all major browsers. Numerous companies already honor the DNT signal, including social networks like Twitter, publishers like the Associated Press, and mobile advertisers like Jumptap, AdTruth, and more are on the way. We are building DNT into Thunderbird, our email client, and our mobile operating system, code named Boot2Gecko, where the user's DNT signal will be available to every app on the device. In addition to our engineering contributions, a Mozilla engineer submitted the first standards proposal for Do Not Track, and a member of our community is co-chair of the W3C standards effort.

Do Not Track is a simple, digital signal sent by the user via the browser to Web sites. As a signal, Do Not Track does not enforce, break, control, disable or impair any online tracking or personalization technology. It is a signal that is sent along with Internet traffic, indicating that the user sitting behind the keyboard would like their privacy to be respected more strongly than might otherwise be the case. To make it effective, the recipients – Web sites and ad networks – must breathe life into the signal by honoring the user's intent. The crucial questions therefore become:

- What does the user intend by the DNT signal?
- What should a site do when it receives this signal?

---

[23] Soghoian, C. The History of the Do Not Track Header (January 21, 2011). <http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html>

[24] Mullin, J. Microsoft: It's Naive To Trust Tracking Sites To Obey Anti-Tracking Orders. *paidContent* (February 10, 2011). <http://paidcontent.org/2011/02/10/419-microsoft-its-naive-to-trust-tracking-sites-to-obey-anti-tracking-signa/>

These questions are the subject of a consensus driven multi-stakeholder effort currently underway at the W3C, as I mentioned a moment ago. The Do Not Track working group is chartered[25] to develop a robust self-regulatory framework for user choice and control on the Web. While the group has agreement on most of the technical requirements of the protocol, there are still two competing views on what DNT should mean. One is that DNT means what it says, no 3rd party tracking of users whether its targeted ads or for other purposes. The other position is that DNT means no targeting, but tracking and collection are still acceptable. Currently, the working group is perusing a middle ground. The participants are collaborating in an open process to determine both the technical and compliance requirements for a Do Not Track system.

No single party can address privacy related to personalization and tracking on their own. The ecosystem is so diverse and specialized that there is no one entity who knows exactly which data is going where. Publishers can't predict which ads will show up on their sites after an auction. Advertisers can't predict which sites their ads will land upon. There is no single place for users to go to find out: “Where did my data end up?”

There is likewise no party that can build a complete solution on their own. Browsers have many options to provide strong choices and controls to their users.[26] However, browsers' technical measures risk being overly blunt, and disabling some features as well as protecting against privacy threats. As noted earlier, the cookie-based opt-outs provided by advertisers and analytics engines are ambiguous, do not scale, are not persistent, and do not truly address many users’ privacy concerns. Advertising self-regulatory groups do not include social networks like Facebook or Twitter. Users are concerned about being followed across the Web whether or not there is advertising involved. In contrast, DNT sends a signal with every request – whether to a publisher, advertiser, or social network – with no need to worry about new businesses or new business models. DNT is a protocol that can address users’ concerns and augment existing systems and initiatives.

---

[25] See the Tracking Protection Working Group charter <http://www.w3.org/2011/tracking-protection/charter>

[26] Lowenthal, T. Browser Vendors: fight for your users (April 29, 2011). <http://www.w3.org/2011/track-privacy/papers/lowenthal_position-paper.pdf>

Research shows that some users want personalization, many favor privacy, but the majority will make up their minds based on whether they see value to them or not.[27] Tracking, in and of itself, is not necessarily a problem when users can participate in the decision and understand how they benefit. Issues arise when users are unable to control their browsing experience, or worse, loose confidence that they are an active participant in how information about them is collected, used and shared among sites and apps.

DNT is narrowly-tailored to give users choice and control in a persistent, accessible way without preventing the customization and valuable advertising that powers our rapidly-growing Web economy. Innovative and transparent ways for users to obtain personalized content in a manner that respects user choice are both desirable and good for the Web. The DNT standard also envisions ways for users to request personalization and offers new opportunities for compelling user engagement and trusted relationships. In addition, unlike the Do Not Call list and the Ad Choices program, DNT is free to advertisers. There are no annual subscriptions to lists or fees to use icons. There is no cost to the taxpayer.

It will take more time for stakeholders to agree and best practices to emerge, as Do Not Track is a unique multi-party, client-server approach to addressing privacy. We will also need a period to educate users and listen to their feedback so that we can match the DNT system with their expectations and produce a compelling experience.

A DNT signal is not the beginning or the end of the privacy conversation, nor the only way user data is protected. Web sites, service providers, ad networks play an essential role, and have much to offer by their own data practices and policies.

[27] McDonald, Aleecia M. and Cranor, Lorrie F. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. In *38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)* (October 2, 2010).

III. Industry's ability to provide users with tools to adequately protect their personal information online

Privacy by Design is a crucial concept for the Committee to champion. As long as the Web economy provides incentives for companies to start collecting lots of user information, scale up, and then bolt on privacy protections after the fact, we are unlikely to see users satisfied with the promise of the available privacy tools and services. Privacy by design is an approach that addresses user data and privacy implications of new products and services from the outset. There are many successful examples of traditional and non-traditional companies that have built fully scalable and commercially viable products and services on the Web based on this approach. For example, one Web search engine never collects any logs[28] that can be associated with a particular person while still capturing all the information they need to build a powerful and viable service. And the GMAT switched to a less-intrusive method of verifying test-takers' identities as it balanced important business needs with student privacy concerns.[29]

For years, the Internet worked on the model that anyone on the same mainframe was a co-worker, not a threat, and networking meant sending text files over modems. Worms, malware, and phishing attacks highlighted how much had changed in a short time. Since then, security has become a priority for companies. Microsoft famously retooled their operating system and software development process to address security problems. Now we are finding a similar crisis with the privacy dimensions of user choice and control. It is not just users who lack a complete privacy picture. Companies are starting to realize they do not know what cookies they set, how they use data, and where it flows internally or externally. As an industry, we are going to need efforts to figure that out, plus ensure we design with privacy in mind.

---

[28] DuckDuckGo Privacy, <https://duckduckgo.com/privacy.html>

[29] Hill, Kashmir. Why 'Privacy By Design' Is The New Corporate Hotness. *Forbes* (July 28, 2011). <http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/>

We often talk about "personal information," but we are beginning to understand that even data that does not include someone's name, email address, or social security number can have real privacy impacts. For example, Netflix viewing history – which on its face appears not to be personally identifiable at all – has been used to identify specific people's sexual orientation and medical conditions.[30] The truth is that it's incredibly hard to predict how several pieces of apparently unrelated information can be combined to produce uncomfortably personal insights. We already have the technology to implement much of the Web ecosystem while leaving users in control of even this sort of information.

* * *

In conclusion, data sharing, control, security, and management are critical consideration for Mozilla. It is embraced in the products and services we create, and derives from a core belief that people should have the ability to maintain control over their entire Web experience, including how their information is collected, used and shared with other parties. We strive to ensure privacy and security innovations support consumers in their everyday activities whether they are sharing information, conducting commercial transactions, engaging in social activities, or browsing the Web, but the key is informed and reasonable choice enabled by transparency. Mozilla is pleased to be part of a vibrant user data landscape that is rapidly evolving to a future that will give people more choice and more control to participate fully in their online experience.

Thank you, again, Senator Rockefeller and members of the Committee for the opportunity to join you today.

[30] Narayanan, A. and V. Shmatikov. Robust De-anonymization of Large Sparse Datasets (2008). <http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>