Mozilla Global Advertising Standards

****Stacy Martin & Tom Lowenthal, 2012

# Standards FAQ

## Purpose

This document describes the high standards to which all Mozilla advertising should adhere. It represents the collected expertise of the Privacy, Marketing, and Engagement teams. Mozilla and any external ad services and agencies should follow these standards for all online advertising and promotional activities. We hope that these standards will help all our outreach activities remain consistent with the Mozilla mission and manifesto, and with our privacy principles.

This document consists of 3-parts:

1. Internal Standards Document
2. Definition of Terms
3. Vendor/Publisher Checklist

The vendor/publisher checklist should be completed by all external partners prior to the launch of an advertising campaign.

## Use Case

This document is to be used as a roadmap for selecting and working with any agency, vendor or publisher relationships and/or plans to be executed by or on behalf of Mozilla.

## Mozilla Specifics

Six core privacy principles guide our data practices and operations at Mozilla. These principles stem from the [Mozilla Manifesto](http://www.mozilla.org/about/manifesto).  We apply these six principles when selecting trusted vendors.

1. **No Surprises:** Only use and share information about our users for their benefit and as spelled out in our notices.
2. **Limited Data:** Collect and retain the least amount of user information necessary and share data anonymously whenever possible.
3. **Real Choices:** Educate users at the point that we collect any data and give them the option to opt out whenever possible.
4. **User Control:** Innovate, develop and advocate for privacy enhancements that put users in control of their online experiences.
5. **Sensible Settings:** Establish default settings that balance safety and user experience appropriately for each transaction.
6. **Trusted Third Parties:** Make privacy a key factor in selecting and interacting with partners.

## General Comments

Mozilla places ads on third party websites to introduce new users to our products and services, to recruit to our community and to encourage users to opt in to receive communications from Mozilla. Consistent with our mission and privacy principals, our goal is to provide full transparency and control over how our ads appear and function. The below bullet points are general statements to be supported in further detail later in this document.

* Tracking or collecting data is only acceptable on an aggregate, non-user specific level.
* Tracking or collecting data is only permissible for basic campaign tracking and billing.
* Cookies must not save any data that could identify an individual.
* It is legitimate to target advertising to the users immediate present .
* It is not legitimate to capture behavioral data to personalize or select future ads.
* Do not collect or create identifiers unique to a specific device, user-agent, or person.

The key principle is that a particular person's actions or identity should not be stored, and that future advertising should not be targeted based on this type of data store. On the other hand, it is completely acceptable to select an advertisement based on the information immediately present information at the time of a request.

**Not acceptable:** A user is given a cookie with an unique ID. As they browse, every page that they visit is logged with their unique ID. When choosing which ad to show, the decision is based on an estimate of their interests based on this list of pages.

**Acceptable:** A user visits a page of movie reviews. Their IP address indicates that they are roughly in the city of San Francisco, where it is about 5pm. Based on this information, they are shown an advertisement for movies showing in San Francisco this evening.

This requirement slightly reduces the level of targeting accuracy that a campaign will start with. It is important to measure rates of click-through and conversion of different placement “contexts”. This information can then be used to tune the campaign towards the optimal contexts. Campaigns may require more thoughtful design and optimization of contextual factors to achieve CPM, CPC, and CPA targets. Further detail on this appears below.

However, click-through and conversion measurement should not result in detailed tracking of individual users. Wherever possible, use ephemeral tracking techniques which to not place or collect individual identifiers.

**Poor implementation**: To see which placement contexts result in the best conversion rates, each user is given a unique cookie when they interact with an advertisement. A server-side database records which placement context each cookie ID is in, and that ID is recorded at each step towards conversion.

**Better implementation:** When a user clicks on an advertisement, they are given a non-unique session cookie in the Mozilla.org domain, recording the parameters of the placement context. At each step towards conversion, the cookie is read, and the server increments its counts of the associated context factors, without ever recording user-specific info. If a user converts, the cookie is immediately expired.

**Superior implementation:** Each as placement links to a URI which contains the relevant context parameters. Subsequent clicks towards conversions retain these URI parameters. When a URI with these parameters is loaded, the server increments its counts of the associated context factors. No cookies are ever set or read.

## Do Not Track

Mozilla pioneered Do Not Track and is firmly committed to providing this user choice. All publisher partners must comply with the DNT specification. A DNT:1 header must at least trigger the publisher's normal behavioral targeting opt-out.

Whenever a publisher sees a request with a DNT:1 header, they should:

* delete the user's behavioral profile,
* expire all tracking cookies, and
* stop collecting data

More information on DNT:

<http://firstpersoncookie.wordpress.com/2011/01/31/dnt-1-tell-sites-i-do-not-want-to-be-tracked/>

A real time case study on implementation:

<https://developer.mozilla.org/en/The_Do_Not_Track_Field_Guide/Case_studies/1_Advertising_company>

To learn more, contact Tom Lowenthal tom@mozilla.com.

## Creative Spec Requirements

Mozilla supports open web standards, and we wish to embody this in the type of advertising we use. Flash is non-free proprietary software whose development is at odds with web standards. Flash (.swf) should not be used in any Mozilla campaigns. Consider using the following alternatives:

* HTML5, JavaScript
* Animated GIF files
* PNG, JPEG, or GIF images

If you are unsure whether a particular technology is compatible with the principle of an open web, and contemporary web standards, contact tom@mozilla.com.

## Ad Serving Specifics

Mozilla does not have a proprietary ad server. Mozilla has certain approved third-party ad-serving vendors. If third-party ad-serving is needed, please use one of these vendors.

Even approved third-party vendors should not use third-party cookies since users are not familiar with the publisher placing the cookie, are likely not aware the cookie was placed, and cannot determine that the cookie is associated with Mozilla. Instead first-party cookies should be set from domains which are obviously associated with Mozilla, such as media.mozilla.org.

These are the ad serving companies that have 1st party cookie systems set up on behalf of Mozilla:

* Mediaplex (a Value Click company)
* TruEffect
* Flash Talking (coming soon)

For more information on working with on of the above 1st party vendors please contact stacy@mozilla.com.

Since we have these first-party solutions, all agency partners must assume cost liability in setting up any additional first-party environments for new ad serving solutions.

## User Tracking

The “General Comments” section as well as “DNT” section above lists out Mozilla’s general standpoint on user tracking and required specifics.

Additional specifics not previously covered:

### Cookie Expiration

All cookies should expire within 3 days of the end of the associated ad campaign. This means that cookies set at different times during the campaign should have different validity periods. A cookie set on the first day of a three week campaign could have a three-week validity period, while one set on the last day, might only be valid for 48h.

### No Profiling

As mentioned earlier in this document, no data specific to a particular user, user-agent, or device should be collected and stored. Similarly, publishers must not profile users based on Mozilla advertising campaigns, at any time. In particular, there should be no tracking based on a device’s unique ID.

## Post Click Tracking (1x1 Pixel Tracking)

An advertiser or agency may place invisible 1x1 tracking pixels on the pages that users reach when the click an ad. These tiny images allow the advertiser to track how frequently users click through successive pages associated with that campaign. These images should be used to track aggregate click-through associated with different placement contexts, and to optimize ad buys during and after a campaign.

This sort of aggregate tracking is okay, but it comes with restrictions. Tracking images should only be placed on campaign-specific landing pages. If a page could readily be reached by users outside the context of the ad campaign, it should not contain tracking images. In some cases this might mean that it makes sense to duplicate existing Mozilla pages, add tracking elements, and place them at campaign-specific URLs, so that non-ad users won’t reach them, but ad and non-ad users have similar experiences.

**Costs** The costs for tag creation should be included in the overall media spend and not presented as incremental to the overall media budget.

**Lead Time** The agency or marketing manager should build in at least 5 to 7 working days pre-campaign for Mozilla to file the bug to have the pixels placed.

## Online Targeting Specifics & Requirements

Mozilla advertising campaigns should not use any targeting based on users past actions, but may target based on users immediate present. Below is a list of acceptable and not accepted targeting practices. For full definitions on each targeting practice, please reference the glossary of terms at the appendix of this document.

The general rule of thumb is: if you need to store information about this user on the server, you should not use that form of targeting. If you can target based only on the information in the user’s HTTP request, you’re probably okay.

### Do Not Use

* behavioral targeting
* demographic targeting
* psychographic targeting
* re-targeting

### Acceptable Targeting Practices

* browser or user-agent targeting
* geo-IP targeting
* targeting based on time-zone

contextual targeting

## Online Media Placement Specifics

Since Mozilla’s mission is based around supporting an open and free web, advertising messages displayed by Mozilla should not interrupt or intrude on a users web experience. Below is a list of acceptable and prohibited media placements.

### Accepted Executions

* Display (Banners) :
* Search engine marketing (SEM/PPC)
* Online video
* Pre-roll, in banner video, episode players
* Video seeing (if listed as sponsored message in editorial well positions)
* Expandable rich media units (only if user initiates the expansion)

### Not Supported Executions

There may be some cases where these can be used. Such cases much be specifically reviewed by Mozilla’s Marketing and Privacy teams on a case-by-case basis.

* high impact units
* page takeover
* interstitial
* pop-ups

## Media Buy Purchase Model Specifics

The following purchase models are tested and approved given all targeting and tracking guidelines are adhered to:

* CPM
* CPL
* CPC
* CPA

## Email Marketing Specifics

Email marketing can be executed in 3 separate ways. The below detail describes each execution and the Mozilla standards specifics:

**List Rental** According to the CAN-SPAM Act of 2003, no advertiser can purchase lists to send promotional messages. The advertiser can “rent” these lists and the email can be sent via rental house/list owner. List rental email marketing can be used only if the user double opted in to receive specific messages. Within the email message when using list rental, the email creative must list the Mozillas physical address and a very clear opt-out link.

**Email Newsletters/Sponsorships**

**Advertorials**

## Mobile/Tablet Specifics (Excluding In App Ads)

If web advertising is targeted towards mobile devices or tablets, it’s still web advertising. The Mozilla online advertising standards listed in this document apply.

Collection of the unique ID of a user’s device (UDID) is explicitly prohibited. It is unacceptable even if the publisher or platform is offering to NOT link to personal data. Device IDs should not be used because users can't readily control or delete them. This results in a profile somewhere that a user can't control. A UDID can be used to track almost everything a user does with their mobile phone without that person’s awareness or choice.  Even if that's not what we plan to use it for, this lack of notice and choice would violate Mozilla's privacy principles of real choices, user control, and no surprises.

## In App Ad Specifics (Mobile)

As of June 2012, Mozilla does not support placing ads within any mobile apps unless through a Mozilla specific marketplace. To place ads in apps, significant engineering work would be needed. For more information on specifics please reach out to tom@mozilla.com

## Social Media Advertising Standpoint & Specifics: (Excluding Mobile Apps)

We treat advertising within social media sites where users voluntarily share information (ie. Facebook, LinkedIn etc.) differently from ads placed on other sites. Since the profiles are created by the user, and the user has openly given their information (ie. Facebook profile), user specific targeting is accepted. Behavioral advertising or re-targeting is not accepted in this environment but the following targeting is acceptable:

* Interest based targeting
* Geo/country based targeting
* Language based targeting

# Vendor/Publisher Check List

[ ]  I have read the Mozilla Global Advertising Standards Document, and I will

 follow it's instructions

[ ]  I have read the [Mozilla Manifesto] and Mozilla's [privacy principles].

 Anything I do on behalf of Mozilla will be governed by those principles

[ ]  I will not collect any user-specific data; I will only collect aggregate data

[ ]  I will only set cookies with opaque identifiers or non-unique info

[ ]  I understand Do Not Track, and every part of the campaign will respect

 any user's preference which is expressed this way

[ ]  I will not use Flash (.swf) or any other technology, which isn't compatible

 with the principle of a free, accessible, open web

[ ]  A third-party ad-serving solution is in place through a Mozilla-approved

 vendor, and it only uses first-party cookies set from a Mozilla domain

[ ]  All cookies will expire within 3-days of the end of associated ad campaign

[ ]  No publishers will profile users based on Mozilla advertising campaigns

[ ]  Post click tracking will only be placed on campaign-specific landing pages,

 not any other Mozilla page

[ ]  I will not use any prohibited targeting or tracking techniques

[ ]  Each media placements purchased on behalf of Mozilla is either has either

 been approved in general or for this specific campaign

[ ]  There will be no in-app mobile ads, and no recording or tracking of identifiers specific to a particular mobile device (like a UDID)

   [Mozilla Manifesto]: <https://www.mozilla.org/about/manifesto.en.html>

   [privacy principles]: <https://www.mozilla.org/privacy/>

# Definition of Terms

**Ad impression** - an ad which is served to a user‘s browser. Ads can be requested by the user‘s browser (referred to as pulled ads) or they can be pushed, such as e-mailed ads.

**Ad network** - an aggregator or broker of advertising inventory for many sites. Ad networks are the sales representatives for the Web sites within the network.

**Ad serving** - the delivery of ads by a server to an end user's computer on which the ads are then displayed by a browser and/or cached. Ad serving is normally performed either by a Web publisher or by a third-party ad server. Ads can be embedded in the page or served separately.

**Behavioral Targeting** - A technique used by online publishers and advertisers to increase the effectiveness of their campaigns. Behavioral targeting uses information collected on an individual‘s web browsing behavior such as the pages they have visited or the searches they have made to select which advertisements to be displayed to that individual. Practitioners believe this helps them deliver their online advertisements to the users who are most likely to be influenced by them.

**Browser Targeting** – A technique used by online publishers and advertisers to effectively target specific users based on their web browser (Firefox, IE9, Chrome, etc.)

**Contextual Ads** - Existing contextual ad engines deliver text and image ads to non-search content pages. Ads are matched to keywords extracted from content. Advertisers can leverage existing keyboard-based paid search campaigns and gain access to a larger audience.

**Conversion** - Term used to describe the process of getting a web visitor to accept an offer or become a paying customer. Advertisers strive for high conversion ratios.

**Cookie** - a small piece of information (i.e., program code) that is stored on a browser for the purpose of identifying that browser during audience activity and between visits or sessions.

**Cookie** **buster** - software that blocks the placement of cookies on a user‘s browser.

**CPA (Cost-per-Action)** - cost of advertising based on a visitor taking some specifically defined action in response to an ad. "Actions" include such things as a sales transaction, a customer acquisition, or a click.

**CPC (Cost-per-click)** - cost of advertising based on the number of clicks received.

**CPL (Cost-per-lead)** - cost of advertising based on the number of database files (leads) received.

**CPM (Cost-per-thousand)** - media term describing the cost of 1,000 impressions. For example, a Web site that charges $1,500 per ad and reports 100,000 visits has a CPM of $15 ($1,500 divided by 100).

**CPO (Cost-per-Order)** - cost of advertising based on the number of orders received. Also called Cost-per-Transaction.

**CPS (Cost-per-Sale)** - the advertiser's cost to generate one sales transaction. If this is being used in conjunction with a media buy, a cookie can be offered on the content site and read on the advertiser's site after the successful completion of an online sale

**Demographics** - common characteristics used for population or audience segmentation, such as age, gender, household income, etc.

**Frequency** - the number of times an ad is delivered to the same browser in a single session or time period. A site can use cookies in order to manage ad frequency.

**Geo-Targeting** - Displaying (or preventing the display of) content based on automated or assumed knowledge of an end user‘s position in the real world. Relevant to both PC and mobile data services.

**IAB (Interactive Advertising Bureau)** - IAB is a non-profit trade association devoted exclusively to maximizing the use and effectiveness of interactive advertising and marketing. See iab.net for more information.

**Impression** - a measurement of responses from a Web server to a page request from the user browser, which is filtered from robotic activity and error codes, and is recorded at a point as close as possible to opportunity to see the page by the user.

**Keyword** - specific word(s) entered into a search engine by the user that result(s) in a list of Web sites related to the key word. Keywords can be purchased by advertisers in order to embed ads linking to the advertiser's site within search results (see ―Search engine marketing.)

**Landing Page** - The page on a web site where one is taken after clicking on a advertisement. While this can be any page, it is often a page designed to expand on the service or product mentioned in the initial advertisement.

**Opt-in** - refers to an individual giving a company permission to use data collected from or about the individual for a particular reason, such as to market the company's products and services. See permission marketing.

**Pay-per-Click** - an advertising pricing model in which advertisers pay agencies and/or media companies based on how many users clicked on an online ad or e-mail message. See CPC

**Pay-per-Impression** - an advertising pricing model in which advertisers pay based on how many users were served their ads. See CPM.

**Pay-per-Lead** - an advertising pricing model in which advertisers pay for each "sales lead" generated. For example, an advertiser might pay for every visitor that clicked on an ad or site and successfully completed a form. See CPL.

**Performance pricing model** - an advertising model in which advertisers pay based on a set of agreed upon performance criteria, such as a percentage of online revenues or delivery of new sales leads. See CPA, CPC, CPL, CPO, CPS.

**Permission marketing** - when an individual has given a company permission to market its products and services to the individual. See opt-in.

**Persistent cookie** - Cookies that remain a client hard drive until they expire (as determined by the website that set them) or are deleted by the end user.

**Psychographics** - Identification of personality characteristics and attitudes that affect a person's lifestyle and purchasing behaviors. Psychographic data points include opinions, attitudes, and beliefs about various aspects relating to lifestyle and purchasing behavior.

**PII (Personally Identifiable Information)** - refers to information such as an individual‘s name, mailing address, phone number or e-mail address.

**PIN (Personal Identification Number)** - a group of numbers which allow a unique user access to a secured Web site and/or a secure area of a Web site. See password.

**Pixel** - picture element (single illuminated dot) on a computer monitor. The metric used to indicate the size of Internet ads.

**PLI (Privacy Leadership Initiative)** - a partnership of CEOs from 15 corporations and 9 business associations using research to create a climate of trust that will accelerate acceptance of the Internet and the emerging Information Economy, both online and offline, as a safe and secure marketplace. See understandingprivacy.org

**Privacy policy** - a statement about what information is being collected; how the information being collected is being used; how an individual can access his/her own data collected; how the individual can opt-out; and what security measures are being taken by the parties collecting the data. Privacy seal program - a program that certifies the Web site owner complies with the site‘s proposed policy. Examples include TRUSTe and BBBOnline. Profiling - the practice of tracking information about consumers' interests by monitoring their movements online. This can be done without using any personal information, but simply by analyzing the content, URL‘s, and other information about a user‘s browsing path/click-stream.

**Re-Targeting** - A technique used by online publishers and advertisers to target users based on past actions on a website and/or websites visited.

**Search engine marketing (SEM)** - a form of Internet Marketing that seeks to promote websites by increasing their visibility in the Search Engine result pages

**Server-initiated ad impression** - one of the two methods used for ad counting. Ad content is delivered to the user via two methods - server-initiated and client-initiated. Server-initiated ad counting uses the publisher‘s Web content server for making requests, formatting and re-directing content. For organizations using a server-initiated ad counting method, counting should occur subsequent to the ad response at either the publisher's ad server or the Web content server, or later in the process. See client-initiated ad impression.

**Server pull** - a process whereby a user's browser maintains an automated or customized connection or profile with a Web server. The browser usually sets up a unique request that is recorded and stored electronically for future reference. Examples are: requests for the automated delivery of e-mail newsletters, the request for Web content based on a specific search criteria determined by the user, or setting up a personalized Web page that customizes the information delivered to the user based on pre-determined self selections.

**Server push** - a process whereby a server maintains an open connection with a browser after the initial request for a page. Through this open connection the server continues to provide updated pages and content even though the visitor has made no further direct requests for such information.

**Session cookies** - These are temporary and are erased when the browser exits at the end of a web surfing session. . See cookie.

**Sniffer** - software that detects capabilities of the user's browser (looking for such things as Java capabilities, plug-ins, screen resolution, and bandwidth).

**Target audience** - the intended audience for an ad, usually defined in terms of specific demographics (age, sex, income, etc.) product purchase behavior, product usage or media usage.

**Third-party ad server** - independent outsourced companies that specialize in managing, maintaining, serving, tracking, and analyzing the results of online ad campaigns. They deliver targeted advertising that can be tailored to consumers' declared or predicted characteristics or preferences.

**Unique Browser** - An identified and unduplicated Cookied Browser that accesses Internet content or advertising during a measurement period. This definition requires taking account for the potentially inflationary impact of cookie deletion among certain of the cookied browsers that access Internet content.

**Unique Cookie** - A count of unique identifiers…that represents unduplicated instances of Internet activity (generally visits) to Internet content or advertising during a measurement period. Unique user - unique individual or browser which has either accessed a site (see unique visitor) or which has been served unique content and/or ads such as e-mail, newsletters, interstitials and pop-under ads. Unique users can be identified by user registration or cookies. Reported unique users should filter out bots. See iab.net for ad campaign measurement guidelines.

**Unique visitor** - a unique user who accesses a Web site within a specific time period. See unique user.

**URL tagging** - the process of embedding unique identifiers into URLs contained in HTML content. These identifiers are recognized by Web servers on subsequent browser requests. Identifying visitors through information in the URLs should also allow for an acceptable calculation of visits, if caching is avoided.

**Web beacon** - a line of code which is used by a Web site or third party ad server to track a user‘s activity, such as a registration or conversion. A Web beacon is often invisible because it is only 1 x 1 pixel in size with no color. Also known as Web bug, 1 by 1 GIF, invisible GIF and tracker GIF.

## Types of Online Advertisement

**Floating ad** - An ad which moves across the user's screen or floats above the content.

**Expanding ad** - An ad which changes size and which may alter the contents of the webpage.

**Polite** ad - A method by which a large ad will be downloaded in smaller pieces to minimize the disruption of the content being viewed

**Wallpaper ad** - An ad which changes the background of the page being viewed.

**Trick** banner - A banner ad that looks like a dialog box with buttons. It simulates an error message or an alert.

**Pop-**up - A new window which opens in front of the current one, displaying an advertisement, or entire webpage.

**Pop-under** - Similar to a Pop-Up except that the window is loaded or sent behind the current window so that the user does not see it until they close one or more active windows.

**Video ad** - similar to a banner ad, except that instead of a static or animated image, actual moving video clips are displayed. This is the kind of advertising most prominent in television, and many advertisers will use the same clips for both television and online advertising.

**Map ad** - text or graphics linked from, and appearing in or over, a location on an electronic map such as on Google Maps.

**Mobile ad** - an SMS text or multi-media message sent to a cell phone.

**Superstitial** - An animated adv on a Web page from Enliven Marketing Technologies. It uses video, 3D content or Flash to provide a TV-like advertisement. Used to be known as Unicast Transitional ads as they were originally made by Unicast Communications but the company was acquired by Viewpoint Corporation in 2004, which then changed its name to Enliven in 2008.[14]

**Interstitial ad** - a full-page ad that appears before a user reaches their original destination.