Submitter: Shane Wiley, Sr. Director – Privacy & Data Governance, Yahoo!, wileys@yahoo-inc.com

W3C Proposal – DAA DNT Hybrid

Do Not Track Headers and CLEAR Ad Notice

Most major web browser vendors recently released features aligned with emerging regulatory calls for a "Do Not Track" solution to online behavioral advertising. Major web browsers recently released features that align with calls for a "Do Not Track" solution to online behavioral advertising – although each company has taken a different approach to tackle the challenge. A better outcome for consumers is to converge on a single approach to exercising DNT choices to online behavioral advertising through web browser controls to reduce confusion and to better align the user experience with the consistency of the CLEAR Ad Notice program managed by the Digital Advertising Alliance (DAA). In short, it is proposed that web browser vendors align behind a single Do Not Track approach to increase consumer awareness through education and exposure to these features (additive vs. distractive).

It's important to keep in perspective that advertising fuels the vast majority of free content and experiences available to consumers across the Internet today. The sites who invest the time, energy, employees, and technology to provide these free experiences must be equal partners in the conversation about these standards. All stakeholders should seek to find a balance to consumer privacy protections and a publisher's ability to monetize their efforts.

DAA/DNT Hybrid Solution

As evidenced by the pains of removing IE6 from general use, it will take users time to upgrade to versions of web browsers that support a consistent, cohesive DNT solution. As currently implemented, DNT headers do not provide granular consumer control over their experience and their ability to express greater options for the brands they trust.

CLEAR Ad Notice was conceived and deployed to provide consumers with more granular information and choice in direct association with the ad they are seeing at that moment. In combination with CLEAR Ad Notice many participants in the advertising ecosystem are also launching detailed transparency and control tools to manage their advertising interests.

With that in mind, a hybrid DAA / DNT Header approach should be adopted to embrace simplified, persistent user controls native to the web browser and merge these with the mature opt-out programs already available to consumers which in turn are mated with maturing transparency mechanisms available through the Advertising Options Icon (CLEAR Ad Notice).

- **DAA:** Provides **transparency** and **granular choice** to users through existing solutions (backwards compatible)
- **DNT Header:** Provides the ability for opt-outs to be **persisted** and **evaluated/enforced**

How would this work?

- Setting Choice: User can set choice either through browser UI (DNT) or through Opt-Out pages (individual or group pages like NAI and AboutAds) available through CLEAR Ad Notice
    - Opt-Out signals are honored whether from the DNT Header or from the Opt-Out Cookie
    - DNT signal with a different value is sent to domains that are "trusted" (see "DNT Exceptions" below)
- Response to Choice: Once a DNT signal is received, the domain responds with a header response for the domain so the browser, the user, and interested 3rd parties can confirm the signal was received and appropriately accepted
    - One of two values should be returned:
        - acknowledged but not honored (see "DNT Exceptions");
        - or, honored.
    - A DNT cookie should be set to allow for external auditing of consumer choice (the DNT signal itself will remain persisted within the browser UI – the cookie is merely for transparency and audit purposes)
        - Modify existing opt-out cookies with a new DNT value;
        - Or, develop an industry DNT cookie for all parties to set to simplify external auditing

DNT Exceptions

To provide consumers with a level of choice (versus an "all or nothing" proposition), it will be important for users to be able to express exceptions to a DNT request. This approach also allows for the "quid pro quo" relationship between publishers and consumers to be expressed in a transparent and editable manner (allowing a user to change their mind at any time).

- Exceptions could be single entries or lists (users should have the option to view the entire list prior to agreement for its application)
- Entries should be expressed as a simple core domain name to simplify the experience for users (for example – publisher123.com, adnetwork345.com, or contentprovider567.com).
- While not necessary it would be beneficial if DNT Exception Lists could be subscription based ("off" by default) to reduce the nuisance to consumers as publishers engage in new 3rd party relationships.
- 1st parities should receive a signal if one or more of the 3rd parties available on their property have been blocked. This will provide the publisher with the option to provide a different (possibly reduced) experience to the user or for the user to provide an exception to gain access to free content.

Definition of "Do Not Track":

The W3C should not attempt to define what DNT means and instead leave this definition to be created by policy development and self-regulatory groups in partnership with consumer advocates and regulators.

This proposal has been developed to be implementable regardless of the DNT definition. That said, this submitter believes it would be most appropriate for industry to continue to maintain current, consistent

industry definitions. As such, at a high-level the scope of **the Do Not Track signal should be equal to the handling of today's behavioral advertising opt-out**.

Notably:

- **Do Not Profile:** The browser activity should not be added to a "profile" of the cookie – this extends to site retargeting efforts which cross non-commonly branded sites
- **Do Not Target:** The browser/device should not be targeted with online behavioral advertising (OBA)
- **Operational Needs:** Standard data collection for operational needs such as impression counting, frequency capping, and fraud detection/defense efforts is still supported.
- **1st Party:** Data collection and personalization activities provided by a 1st party are not subject to DNT. This extends to 3rd parties providing services only to the 1st party domain on their behalf and not developing cross non-commonly branded site OBA profiles.
- **Analytics:** Anonymous data necessary for basic reporting of impressions, clicks, and conversions should be maintained (not used to alter future browser experiences - outside of fraud defense)

Honoring User Preferences

As multiple systems may be setting, sending, and receiving DNT and/or Opt-Out signals at the same time, it is important to ensure publishers, advertisers, ad networks, and web browser vendors consistently honor user choices in circumstances where "mixed signals" may be received.

- **No DNT Signal / No Opt-Out:** Browser / device is not opted-out
- **DNT Signal / No Opt-Out:** Browser/device is opted-out
- **Opt-Out / No DNT Signal:** Browser/device is opted-out
- **Opt-Out / DNT Exception:** Exception is honored (browser/device is not opted-out)

Conclusion

Yahoo! strongly supports the standards development process and is submitting these recommendations in the hope that vigorous, enlightened, respectful debate ensues to drive consensus towards a solution that meets the needs of consumers, publishers, advertisers, and the parties that support each.