TRUSTe Position Paper October 21, 2012

Taking a Balanced Approach to Privacy

Microsoft's recent steps around setting the DNT default to "on" [DNT:1], and Apache's response to ignore the signal, has sparked discussions around what it means to provide choice, especially since online tracking and the use of technology to collect data play a critical role in the online eco-system enabling a rich online experience providing personalization, improvements to data security and usability, and efficient advertising and monetization models.

By virtue of the definition of the word - choice is the act of demonstrating a preference that a particular activity be engaged or avoided. In privacy parlance choice is about an individual indicating a preference about when a particular data collection or use practice is exercised against information about an individual. Choice can either be inferred or expressed. In its program requirements, TRUSTe defines these terms in the context of whether a company can engage in a practice based upon actions taken (or not taken) by an individual. It is up to the individual to exercise a preference over whether a company can or cannot engage in a particular data collection activity.

TRUSTe has taken a similar approach when developing its behavioral advertising solutions [Trusted Ads and Trusted Mobile Ads] that enable users to exercise their preference around having data collected and used for ad targeting purposes. Fundamental to these solutions is providing users clear and conspicuous notice (transparency) regarding why data is being collected thus allowing users to exercise their preference (choice) in an effective and meaningful way so the preference being communicated is what the user intended. The underlying technology for Trusted Ads utilizes a cookie-based approach.

DNT extends beyond the cookie-based approach utilizing the browser (user agent) headers to communicate a preference. Here a set preference is global and applies to all websites and parties operating on those sites. Some view this as an all or nothing proposition thus creating complexities around standardizing behaviors around when a DNT:1 signal is received. As noted above, the user needs to exercise their preference meaning the default is unset. There are instances where a user agent may set the default on the user's behalf. Even though setting the default does not reflect TRUSTe's viewpoint that the preference must be set by the user - ignoring a DNT:1 signal from a user agent with a preset default does not solve the problem either because in this instance users who indicated a preference not to be tracked will not be honored.

Resolving this requires a balanced approach that provides transparency and the user an opportunity to indicate their preference. One approach is to examine how DNT and cookie-based approaches can work in tandem. This can be done through utilizing out-of-band exceptions requests. A user visits a site, site or a third party integrated into the site recognizes the DNT:1 signal, provides the user notice explaining the DNT setting is 1, and provide the user the option to grant a site-wide or web-wide exception. The solution also gives the user the option to exercise preference at a more granular level using the cookie-based approach – opting-out of those parties they do not wish to be tracked. This can be done based upon the party's function (i.e. analytics or social plugin) or by domain (i.e. example.com) allowing the user to allow for functionality they find most beneficial or trustworthy

companies. One of the challenges with this solution, and one area the W3C can explore in developing standardization, is how to address choice collision and develop standards around the logic needed to ascertain what the user intended.

Highlighting trustworthy companies enables users to make an informed choice about whether they are tracked and by whom. A key component of this is Accountability. Companies agreeing to some level of oversight by an independent third party, such as TRUSTe's Trusted Data Collection certification program, demonstrates those companies are accountable not only to themselves but to users. The ability to demonstrate Accountability needs be built into any solution that enables users to exercise choice over the collection and use of their data. The W3C, as it has done in the DNT Preference Expression Specification, should ensure privacy considerations outlined in any of its standards support a mechanism for trustworthy companies to demonstrate accountability.

Many questions remain around how DNT will be implemented; including how this will work in the mobile space. The W3C Tracking Protection Group is working through these very complex questions, which at some point need to extend to mobile. TRUSTe believes a balanced solutions-based approach that includes an accountability component is needed to address these and other privacy related questions.

TRUSTe is actively participating in this discussion and others being had by regulators and various industry groups. TRUSTe looks to continue to play an active role in these discussions promoting solutions that support a balanced framework, and enables businesses to innovate and users to express preferences based on a privacy framework built upon transparency, choice, and accountability.