TRUSTe Position Paper for W3C Workshop on Web Tracking and User Privacy

TRUSTe has been actively involved in privacy compliance programs for websites, 3rd party ad and data providers, applications and cloud services. The recent upswing for enhanced privacy programs regarding 3rd party tracking and online behavioral advertising has led to a mix of self-regulatory programs and new consumer features added to recent browsers such as IE9 and FF4.

TRUSTe has deployed a mix of solutions ranging from a DAA-approved Notice and Choice program to certification programs for data companies plus technology for consumers to utilize for preference management. TRUSTe has been providing services for consumers that help them identify companies that meet a minimum industry best standards bar to signal good privacy and data governance practices. TRUSTe has also offered objective preference services that enable consumers to select from a range of participation options that meet their personal preferences and values.

For many consumers, TRUSTe's brand has served as short cut to understanding this very complex calculation of what good privacy means. TRUSTe has provided these services in ways that participate in self-regulatory regimes and those that specifically offer Safe Harbors in exchange for meeting minimum standards as mandated by governmental organizations.

As the dialog has shifted towards the discussion of a Do-Not-Track header, TRUSTe is interested in participating in the dialog and sharing its experiences in the implementation of these types of solutions, and to help shape the ultimate definition and direction of how technology can be best applied to consumers in what many consider a very nuanced and non-primary part of their online experience.

From a very high level, there are three primary constituencies that form the inflection points of the spectrum to address with respect to privacy controls: 1) Those very sensitive to their privacy and very proactive to learn and use the technical controls available to them to control their experience, 2) Those that either do not understand or do not care about privacy controls and thus do not want overly complex privacy controls, and 3) The large band in the middle which are people that do care to some degree when asked, but do not take the time to proactively manage any sort of privacy controls unless some incident has happened to them personally.

Any sort of controls that are offered directly to consumers need to consider these constituencies. As has been proven by past controls, if too complex, they will not be used properly. Or like the experience of AdBlock+ showed in the Firefox community, a security perspective will prevail, which leads to locking down everything and taking the most conservative path forward with respect to privacy. However, controls need to have the features that address those users that want the deep granular control.

With respect to the ad technology layers, most consumers do not understand the various entities in the ecosystem, as these are not companies with consumer-familiar brands. Requiring consumers to assess each is an inappropriate task with respect to its desired purpose. Simplicity needs to be a starting point unless there are easy ways to communicate differentiation among various ad and data companies that might be useful to consumers. Oversight and certification offer options to do this.

From the business or server side, the current defacto choice system has been based upon cookies for opt-ing out of seeing targeted ads, which were historically delivered via a website or industry groups' privacy policy and most recently, moving into the ad unit and on the same page as the ads appear. Ad companies using OBA are required via their self-regulatory organizations to deploy such system by approximately mid-year 2011. There are well-documented limitations to a cookie-based system around persistence and usage-only controls, which has led to browser extensions providing various features including script-blocking that provides control of cookie-based tracking by blocking the scripts that deliver those cookies.

The domain blocking systems, historically AdBlock+ (an all block solution) and MSFT's IE9 Tracking Protection Lists (a combination white and black list approach) presents a solution where companies need to consider their position on the most distributed lists to understand whether consumers are seeing their ads or not, as these solutions block the full ad content in addition to the collection mechanisms.

TRUSTe has built a TPL to work with the IE9 program which will provide a balanced list of ALLOWed and BLOCKed companies offering consumers a choice to see relevant ads, but only from companies that respect privacy per TRUSTe's documented standards. The qualifications for the ALLOW require a certification program that elevates only the best companies and requires DAA deployment where applicable.

With respect to the DNT header, there are both technical and political paths in consideration, of which the latter is out of scope of this position paper. A DNT header presents a more simplified preference for users to indicate this preference once and universally. However, this implies that the consumer understands what "tracking" is and what the implications of selecting a universal "opt-out" is.

From the business side, there is the open set of questions of compliance: If a consumer signals their preference how do they know a particular ad server (1) received it and (2) honored it? Assuming there is a methodology to convey this acceptance and honoring, how will this information be managed in the event of a dispute? How will information about the consumer's preferences be managed to determine if companies did not receive or honor it, and will this change the user experience?

Additionally, how can companies that provide the necessary industry requirements be recognized positively versus other companies that just ignore this system?

These and other questions deserve careful consideration; else they can relegate this technology to a partially adopted and confusing state that would reduce its effectiveness.

TRUSTe can contribute by helping companies deploy the necessary program elements to get into compliance with this system and by providing consumer-friendly approaches to demonstrate their respect of the opt-out preference to elevate their good standing and present the user with multiple preference options.