Privacy has many dimensions, and a definitional spectrum arises which spans between techniques that foster anonymity and those that foster transparency and choice. This double-meaning has led to some confusion as to what privacy really is and how it relates to security. Expanding on the latter scope of transparency and choice, privacy can be thought of as how companies disclose the use of data once they receive it and how they ensure the consumer offering the data has sufficient control over the primary and secondary uses of their data once submitted.

The primary method by which the majority of websites offer these types of privacy services is through a text/html-based privacy policy and possibly through the use of an opt-out/choice service via email or website interfaces. There are many shortcomings and limitations to the current system, which has relegated privacy into a state that is difficult to define by the bulk of online users, to systematize across the millions of websites offering services using personal and sensitive information, and to properly enforce practices across sites and services providers of all types and sizes. The dichotomy of this system is ironic in that millions of websites have the ubiquitous privacy policy, but the number of consumers that read and utilize privacy policies probably number much fewer.

There are several areas that become suboptimal in this system. The first typically involves some third party receiving data to offer a service on behalf of the 1st party, sometimes with proper permission by the consumer and sometimes otherwise. From the consumer's behalf though, it is tough to track who received his or her information and under what policy, what other parties were privy to it and what happened to the information further downstream. It is not an uncommon disclosure to see a website that uses a partner, but then discloses that the consumer is governed under the partner's privacy policy, even though the consumer has no direct choice in the selection of that partner in the first place. To abstract further, personal information is not encoded in any fashion to apply usage rights around the data as it travels through this ecosystem that leads to consumers feeling a general loss of control of their personal data.

A second area includes the simple disclosure of a business' privacy practices to a consumer in a fashion that is straightforward enough to make a proactive decision prior to submitting the data. Or at a minimum, that enables the consumer to keep an audit of where his or her info has been presented to a first party site and what other 3rd parties had access to that data and under what circumstances. Browsers have clearly not provided users with simple privacy interfaces in the same way they have provided simple DNS and security interfaces. With the advent of applications and web services, this problem has been compounded even further to essentially create an environment of less transparency than the browser-based desktop web.

The Ad and cookie ecosystem is starting to take some steps toward a better solution, but any solution would require some privacy payload to be added to the ad tagging layer, and most likely only for cases of behavioral advertising. Due to the distributed nature of the ad ecosystem, it is unclear how to enforce this across all entities. Furthermore, this approach still misses an important level of transparency for the various entities that exist as a cookie on a website vs. the actual website that are not OBA-based. How does a consumer know to connect the site policy from which the cookie originates with the cookie itself? Browser cookie interfaces can be best described as too clunky for the average consumer to manage these elements themselves and most consumers have given up in this area. The use of

certain browser plug-ins have helped some consumers better understand this ecosystem, but have been limited by the usual distribution challenges of third party plug-ins developed by small development shops.

What is needed to help advance this ecosystem forward? In almost all cases, privacy policies need to be augmented with a machine readable, service process-able XML counterpart. This would lead to new applications that could help consumers better understand what is contained in a given site's full policy (including their partners), at the site (URL) and cookie layers and for applications that sit on proprietary networks and clients. XML policies can also help sites manage data flows between their site and their partners sites and services and provide new foundations for tools that can encode information to provide accountability for that information all the way back to the sourcing consumer.

The traditional site use case of utilization of a browser client to promote a site's policy presents the need of several elements to build the necessary trust system around the xml policy infrastructure:

1) a method to illustrate the policy in a graphical fashion via iconography or other similar mechanism,
2) a method to delineate self-asserted policies vs. policies vetted by a trusted 3rd party which provide accountability services,
(3) methods to control 3rd parties that are trusted to provide such services, and
(4) methods to provide user feedback and dispute resolution.

A similar set of components can be established for the more general "enterprise" use case of partner management and sharing data across corporate boundaries.

For any trust system to achieve the appropriate level of acceptance and utilization, a combination of industry investment and standards development is necessary to develop the structure, dictionary and usage guidelines of the XML. TRUSTe's view is that the time for such a system is now more relevant than ever. Impending requirements from legislative and regulatory bodies, increased consumer awareness around behavioral advertising and social networks, and the advent of more products and services leveraging 3rd parties and privacy sensitive technologies, all lead to a pertinent opportunity time to address this collaboratively. Additionally, there are some lessons learned we can take from past efforts in various different communities that can help shape the effectiveness of such a campaign going forward.

**TRUSTe Contact:**

Kevin Trilli
http://www.truste.com/about_TRUSTe/people.html
http://www.Twitter.com/squawkt22