Standardization for Privacy Management

Position paper for the W3C "Do Not Track and Beyond" Workshop, November 2012

Mark Frigon, Arnaud Le Hors – IBM Corporation
October 22nd, 2012

Today, policymakers, businesses and society grapple with privacy issues at a time when advances in technology help us personalize service and solve complex problems through analysis of user data. Privacy discussions began with the emergence of the Internet. As the Internet has grown so has the gathering and use of varying amounts of information including at times sensitive information about individuals. Good data stewardship by businesses and governments can help address some of the privacy concerns , but is this enough?

Too often industry practices and/or technology solutions tend to be ones that are the least disruptive for the particular industry from which the proposal to protect consumer privacy emanates:

- Browser-based initiatives such as "Do Not Track" seek to preserve the browser capabilities, such as javascript and cookies, and thus recommend pushing enforcement of decisions around privacy from the browser-side and on to the server-side.
- The advertising network-based proposals, such as AdChoices, appear to ignore a more consumer-friendly universal browser-based "opt-in" approach, in favor of one that would require users to explicitly "opt-out".

While some of these technologies have gained considerable traction, most approach the problem with differing, and at times, conflicting implementations:

- Advertising-based initiatives rely on a browser cookie to store any consumer's "opt-outs". However, the EU Directive suggests that no such cookies may be placed on a consumer's browser without their explicit consent, rendering any consumer opt-out preferences moot.

- Browser-based “Do Not Track” approach allows consumers to request that websites do not track them. However, such approach relies on websites to honor the browser request and in no way prevents websites from actually storing sensitive data.

Counterproductively, all the differing approaches have only created more confusion for consumers as to how and what personal data is being collected and how to sufficiently manage one’s privacy. In addition, companies face uncertainty around which approaches will ultimately be adopted or codified. Accordingly website operators face a choice between the expense of implementing several approaches or, conversely, choosing complacency.

IBM’s Customer Experience Digital Data Acquisition proposal to the W3C offers a framework for a more standardized and flexible approach to consumer privacy management and enforcement. The proposed “Registrant” object in the Digital Data Acquisition proposal offers a framework from which to standardize privacy efforts. The Registration object offers a unique identifier field (“digitaldata.registrant.Registrantid”) which website operators can use to store requisite visitor identification. Additionally, other forms for sensitive data could be stored in the digitaldata.registrant.attributes array. This array provides an extensible container to store and access additional attributes that may tie to the user: user preferences, permission, membership levels, etc.

Additionally a common problem exists when a website operator might not be fully aware of all the cookies being placed on its own website due to 3rd party javascript “includes” for advertising, social media plug-ins, analytics, and other capabilities. Standardization around a common data model and common consumer object offers website operators the possibility of having more control around which information its vendors collect from its own customer-base. For example, an advertising network might “look” for a consumer’s social network IDs to provide more targeted advertising without the knowledge of the website operator. Such technical possibilities make it very difficult for a website operator to manage its own privacy policy.

In order to best balance the interest of all parties involved (consumers, website operators, browser manufactures, advertisers, policymakers, etc) we believe a standard backed by the

W3C to be the best way to gain adoption of a common privacy standard. Because of this we have submitted the Customer Experience Digital Data Acquisition specification to W3C, and are eager to work with workshop participants to explore the following questions:

1. Can browsers facilitate user management of the registration data while allowing websites to request access to potentially sensitive information?
2. What controls can website operators be given to enforce 3rd party "includes" collect and store data consistent with the website operator's privacy policy?
3. How might a standard help manage user data elements that may be defined as personally identifiable under different conditions?
4. What distinctions, if any, should be made between 1st party and 3rd party data access? Should the consumer or the website operator determine access based on a privacy policy?

We are committed to working through these questions, discussing feedback, and finding possible resolutions and solutions to provide consumers with more transparency, website providers with more control, and policymakers with an example of a self-regulatory approach. In addition to discussion during this workshop, we encourage all interested parties to join in the review and further development of the Customer Experience Digital Data Acquisition specification within a new Community Group. Our goal is to eventually have the specification "graduate" from the Community Group and move onto the Recommendation track as the basis for a new Working Group.

References

Customer Experience Digital Data Acquisition submission
http://w3.org/Submission/2012/04/

Tracking Protection Working Group
http://www.w3.org/2011/tracking-protection/

AdChoices
http://www.youradchoices.com/