Objectives for W3C Work on Web Tracking and User Privacy

W3C Workshop on Web Tracking and User Privacy

28/29 April 2011, Princeton, NJ, USA

Submitted by: AT&T

Contributors: Bryan Sullivan
Ileana Leuca
Sherry L Ramsey
Michael Merritt

---

1. Introduction

Past efforts at privacy-enabling standards (e.g. P3P) have reinforced that specifications alone don't solve problems. W3C should thus first facilitate a dialog on Web tracking and user privacy which establishes clear objectives addressing the Web as an ecosystem, part of an overall services marketplace in which Web tracking has a role, and in which user privacy is a clearly defined and achievable goal. It may take some time for an iterative process of specification, prototyping, and deployment experience to achieve a workable balance between the needs for tracking (e.g. for marketing and service personalization) and the desire for privacy. But that timeline will be shortest only if a comprehensive, shared understanding is first achieved on:

- The roles and objectives of tracking and marketplace stakeholders
- Characteristics of a desirable solution balancing tracking and user privacy
- The limits of current technology to achieve the desired solution

2. Roles and objectives of tracking and marketplace stakeholders

The Web is an ecosystem within a larger services marketplace, in which marketing data collection and service personalization are examples of how user/service information is used. Before considering detailed requirements or technologies supporting possible solutions, W3C should first:

- Seek consensus on the actual (i.e. current) role and methods of tracking in the Web ecosystem: Tracking does have an actual role, whether one considers it necessary or undesirable, and that role needs to be understood prior to

implementation of privacy-enabling solutions, to prevent undue negative effects on the Web ecosystem. Further, the methods currently used for tracking will need to be understood to ensure that privacy-enabling solutions are effective.

- Frame the role of tracking and desire for privacy within the set of roles and objectives of marketplace stakeholders, including:
    - Users, including individuals, families, and enterprises
    - Web user-agent developers, for browsers and other Web-enabling runtime environments (e.g. W3C widget runtimes)
    - Application developers, for client and server based applications
    - Service providers, including network service providers and Web service providers

If there is a role for "privacy/trust certification" as part of what W3C recommends, this should support market-based/globally-applicable approaches, e.g. as with existing PKI services and trusted application distributor models, e.g. for which privacy certification can be an aspect of overall user safety based upon trust in the application distributor.

3. Characteristics of a desirable solution balancing tracking and user privacy

The most important lesson learned from earlier efforts at W3C privacy standards is that W3C should standardize what has been proven to work in the market, i.e. has been developed, deployed, and used for some time, successfully. Standardization of technologies should not occur first – rather, objectives and guiding characteristics for solutions (including technology choices, where necessary) should be established, and quickly prototyped by Web user agent developers. This will necessarily require an iterative process of specification, prototype, and deployment experience, before a final technology standard is achieved.

Some objectives and guiding characteristics for solutions should include support for:

- an overall good user experience, e.g. easy to use, whether one wants to "opt-in" or "opt-out" by default, and change preferences easily and quickly as conditions warrant
- context adaptability, e.g. works well in different types of devices and user-agents, and whether a user's own or borrowed device is used
- effectiveness, e.g. resulting in a real sense of enhanced privacy
- limited impact on the Web services marketplace, e.g. does not "break the Web" or overly impact existing Web business models
- a technology basis in the W3C's existing content formats and user-agent behavior specifications, e.g.
    - HTML5, CSS, DOM
    - POWDER, e.g. as extended by WAC in "WAC 2.0", to address "Privacy Considerations for API Usage" and "Privacy Considerations for Device Property Access"

4. The limits of current technology to achieve the desired solution

It is important to understand the limits of technology to address the overall objectives of user privacy, in order to set reasonable expectations on what types of protection can be provided. For example, goals for user privacy may include that the user is always able to:

- Know that use of their information is actually limited to the disclosed use
- Know what information has been shared with whom (including who they have shared it with, etc), and where it still exists
- Revoke access to private information (including that which has already been shared, collected, or stored) and capability to request removal of retained individually identifiable information or be assured that it has been anonymized or aggregated.

These goals however are only partially achievable with current technology. At most it may be possible to express intent for private data use/exposure, and consent of the user to that intent. Verification of actual compliance to the stated intent and consent may require unspecified audit processes.

5. References

POWDER: Protocol for Web Description Resources (POWDER), W3C

WAC 2.0: WAC 2.0 Proposed Release Version (PRV), Wholesale Applications Community (WAC)