SENDING OUT A PING FOR WEB PRIVACY: LAYING OUT A PLAN
Christine Runnegar and Tara Whalen, Co-Chairs, W3C Privacy Interest Group

This is not so much a position paper, but rather a call to action.

The Privacy Interest Group (PING) was chartered by the W3C in 2012 "to improve the support of privacy in Web standards by monitoring ongoing privacy issues that affect the Web, investigating potential areas for new privacy work, and providing guidelines and advice for addressing privacy in standards development"[i].

Already, PING has made some progress towards these goals[ii], but more concerted work is needed across the W3C community.

Guidelines and advice

PING's mandate includes the development of privacy guidance for Web standards developers.

One of the first questions the PING chairs were asked was:

> "What is the intended audience"?

The primary audience is Web specification authors, however, there is also interest within PING to develop guidance (e.g. best practices) for implementers and deployers, particularly as additional privacy concerns arise at the point where implementation and deployment choices are made. Such guidance needs to be relevant, understandable and useful for the target audience.

Spotting potential privacy risks and vulnerabilities is an art, and possibly difficult for specification authors with no background in privacy. Nonetheless, there are (at least anecdotally) recurring privacy issues with Web standards that could stand to be articulated. There are also a number of different proposed design approaches to improve privacy of a specification (e.g., the permission-based model used in the Geolocation API, data minimisation, etc.) that could be evaluated (e.g., pros and cons).

Privacy reviews

There is consensus that W3C specifications, especially at an early stage in their development, would benefit from privacy reviews. PING has been identified as the logical coordinator for such reviews, and already four specifications have been proposed as candidates: Navigation timing; Web Intents; Content Security Policy 1.0; and the Web Cryptography API (at a future date to be advised). Charters for new groups also specifically require privacy reviews (e.g., Systems Applications Working Group Charter[iii]).

While there is considerable and varied privacy expertise in PING, it is not yet clear whether PING members will have sufficient expertise in the relevant specification subject matters to provide meaningful privacy reviews. There is also the question of resources and the weight that would be given to such reviews. Are PING members willing and able to commit to providing timely privacy reviews? How would those reviews be taken into account? How will the inevitable conflicts between privacy and functionality, usability, security, reliability, etc. be resolved?

Ad hoc informal privacy reviews provided by privacy experts have been useful in identifying possible issues (e.g., the potential for fingerprinting). However, to ensure greater consistency in approach across Web standards, it would be useful to develop methodology for privacy vulnerability and risk assessment, together with a set of preferred design criteria. Such guidance would also help other W3C working groups conduct their own privacy reviews.

This submission is provided by Christine Runnegar and Tara Whalen in their capacity as PING co-chairs.
22 October 2012

Identifying potential areas of new work

Discussions in PING have, to date, identified two key areas of potential new work:

- Fingerprinting
  - [for PING] – explaining what is fingerprinting, the challenges and best ways to mitigate fingerprinting while still allowing for greater integration and functionality
  - [for others] – develop a standard anonymous fingerprint
  - [for others] – develop ways to expose fingerprinting (e.g., make it easier for the browser to detect fingerprinting)
- Privacy indicators for the browser

Questions for the workshop:

- What are known privacy vulnerabilities and risks associated with Web standards?
- What should we do about them?
- What privacy design principles make sense for the Web?
- How do we ensure privacy concerns are raised at an early stage?
- How do privacy standards work and privacy regulation interact (or should interact)?
- When and how should privacy reviews be conducted? How will the reviews be recorded?
- How will conflicts between privacy and functionality, usability, security, reliability, etc. be resolved?

[i] http://www.w3.org/2011/07/privacy-ig-charter
[ii] Please see the informal chairs' summaries at:
http://lists.w3.org/Archives/Public/public-privacy/2012AprJun/0065.html
http://lists.w3.org/Archives/Public/public-privacy/2012AprJun/0083.html
http://lists.w3.org/Archives/Public/public-privacy/2012JulSep/0004.html
http://lists.w3.org/Archives/Public/public-privacy/2012JulSep/0019.html
http://lists.w3.org/Archives/Public/public-privacy/2012JulSep/0053.html
http://lists.w3.org/Archives/Public/public-privacy/2012OctDec/0001.html
[iii] http://www.w3.org/2012/09/sysapps-wg-charter.html