# W3C Workshop on Privacy and User–Centric Controls (Berlin, 20-21 November 2014)

## Expression of interest (Christine Runnegar, as a co-chair of the W3C Privacy Interest Group (PING))

The Privacy Interest Group (PING) is chartered " … 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".

One aspect that is directly relevant to this work is – What design guidelines should the W3C adopt with respect to "user control" over data collection and handling in W3C specifications?

Practically, what does "user control" mean in this context?

Or, put another way, what minimum elements must be present to enable a user to exercise at least some measure of control?

These might be:

- choice (i.e. more than one available option)
- user understanding of the implications of his or her choice
- user trust in the site/app asking the user to exercise his or her choice
- the ability for a user to communicate his or her choice ("permission")
- the ability for a user to change his or her choice ("revoke/change permission")
- the ability for the implemented specification to carry out the user's choice
- the ability for the user's choice to persist or not persist (as appropriate)
- the ability for the implemented specification to communicate to the user what choice has been exercised
- the ability for a user or a third party such as a regulator or researcher to detect whether the choice is being honoured ("the ability to check compliance")

Perhaps the hardest element to achieve is: "user understanding" – i.e. where users are able to make informed choices that suit their needs and expectations, in terms of both functionality and privacy. And, while the totality of "user understanding" may be beyond the scope of Web specifications, maybe there are components that could be included to facilitate implementations that strive to achieve this goal (e.g. a mechanism that would allow implementers to explain why data is needed.) Further, perhaps some components could be standardised (e.g. a browser-based permissions manager).

Similarly, user trust in the origin is heavily dependent on implementation, but again, perhaps there are ways to improve the integrity of the origin and its data requests through the specification. One such idea, that has been raised in a couple of W3C working groups and will be discussed at TPAC, is the notion of "authenticated origin"[1].

Finally, an overarching consideration in this discussion are the privacy and security considerations of the specification, and how they are handled. In this respect, PING is developing guidance for Web specification authors on how to incorporate privacy in the design of Web standards. This workshop offers an opportunity to discuss some of the current thinking in this area.

[1] See, for example: "An origin can be called authenticated when it either refers to a source which is impossible not to trust (e.g. localhost), or to a source which can be adequately verified as authentic."
from http://w3c.github.io/webappsec/specs/mixedcontent