Position Paper for W3C Workshop on Web Tracking and User Privacy

Li Li, Wu Chou

Avaya Labs Research, Avaya, USA

Web privacy and tracking protection technologies will have impact to enterprise applications, as more and more enterprise applications are based on the Web infrastructure and technologies. In a typical scenario, a user on the enterprise Intranet would use the same Web browser to access both internal and external Web sites. It may be unrealistic or inconvenient to ask a user to change the Web browser settings on the fly based on which site to visit. Therefore, settings of the Web browser are likely to be shared internally and externally.

For this reason, a global binary “Do Not Track” option applicable to all Web sites may not be suitable for enterprise applications, as enterprise needs to track the use of the information on the Web for reasons such as security and service quality. Such a binary option in the browser may disable an internal Web site that uses Web tracking technologies to improve organizational productivity. For example, an internal Web site may embed a Web beacon from an enterprise tracking service to collect an employee’s online activities, while at the same time, the employee does not want to be tracked by any external advertisement site. It is possible that this tracking service is deployed in a trusted third party domain outside the enterprise Intranet or in a hosted cloud. In any case, when the employee turns on “Do Not Track” in the Web browser, both the unwanted and wanted tracking will be blocked.

We hope Web browser vendors can adopt a privacy framework that allows for finer-grained tracking control, such that enterprise privacy policies along with personal preferences can be both incorporated in a Web browser. We think the Tracking Protection List (TPL) introduced by Microsoft IE9 [1] is a good starting point. In addition, we think it is useful to have two levels of tracking controls, one for enterprise policies, and one for personal preferences.

It is possible to enforce enterprise policies at a HTTP proxy shared by the browsers. However, many Web browsers do not use a proxy at all for performance reasons. A transparent proxy can enforce enterprise tracking policies without any browser configuration.

However, in reality, it needs to enforce the tracking polices in the presence of personal preferences, and personal preference may block the enterprise tracking polices if they are deployed on the proxy, including transparent proxy. For example, if the personal preferences block a tracking site xyz.com, but tracking polices deployed at the proxy allow it, then the site will still be blocked if the browser does not send any request to the proxy. For these reasons, a browser-based configuration is a more attractive solution.

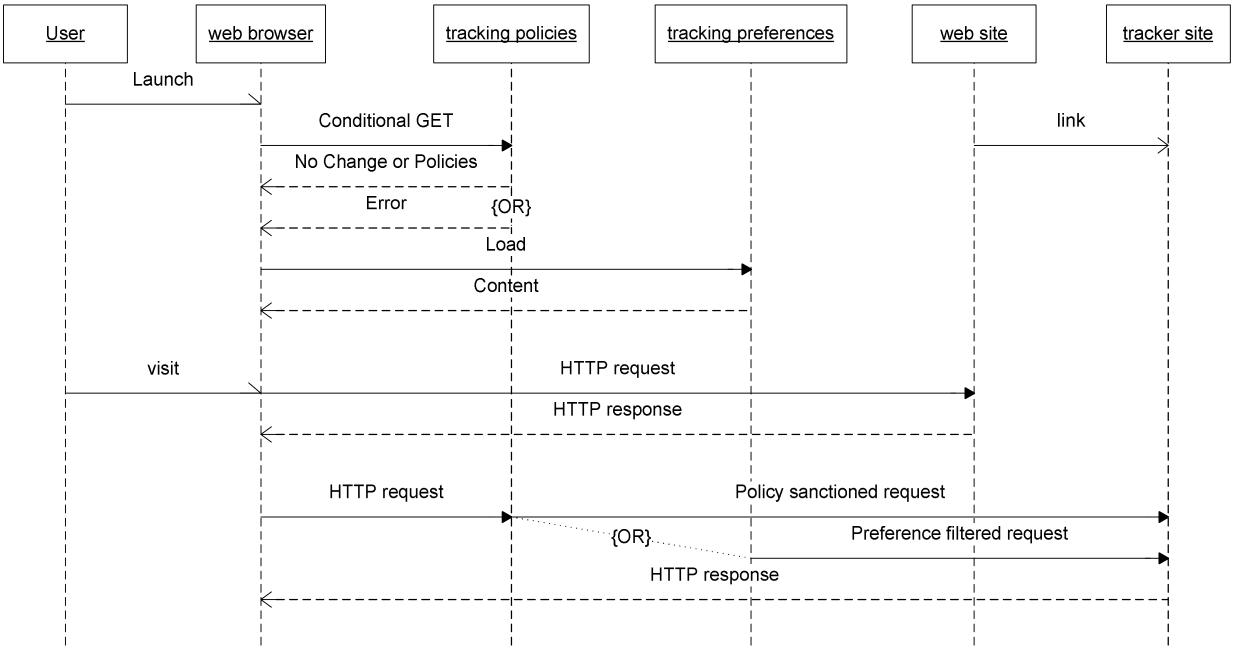
To realize such a solution in browser, the enterprise tracking policies, whenever available, will have precedence over the personal ones. Combined with “Do Not Track,” this leads to a layered tracking protection approach against a tracking site as follows:

1) if it is in enterprise policies, then use the matched policy; otherwise,
2) if it is in personal preferences, then use the matched preference; otherwise,
3) use the "Do Not Track" option.

The enterprise tracking policies are specified in a XML file located in an internal enterprise Web server only accessible on the enterprise network, possibly through VPN. This file is managed by authorized administrators and can be consulted by a Web browser using HTTP GET to that URL. The personal privacy preferences are managed by a user through the Web browser interface.

As notebook computers and smart phones can move in and out of an enterprise network, the enterprise tracking policies should be activated or deactivated accordingly. This process can be automated by a Web browser sending a Conditional HTTP GET to the tracking policies URL at the browser startup time. If this Conditional HTTP GET request succeeds, then the Web browser is inside the enterprise and on the enterprise Intranet. Otherwise, the enterprise tracking policies are not consulted and only personal preferences are used.

The flow diagram of this approach is depicted below that illustrates the interactions between each related components, where "Do Not Track" option is treated as part of the tracking preferences.



The advantage of this approach is that the applicability of tracking policies is managed automatically by a browser during the browser startup time. A disadvantage is that it may increase browser startup time, as it needs to do a Conditional HTTP GET for enterprise tracking policies. But this occurs only once at the time when the browser starts up.

To ensure the interoperability between Web browsers and tracking controls (XML files), tracking controls should be standardized. The standard should enable the switch of Web browser while maintaining the tracking preferences systematically without ad-hoc translations that might introduce inconsistency. As an advantage of the described approach, there is no need to import enterprise tracking policies except passing the enterprise tracking policies URL, as enterprise tracking policies are automatically loaded when the browser starts up inside the enterprise.

[1] http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx