The Internet Society works to ensure the continued existence of a healthy Internet ecosystem. This includes support for multi-stakeholder activities that are open, inclusive, and generative. Key to this effort is the need to understand the complex balance between issues such as privacy, security, and reliability. When balanced properly, the result is a trusted network in which all participants, including users, enterprise and governments, have confidence using.

The organic growth of the Web as an effective means of communication over the Internet has given rise to uses of the technology that go beyond what was initially intended. Each innovation has provided the opportunity for both positive and negative, often unintended, consequences. One such set of trade-offs can be found in the pervasive use of mechanisms deployed to track users across the Web.

When a user directs a web browser to a specific site to request a page of content, there is a general (though often vague) understanding that the data between the end points moves through an unknown number of intermediaries (e.g. routers). Users, however, often operate with an implicit expectation that the persistent details of their interaction are limited to the two end points (i.e. the user and the known server). This is in strict contrast to the current norm in web browsing: each site often logs page content being retrieved, and a page is often a composite of content served from a number of additional end points (a.k.a. "third parties"). Each of these end points, in turn, is able to track various details regarding the user (e.g. their browsing, IP-based geo-location, etc.).

Increasing reliance on the Internet and related tools, such as the Web, is catalyzing demand for harmonized and interoperable privacy and data protection. A key component of the approach is the development of international legal frameworks. As part of this effort, policymakers are looking to technology, industry codes of conduct, certification schemes, and user education to compliment the emerging frameworks. [i]

Web tracking is receiving particular attention. For example, the Preliminary Federal Trade Commission Staff Report (December 2010) entitled *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers*[1] states, among other things:

> … Commission staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as "Do Not Track." Such a universal mechanism could be accomplished by legislation or potentially through robust, enforceable self-regulation. The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those choices.
>
> Such a mechanism would ensure that consumers would not have to exercise choices on a company-by-company or industry-by-industry basis, and that such choices would be persistent. It should also address some of the concerns with the existing browser mechanisms, by being more clear, easy-to-locate, and effective, and by conveying directly to websites the user's choice to opt out of tracking. …

Supporting these efforts, research shows that users frequently respond to survey questions stating they do not want their browsing data to be collected without their knowledge and consent. A common conclusion from many surveys (including ones from The Annenberg Public Policy Center at the University of Pennsylvania, The Samuelson Law, Technology & Public Policy Clinic at UC Berkeley, and The PEW Internet & American Life Project) is that users want more transparency about data being collected, its use, and to have more control over it.

[1] http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

Missing from the analysis of these surveys, however, is consideration of how users expect to effectively balance all of the related issues around increased privacy controls. It is unclear how users will react when privacy is increased with a related impact on security, usability, and reliability. Historically, when considering adoption of security technologies, average users opt for the simplest experience, even when it is the least secure.

To fill out the picture further, there are various reasons to employ mechanisms for tracking Web users. There are also various methods by which users can be tracked. Some methods include cookies (browser-based or managed by add-ons such as Adobe Flash), others rely on browser fingerprinting (i.e. using unique characteristics in response headers), while still others leverage network and device characteristics (e.g. IP addresses and MAC identifiers).

Regardless of the reason for tracking users or the method used, tracking falls into one of two classes:

- **Single-Site Tracking** – There is a "first-party" relationship between the user and the known site. Activities are being tracked, sometimes unknowingly, but the resulting data is managed for the use of the site itself.

- **Multi-Site Tracking** – In contrast to single-site tracking, users are tracked across sites and by multiple sites. This introduces one or more third parties to the interaction between the user and the known site.

A common use of tracking for a single site is to observe and monitor the interactions of users within their service. A goal is to compare similar users in an effort to personalize the user experience on the site (a.k.a. "behavioral profiling"). Another related use is to improve the effectiveness of display advertising by observing and analyzing user patterns across multiple sites (a.k.a. "behavioral advertising"). In addition to content and service delivery, another common use of tracking is to improve security by monitoring user activities (e.g. building behavioral risk profiles).

Some consideration should also be given to differences between tracking methods used within the context of browsing activities and those used for the business of brokering user data. In one case, regardless of how the tracked data is collected (on a single site or across multiple sites), it is analyzed and used only by the collector and its agents. In other cases, the collector may share with or sell to other (often undisclosed) parties (a.k.a. second parties) the data that is collected. It is important when considering issues around tracking users to be aware of both modes, understanding that they may also work in conjunction.

Given the rapid expansion of the Web into all aspects of daily life, it is clear that issues of online privacy need to be addressed, while not adversely affecting the overall utility of the Internet. Protecting user privacy online cannot be taken lightly, and requires well-considered solutions that are open, transparent, and inclusive.

This paper was prepared by Christine Runnegar (runnegar@isoc.org) and J. Trent Adams (adams@isoc.org) for the purpose of participating in the W3C "Workshop on Web Tracking and User Privacy" at the Center for Information Technology Policy at Princeton University in Princeton, NJ, USA (28-29 April 2011)

_____

i. Some examples of recent international and regional privacy initiatives:

The OECD "is preparing an anniversary report on the evolving privacy landscape" (see http://www.oecd.org/document/35/0,3746,en_2649_34255_44488739_1_1_1_1,00.html)

In Europe, the Council of Europe is considering how to modernize the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108) (see http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp) and the European Commission is in "… the process of reviewing the general EU legal framework on the protection of personal data" including *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (see http://ec.europa.eu/justice/policies/privacy/review/index_en.htm).

APEC economies, through the APEC Data Privacy Pathfinder, are "… develop[ing] and test[ing] the essential practical elements of a system that would enable accountable cross-border data flows under the guidance of APEC data privacy principles" (see http://www.apec.org/en/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx)

In 2009, the 31st International Conference of Data Protection and Privacy Commissioners produced a *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data* ("the Madrid Resolution") (see International Standards on the Protection of Personal Data and Privacy at http://www.justice.gov.il/PrivacyGenerations/adopted.htm).

In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a *Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data* (see Resolution on International Conference at http://www.justice.gov.il/PrivacyGenerations/adopted.htm).