An Argument for a Holistic Approach to User Consent & Consumer Control

Brad Kulick, Sr. Director of Privacy, Advertising and Analytics, Oath
Wendell Baker, Distinguished Architect, Targeting & Identity, Oath

Oath is home to media, tech, and communication brands that 1 billion people use on a regular basis. Some of Oath's largest brands like Yahoo and AOL have ties to the nascent days of the Internet. This success is due in large part to the respect and attention that Oath, and its predecessor companies have paid to user privacy and choice. Indeed Oath and its precursors have helped to drive many industry privacy initiatives, including the formation of self-regulatory bodies and guidelines for the appropriate handling of user data. And yet, it is becoming increasingly difficult to achieve safe, legal, consumer facing experiences using the modern web technologies.

Oath primarily provides services that users access via their browsers on personal computers or "smart" personal communication devices. Oath products are built at the application layer and respect the browser's user experience choice settings in addition to supporting further levels of consent and control at the service level for registered users. It is at the intersection of the application function and the constrained browser affordances that challenges are beginning to arise. Significant amounts of technical effort are spent assessing and working in and around the constraints of present-day standards-based web technologies.

A commonality among many of the problems that Oath and other media, tech, and application service providers encounter within the Internet ecosystem revolve around the fact that as web-based technologies evolve and mature, they are not always sufficiently respecting of existing stakeholder expectations. The ripple effects of the evolution forces companies with web-based businesses to spend unnecessary cycles and resources to re-establish acceptable and previously-working mechanisms to operate the core services that they provide to consumers.

We have some modest suggestions which we believe would dramatically enhance the efficacy of standards-based web technologies in support of consumer privacy, safety and ease of use not to mention the benefits of simplicity and engineering efficiency. These are:

Client-Stored State: While the Same Origin Policy has served well to sandbox applications from each other within the multi-tenant environment of The Web Browser, the mix-and-match nature of web media and web applications suggests that there might be another way to share state across isolation boundaries. The Domain Name Service namespace is the basis of the Same Origin Policy (SOP), but that boundary becomes a limitation when companies with branded identities tied to those names merge, split, rebrand, or simply wish to cooperate. It is

common for a group of consumer-facing service companies to wish to form a cooperative or pool to share information between themselves and with a consumer to whose benefit they operate. Perhaps some other mechanism for cross-domain application permissioning is more appropriate than the SOP. The use of similarly-signed certificates is a technique which has found success in the non-browser application space.

Tracking, Analytics and Tracking Protection: Affordances for consumer-level control of data usage was first presented in the W3C context as Do Not Track (DNT). However, after five years within W3C, critical mass for adoption did not arise, despite it being the strongest technical option to support GDPR consent requirements. Instead, industry having need of a solution on time, developed the Transparency and Consent Framework (TCF). This solution is limited, is standards-based only within a single industry and does not take advantage of Web Standards at large. One could imagine such capabilities being a normal part of a standards-conformant browser implementation.

Pseudonymous Identification: Today much effort and is spent in developing pseudonymous identifiers and in synchronizing very large databases of such identifiers among commercially cooperating companies and consumers. Elsewhere, outside of the standards-based Web, “in Apps”, there is a single unique identifier which offers consumer-facing control of the pseudonymous identification capability. The Web would be a very different place of these facilities were brought front-and-center into the conformant Web Browser. What if The Web had a device-level identifier (a “advertising identifier”) like the IDFA or GPSAID? What if it were available from the JavaScript APIs and controlled by browser-native UX?

Oath looks forward to cooperating with others to build a foundation to develop standards-based solutions across the Internet ecosystem.