The Chained Identity Systems of Online Entertainment

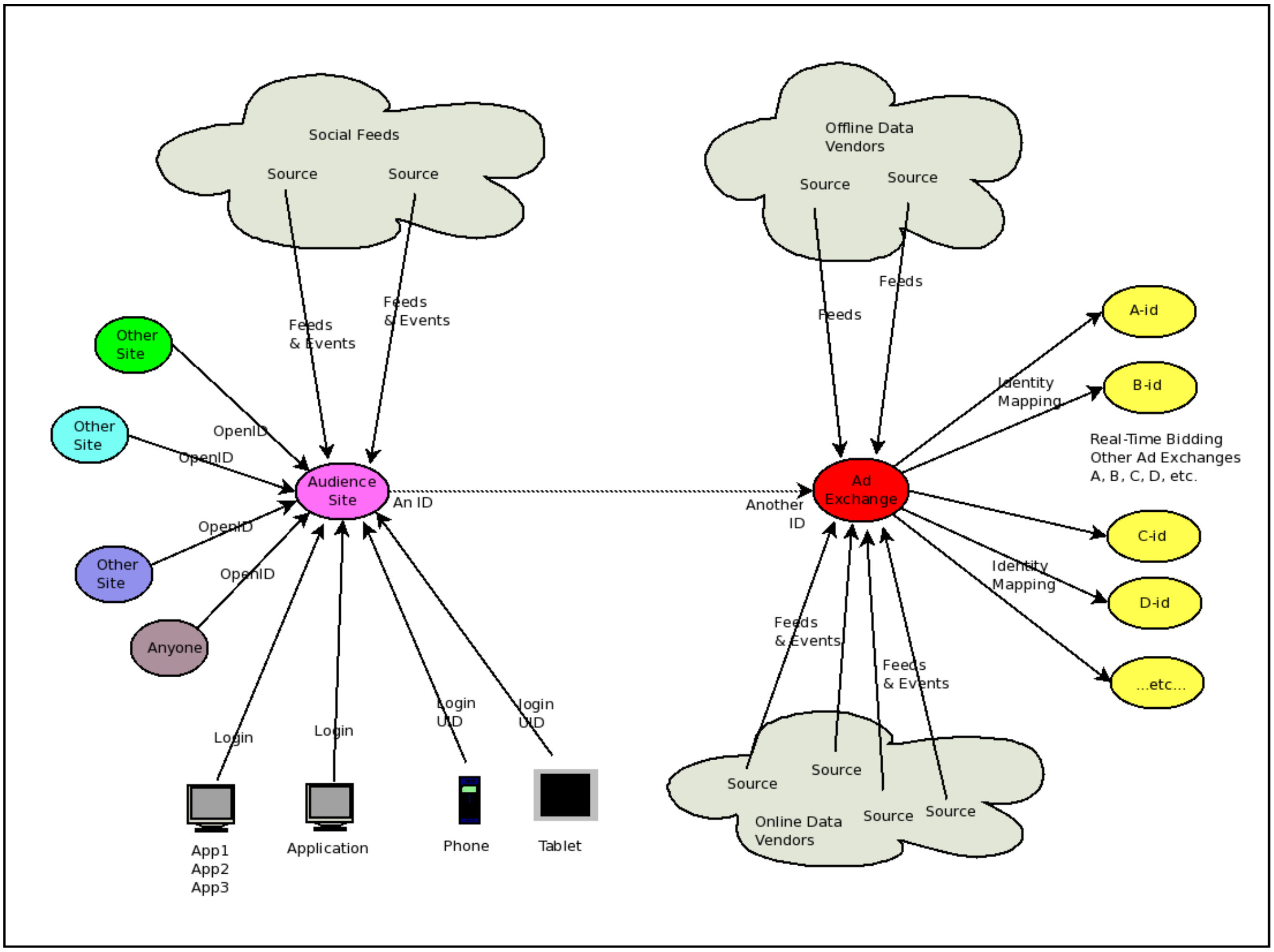
Wendell Baker
Architect, Non-Guaranteed Ad Serving
RightMedia from Yahoo!, Inc.
Santa Clara, CA 95054

Online experiences are expanding and generalizing as richer and more meaningful real-world interactions are connected to, enhanced by and created within computer-based media. This is occurring in both the pragmatic commercial and the open-ended entertainment domains. In either case a linkage is made between a real person, on whose behalf these systems operate, and the resources in whose name the claims on the system are made. This is the realm of *identity* management. Within this scope, the key questions, as online systems proliferate, are how shall identity be managed, created, destroyed, modified, and whether tools and workflows can simplify these tasks.

There is an obvious opportunity here to build identity management directly into the predominant mediator of the online experience: “the browser”. The proposition here is that an identity manager capability built into the JavaScript+HTML document reading apparatus may offer some limited short-term remediation for the plethora of identities and credentials (better known as 'usernames' and 'passwords'). However, there are significant and increasingly important applications of online services that don't involve “a browser” or even “the browser” as a unique or available choice. These use cases are of increasing importance in next-generation computing environments: mobile devices, connected devices, cloud-based and peer-to-peer applications.

There is an additional dimension to the problem domain which is present in online entertainment systems as we know them today. It is from this perspective of the online entertainment provider that we can draw insights as to the proper long-term location for the identity management infrastructure in the service architecture. The business model for online entertainment systems broadly has two competing goals: audience gathering and promotional content delivery. Both need to be executed well, with individual user experiences in mind, with monetization capabilities in mind and with applicable nonfunctional aspects such as regulatory compliance, privacy, measurability, efficacy, brand safety, and so forth supported. Because of these competing goals, in present-day architectures there are typically two parallel identity systems: the audience-side system (membership) which is the one you login with, and the advertising one which is used by the content selection algorithms and ties to both the present-day generation of Online Behavioral Advertising (OBA) interest managers and policy controls such as Do Not Track (DNT). We can refer to the audience side identity system a *voluntary* identity system as it works on behalf of the user. The advertising identity system can be thought of as a *force-placed* identity that acts on behalf of the entertainment network to mediate the accounting of user experience in the monetization dimensions and secondarily to register user policy declarations such as “opt-in,” “opt-out” or “Do Not Track.”

Providing an identity manager concept within “the browser” offers a direct solution to the problem of remembering a username and password combination for a single browser instance at a web site but does little to support the management of voluntary identity across different browsers on different devices or across non-browser applications. Else one has to believe that synchronizing one's username, password and interest portfolio *in toto* “across the cloud” between browsers, among vendors, and across software generations is feasible and safe. When sourced from within the browser, a primary identity definition is not portable across the full experience. Quirks and feature omissions invariably will corrupt the smooth application of credentials and policy among the services and among the client-side access methods. In addition, browser-defined identity does not address the identity chaining which is currently occurring as a defined and expected behavior of entertainment systems. Identity chaining occurs between systems due to both the active, voluntary, social sharing of the user population and the background bookkeeping activities of the monetization systems. The following diagram illustrates many of the chains of identity that support online entertainment systems.



The identity ecosystem from the perspective of an online entertainment provider typically consists of an audience side and an advertising side. The audience side of the house creates experiences that are fun to play and encourage the users to return to the site. The advertising side is often a key aspect of the monetization strategy for the service even if it is used to augment subscription or other business models. At this level of detail, one can envision support for “fully anonymous” or “unregistered” users being supported through the ephemeral assignment of a hidden identifier which is used for the duration of the session. The current structure of the online entertainment industry maintains both of these systems in parallel though that is changing.

Audience sites typically manage user identities using a "screen name" or "email provider" approach. This works well, from the perspective of the service, to nominate the person sitting behind the program or device that is contacting the service. Name choice has a substantial personal choice component to it and the visible symbol of the name becomes part of the online persona. This works well when "the browser" is the only interface to the site. However, with the rise of embedded services, devices and the "app" economy (installed-on-client programs that are not obviously a JavaScript-enabled HTML browser) there is interest in identifying the device or application and the user behind the application as separate entities. Also, to ease the burden of the “sign on” process, audience sites are increasingly finding ways to chain identities together using open protocols such as OpenID or by other means such that registration credentials are passed or delegated to affect a flavor of “single sign-on.” This identity management machinery is characterized by its explicit, active and voluntary nature. Identity chaining in this sense facilitates activities of direct and immediate benefit to users: accessing the service. Providing explicit support within an HTML+JavaScript browser to facilitate username+password memory or to enable identity chaining across service providers has benefit, but it is not a complete solution to principled identity management in the online realm.

In parallel with the audience side membership apparatus, there is frequently a separate identity system which is used for the fine-grained bookkeeping needed for the performance and monetization systems that support the entertainment service. In the monetization context, user identity and the user's associated attributes are a key component in the definition of the advertisement system's *opportunity to display* event; others are the publisher constraints and the current contextual environment which are not relevant here. There are legitimate and important user experience and policy reasons why the audience-side and advertising-side identity systems ought to be linked together. Frequently though they exist as unlinked, wholly independent, systems. They may be operated by separate organizations as is the case with a merchant advertising platform. The monetization side typically assigns and maintains user identities in its own interest using a "force-placed" approach where the focus is on unmanaged and self-correcting operation. These identity stamps are generally not shared between systems unless there are careful, principled, bilateral arrangements in place to protect both user privacy and also the publisher's rights in the data. In such cases, the user identity stamp is typically transformed (cryptographically hashed) when the opportunity is offered on a different marketplace. This is represented in the diagram by the linkages between the red and yellow bubbles. This indirect association preserves the privacy of the user base and while ensures that the publisher's data rights are preserved. Engineering and business concerns govern whether the user mapping table is stored in the local or remote marketplace; that is, in the red bubble or each of the yellow bubbles separately.

The proposition at hand is whether and to what extent a first class “identity manager” in the next-generation web browser would solve an outstanding problem or provide a useful extension to existing practice. By walking through the linkages between the identity systems that span an online entertainment service provider, one can observe a range of interface devices and styles and a range of concerns that would intersect with such a capability. On the audience side, some of the concerns and interface types would be well served by the existence of such a capability. The act of “signing in” is nowadays a fundamental part of the online experience and having browser-to-server support for that activity would be a good thing for safety and ease of use. A “manager” concept in the browser could provide some benefit towards controlling the thicket of usernames, passwords and preferences that greet the user. A “manager” concept could also help in the chaining between different identity domains using open protocols. However, there are other aspects which are not and could not be addressed by such a facility. The next-generation online experiences mediated by apps, tablets, phones and TVs will not necessarily have sufficient interface power or scope to manage primary or multiple identities. They will necessarily work against narrower experience expectations. As well, the normally-invisible identity management systems in the monetization side will still not be linked in with this “identity manager” so the need for separate interest, policy and preference managers would remain.