Considering Browsers' Role in a User-Centric Online Identity Ecosystem: Privacy and Context

W3C Workshop on Identity in the Browser
May 24-25, 2011

Aaron Brauer-Rieke
Center for Democracy & Technology

Browsers might help move us toward a user-centric identity ecosystem that enhances user privacy, security, and convenience. We summarize the current online identity landscape, outline privacy principles, and contextualize the browser's role in online identity management.

---

1. Introduction and Summary

Our reliance upon Internet transactions continues to grow. Unfortunately, management of our online identities remains remarkably inadequate. We are prompted to create redundant online accounts and juggle myriad passwords. This state of affairs causes not only notable inconvenience[1] but also security risks[2] and privacy concerns.[3] There is a growing recognition that a more robust and elegant solution to online identity is desirable. This notion was most recently endorsed by the United States' National Strategy for Trusted Identities in Cyberspace (NSTIC).[4]

The browser is an important gateway between users and the web, and a persistent user interface. Accordingly, browsers are likely to play some enhanced role in the management of online identities. Recognizing the browser's potential importance, this paper provides context and privacy guidance to help frame this workshop's discussion of "identity in the browser."

2. The Current Identity Landscape

Today's Web is site-centric as opposed to user-centric. This means users typically have to obtain separate accounts and credentials for each online service they use. It is not difficult to

---

[1] *See, e.g.,* Yuki Noguchi, *Access Denied*, THE WASHINGTON POST, September 23, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/09/22/AR2006092201612_pf.html (discussing password fatigue and attendant security risks).

[2] Researchers have "observe[d] numerous ways in which the technical failures of lower-security sites can compromise higher-security sites due to the well-established tendency of users to re-use passwords." Joseph Bonneau & Soren Preibush, *The Password Thicket: Technical and Market Failures in Human Authentication on the Web*, THE NINTH WORKSHOP ON THE ECONS. OF INFO. SECURITY (WEIS 2010), at 1, *available at* http://weis2010.econinfosec.org/papers/session3/weis2010_bonneau.pdf.

[3] The relationship between identity and privacy is a nuanced one. On one hand, fraud detection systems that rely on identity and transaction information might protect users. However, the sharing identity information with a multitude of parties that do not properly secure it increases privacy risks.

[4] National Strategy for Trusted Identities in Cyberspace, April 15, 2011, *available at* http://www.nist.gov/nstic/strategy.pdf.

envision a better way. For example, one approach with potential is the U.S. federal government's recently-released National Strategy for Trusted Identities in Cyberspace (NSTIC). The Strategy offers an ambitious vision for online identities: "Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."[5] This vision recognizes that creating a robust online identity ecosystem can be empowering and convenient for users, improve security, and fuel commerce—all at the same time. The Center for Democracy & Technology (CDT) has endorsed the NSTIC vision while recognizing its proper implementation will be difficult.[6]

Making this vision a reality will be difficult, especially at higher levels of assurance. Simply put, we have yet to achieve consensus on the necessary rules and tools. Rules—e.g., those pertaining to privacy, liability, proofing, and security—are necessary to ensure that an identity platform functions in a reliable and desirable fashion. Tools—e.g., protocols, user agents, digital certificates, encryption; the *technology,* generally speaking—are necessary for the system to run securely and to ensure the user can make sense of it all. An Internet-scale identity ecosystem demands significant progress on both fronts.

Despite some promising efforts, a true user-centric identity *ecosystem*—i.e., an environment in which multiple, interoperable identity providers and relying parties interact—has yet to emerge, even for casual Web services. For example, the OpenID Foundation claims there are more than a billion OpenID enabled user accounts through major identity providers (e.g., Google, Yahoo, Facebook).[7] InfoCard has proposed a promising interface to manage online identities including conscious presentation and unlinkability between an identity provider and relying party.[8] However, these solutions have not enjoyed mainstream adoption.[9] The reasons are numerous and capably discussed in other literature: a lack of incentives for relying parties to adopt user-centric identity solutions, a lack of a consistent and intuitive user experience, and a lack of viable business models for identity providers.[10] Privacy concerns (such as tracking by consolidated identity providers) and security concerns (such as increased exposure to phishing attacks) also loom.[11]

However, there have been some recent successes, most notably Facebook Login. Today, Facebook is easily the most prevalent third-party identity provider among popular websites.[12]

---

[5] *Id.* at 15

[6] Press Release, Center for Democracy & Technology, White House Rolls Out Strategy for Trusted IDs in Cyberspace, April 15, 2011 *available at* http://www.cdt.org/pr_statement/white-house-rolls-out-strategy-trusted-ids-cyberspace. *See also* Leslie Harris, President and CEO of the Center for Democracy & Technology, *National Identity Strategy Envisions a More Trustworthy Internet*, The Commerce Blog, April 15, 2011, http://www.commerce.gov/node/12919.

[7] *See generally* The OpenID Foundation, http://openid.net/foundation/ (last visited April 27, 2011).

[8] *See generally* The Information Card Ecosystem, http://informationcard.net/ (last visited April 27, 2011).

[9] For example, "[a] recent search found only 882 RPs on OpenID directory . . . . [an] adoption rate of less than 0.02%." Sun, et. al., *A Billion keys, but Few Locks: The Crisis of Web Single Sign-On*, July 19, 2010 *available at* http://lersse-dl.ece.ubc.ca/record/244.

[10] *See generally, id.*

[11] *Id.*

[12] Of the most popular 100 websites (based on Quantcast's ranked list of U.S. sites as of July 8, 2010), 82 provided functionality for a user to "sign-on." Of the 82 sites providing sign-on functionality, almost exactly half, 42,

While logged into Facebook, its users can authenticate with third-party websites and enjoy the social features of Facebook integrated with the third-party site. Facebook overcomes some of the hurdles described above by providing incentives for relying parties (who are likely attracted to the exposure on Facebook's social network) and a familiar user experience (many users understand that they already have a Facebook account and recognize the login button). Unfortunately, Facebook has yet to provide accountable data minimization practices (relying parties frequently request more data than that required under the "need to operate your application" standard) and is unclear regarding its use of users' transactional data.

Establishing a true identity ecosystem, such as that envisioned by NSTIC, requires recognition of these challenges and successes.

3. Privacy Principles for Identity Systems

All identity-related systems should support the user's enhanced control, security, and privacy. Accordingly, we offer the following set of principles to guide discussion of the browser's role. The principles below are drawn from CDT's "Privacy Principles for Identity in the Digital Age" white paper.[13] They are divided between three "overarching principles" that address the identity ecosystem as a whole and a number of more specific principles drawn from the Fair Information Practice Principles (FIPPs).

Overarching Principles

Diversity and Decentralization: Online identities should function like keys on a ring, with different identities (and, ideally, different identity providers) for different purposes. It is not optimal to overly-centralize identity information or use a single credential for all purposes.

Proportionality: The amount and type of information collected from individuals by an identity system should be proportional to the purpose for which it was collected.

Privacy and Security by Design: Privacy and security considerations should be incorporated into identity systems from the outset of the design process.

FIPPs-based Principles

Purpose Specification: The first step in designing an identity system should be to specify the purpose of the system and the purposes for which identity information will be collected and used.

---

accepted attributes from a third-party identity provider. Facebook was easily the most prevalent identity provider, in this set with 82.5% (33) sites supporting Facebook Login. More than half of these sites (55%, 22) featured Facebook as the exclusive third-party identity provider.

[13] Center for Democracy & Technology, Privacy Principles for Identity in the Digital Age, December 1, 2007 *available at* http://www.cdt.org/report/privacy-principles-identity-digital-age.

Limited Use: Identity, authentication, and linked information should be used and retained only for the specific purposes for which they were collected.

Individual Control and Choice: Whenever possible, an identity system should offer individuals reasonable, granular control and choice over the attributes and identifiers needed to enroll in the system and the credentials that can subsequently be used within the system.

Notice: Individuals should be provided with a clear statement about the collection and use of identity, authentication, and linked information.

Security: Organizations that handle identity, authentication, and linked information should provide reasonable technical, physical, and administrative safeguards to protect against loss or misuse of the information.

Accountability: Organizations that handle identity, authentication, and linked information should be able to verify that they are complying with applicable privacy and security protections.

Access: Individuals should be provided reasonable access to the identity, authentication, and linked information that organizations maintain about them and use in the ordinary course of business.

Data Quality: Organizations should strive to ensure that the identity information they hold is timely, complete, and accurate.

4. Contextualizing the Browser's Role

Browsers are today among the most important consumer-facing Internet tools. Indeed, most browsers "help out" with identity management already. For example, browsers offer to remember and automatically supply usernames and passwords on behalf of their users. Browsers also handle cookies that maintain authentication states and support TLS to encrypt traffic. However, this workshop seems to contemplate a more proactive and comprehensive role for the browser in the management and presentation of online identity.

There are many different ways to envision "identity in the browser." At one end of the spectrum, browsers might actually store and present identity credentials (e.g., tokens) or interact with hardware trusted platform modules (TPMs). Alternatively, we might imagine a "lighter touch" where a browser provides a user interface (UI) to assist users with the management of third-party identity solutions. At the other end of the spectrum, browsers could simply retain their familiar role today. This paper remains largely agnostic regarding these implementation strategies, the merits of which will vary significantly depending on technical details. We encourage further discussion of their relative strengths and weaknesses in this workshop and elsewhere. Of course, any implementation should square with the privacy principles laid out above.

In considering browsers' role in an identity ecosystem, it is vital that browser developers move away, at least in this context, from the historic web-based paradigm in which most policies are set by a visited website, and a web visitor is largely in the position of "taking or leaving" the rules and policies set by the website. In the context of identity, it will be essential that the user is truly in control and able to provide the identity (and thus the level of information) of the user's choosing.

5. Conclusion

CDT encourages browser developers and the W3C to explore ways to assist users in creating, maintaining, and presenting digital identities. In any implementation, a central design requirement should be that users are given true and robust control over their identities.