2010

The Trouble With Logins: The Challenges of Online Identity

Steven Ovadia
CUNY La Guardia Community College

Behavioral & Social Sciences Librarian, 29:296–300, 2010

ISSN: 0163-9269 print / 1544-4546 online
DOI: 10.1080/01639269.2010.521046

Routledge
Taylor & Francis Group

INTERNET CONNECTION

The Trouble With Logins: The Challenges of Online Identity

STEVEN OVADIA
LaGuardia Community College, Long Island City, New York

Most librarians have had the experience of a patron coming to the reference desk, asking for help trying to get into some account to which the person has forgotten the login and/or password. It could be a personal e-mail account. It could be the campus course management system. But whatever the service, the patron cannot log in. And often at some point in the reference transaction the patron will express frustration at all of the logins and passwords he or she needs to remember.

Just about every personalized or semipersonalized Web service requires some sort of login. While certain suites of services, like Zoho or Google, can use one login for different types of services, like e-mail or document creation, most times, when a user is accessing different Web services across different companies or organizations, separate logins and passwords are required. Obviously, users can try to use the same login and password for all of their online services, but that isn't always feasible, given login name limitations and password syntax rules. Also, there's no way to change a password across services, so unless a user is very disciplined in her login/password choices, eventually credentials can become out of sync with each other. Most users have resigned themselves to dealing with multiple logins and passwords in whichever way best makes sense for them. But this raises the question of whether online identity needs to be such a complicated prospect.

In some ways it does need to be a complicated prospect because online identity is a complex thing, riddled with security and privacy concerns. But there are some online initiatives that are trying to simplify the world of logins and online identities.

The most common and perhaps mature solution is OpenID, an open-source, nonproprietary authentication mechanism that lets users create one

Address correspondence to Steven Ovadia, Library Media Resources Center, LaGuardia Community College, 31-10 Thomson Avenue, Long Island City, NY 11101. E-mail: sovadia@lagcc.cuny.edu

login and password that can be used across different sites (Mills 2008). Many commonly used services, like AOL, Flickr, and Yahoo!, allow their login information to be used as an OpenID (OpenID n.d.). Because OpenID is nonproprietary, different Web services can opt in to either accepting OpenID credentials or providing the credential.

If you have not heard of or noticed OpenID around the Web, it's because it's still not universally accepted. Even sites that accept OpenID do not always make it readily apparent. OpenID has probably yet to become ubiquitous because of security concerns. Some people consider OpenID too vulnerable to phishing attacks. If exploited, it could become a potential gateway into all of a user's private, OpenID-linked information (Fest 2008, 10).

Still, the idea of an almost magical single sign-on remains attractive to users and to Web providers. Facebook entered the identity management market in late 2008 with Facebook Connect, a service that lets Facebook users login to certain non-Facebook sites using their Facebook credential (Wortham 2010). Like OpenID, the only limit is the participation of the sites in the service. And of course, since this is Facebook, there are always privacy concerns, mainly over whether Facebook can be trusted with private user information (MacMillan 2009).

It seems some people are putting their faith in OAuth (Open Authorization) as an online identity management tool. OAuth is a technical specification that allows users to provide access to personal information, from photos to banking information, without actually revealing password information to a site. OAuth advocates frequently use the valet key metaphor, in that a valet keys allows someone access to a car, but in a controlled and limited fashion (Connolly 2010). OAuth attempts to do the same thing with online identity, providing sites with just enough information to accomplish what the user has requested, but not allowing third-party sites access to any other user information.

Eran Hammer-Lahav, one of the developers who has worked on the OAuth standard, provides a more comprehensive explanation:

> As the web grows, more and more sites rely on distributed services and cloud computing: a photo lab printing your Flickr photos, a social network using your Google address book to look for friends, or a third-party application utilizing APIs [Application Programming Interface] from multiple services.
>
> The problem is, in order for these applications to access user data on other sites, they ask for user names and passwords. Not only does this require exposing user passwords to someone else—often the same passwords used for online banking and other sites—it also provides these [applications] unlimited access to do as they wish. They can do anything, including changing the passwords and lock[ing] users out.

> OAuth provides a method for users to grant third-party access to their resources without sharing their passwords. It also provides a way to grant limited access (in scope, duration, etc.). (2010)

The logistics of OAuth are complex, but conceptually, it's a way for users to provide access to certain parts of their online identities, while not revealing the rest of their personal data or information.

OAuth seems like it might be a specification that could help usher in the era of what David Siegel calls "Identity 3.0" (2009). Siegel outlines quite a few Identity 3.0 principles that third-party access brokers would follow:

- Using the principle of least privilege, meaning both parties to a transaction would reveal information in stages as necessary.
- Helping users and sites engage with others without giving away sensitive information.
- Authorizing third parties to do only the things users want them to do on their behalf and nothing else.
- Helping to prevent phishing, fraud, identity theft, and other common cyber crimes (2009, 107).

Mather also discussed the idea of Identity 3.0, suggesting there might be a need for some kind of external, nontextual verification mechanism, like a video camera (2008). Both Mather and Siegel also explore the idea of multiple online identities. Siegel's vision of Identity 3.0 includes multiple identities, while Mather's concept includes the idea of virtual identity management, like someone's Second Life persona (2008; 2009). That inclusion is interesting from a sociological perspective in that a recent study showed that members of generation X and generation Y struggle with the tension between authentic identities, where one can accurately connect an online identity to an individual, and inauthentic identities that let users experiment with online personas a bit more and in a more low-stakes manner (Yerbury 2010).

Identity 3.0, as imagined by Siegel and Mather, seems to provide a space for identity experimentation, while also providing a mechanism for identity authentication. Because their identity concept provides layers of information to third-party sites, users can, within their proposed framework, manage their "true" identity, and/or experiment with an alternative one. In theory, someone buying a book online could have accurate address information that will allow them to receive the book. But they could also have inaccurate address information linked to another profile/persona that allows them to indicate they live in another part of the world. Both profiles/personas, with their accurate and inaccurate information, could be controlled by a single, master profile. Whether this is a good thing or a bad thing remains to be seen.

If it does become possible to manage multiple online identities, as just described, it will be because of strong privacy controls provided by whatever standard or standards wind up being commonly adapted. As it stands now, online privacy for many people is more a matter of security through obscurity rather than a coherent privacy strategy. Rowe and Ciravegna conducted an experiment where they were able to successfully build profiles of users using publicly shared information (2010). Perhaps even more troubling, they were also able to automate the process (Rowe and Ciravegna 2010).

Given that privacy and identity are such important issues, it's not surprising that some people have explored the idea of government regulation of identity. In Europe, many European Union members are already moving forward with national electronic ID cards (Collings 2008). These cards have not been able to help resolve the challenges of managing Web identities, though. Hoikkanen et al. indicated "infomediaries" as a challenge to an all-encompassing electronic government-sponsored identity strategy (2010, 5). Hoikkanen et al. define infomediaries as "private gatekeepers of people's personal data (ISPs, Google, Facebook)" (2010, 5).

Unfortunately for librarians, there is not much to be done in terms of moving the online identity management cause forward. There are many factors, technologies, and specifications that make it too complex an issue to be guided by professionals who are not directly involved in the initiative.

However, librarians can serve as interpreters to users, helping them to understand the importance of online identity as well as the privacy implications. Librarians at many academic institutions wind up in some sort of technological leadership role. In that role, they can discuss online identity with patrons, outlining the current state of online identity management, but also presenting future possibilities.

While decidedly less lofty than the Identity 3.0 dreams of Siegel or Mather, even something as simple as OpenID, which, while not horribly secure, can be helpful for certain users, allowing them to access low-stakes websites with a single login.

It seems everyone has dreamt of the elusive master sign-on credential, the universal login and password combination that gives users access to every site to which they have (or want) access. While that dream might not ever come to fruition, it seems there are initiatives moving forward that will make it easier for users to manage their online identities. As information professionals, librarians need to monitor the emerging identity management tools and services, insuring that these services simplify online identities for users without making them vulnerable to things like identity theft and privacy exploitations.

It's hard to say just how far away Identity 3.0 is, but no matter how close the concept is to becoming a reality, users still need advocates to protect them but also to inform them. Online identity is complex to navigate but an increasingly important concept to understand.

REFERENCES

Collings, T. 2008. Some thoughts on the underlying logic and process underpinning electronic identity (e-ID). *Information Security Technical Report 13*: 61–70.

Connolly, P. J. 3 May 2010. OAuth is the 'hottest thing' in identity management. *eWEEK 27* (9): 12–13.

Fest, G. 2008. The lure and peril of OpenID. *Bank Technology News 21* (4): 10.

Hammer-Lahav, E. 2010. The authoritative guide to OAuth 1.0: Introduction. *hueniverse*. 11 May. http://hueniverse.com/oauth/guide/intro (accessed July 26, 2010).

Hoikkanen, A., M. Bacigalupo, R.Compano, W. Lusoli, and I. Maghiros. 2010. New challenges and possible policy options for the regulation of electronic identity. *Journal of International Commercial Law and Technology 5* (1): 1–10.

MacMillan, D. 2009. Why Facebook wants your ID. *BusinessWeek 4161*: 92–93.

Mather, T. 2008. Get ready for Identity 3.0. *SC Magazine: For IT Security Professionals*: *66* (March).

Mills, E. 2008. Consumer technology; One key fits all: So many web sites, so many user names, so many passwords; OpenID may be the solution. *Wall Street Journal*, *29 September*, R11.

OpenID. n.d. Surprise! You may already have an OpenID. *OpenID*. http://openid.net/get-an-openid (accessed July 26, 2010).

Rowe, M., and F. Ciravegna. 2010. Disambiguating web references using Web 2.0 data and semantics. *Web Semantics: Science, Services, and Agents on the World Wide Web 8*: 125–42.

Siegel, D. 2009. *Pull: The power of the semantic web to transform your business*. New York: Portfolio.

Wortham, J. 2010. Why Facebook Connect, a leg up in attracting users to new social web sites. *New York Times*, *13 March*, B3.

Yerbury, H. 2010. Who to be? Generations X and Y in civil society online. *Youth Studies Australia 29* (2): 25–32.