

Power to the People Via User-centric Identity

Identity Woman - April 16, 2007 at Web 2.0 Expo

Why Identity Matters for Web 2.0

Web 2.0 is about the emergence of an *alive* web – made up of people connecting and sharing together in groups. It is literally *pulsing* with the thoughts, hopes, wishes, actions, poems, prose, photos, video's and many cultural expressions of our lives. Our identities – who we are is socially constructed. We could start with the word ubuntu – it is not just the name of a user-friendly Linux distribution it is a zulu word that means “*I am who I am because of who we are together.*”

Doc Searls has put it another way - *we are the authors of each other*. We have had “identity” since the dawn of time – our identity is innately shaped by the culture we live in, the geography of place and the resources at hand. Through Web 2.0 tools we are just doing what has been done for millennia in communities where sharing stories shaped culture and gave us a sense of who we are – exchanging all sorts of value with each other – some of which were around material goods, and some of which were around services. And much of it was mutual authoring through the creation and sharing of culture, meaning and reputation. Who we are and who the individual was mattered enormously in the context of the “we”.

I recently heard a talk by David Weinberger where he talked about first, second and third order information storage related to books. I think this frame can be helpful for us to think about what is going on with identity for people and the web. In first order storage, books exist in one place on a book shelf. Second order storage is the card catalogue with the meta-data about the books on the book shelf. With digital media and the internet we have third order storage of books where the data (the book content) and the meta data (information about the book) are both virtual and can exist in more than one place at a time.

Although our bodies can only be in one place at a time a lot of what web 2.0 is about is the extension of ourselves into the digital realm. Some of us have personal pages on multiple social networks. We put information about ourselves online and share it in all kinds of places. We work together to filter and sort information for our communities. We play games with people from around the world. (70% of Second Life is from outside the US). We manage our Instant Messaging presence on multiple networks simultaneously! Who we are when we do all these things matters a lot because the bread crumbs we leave behind. The impressions we make on others – the way those people mark, tag or otherwise order our shared experience.

We are also seeing challenges in this new atom bit mix. In *extending* ourselves into the digital realm things happen to our identities that were not possible when all records about us were stored physically. This new fluidity can be a bit disconcerting and raises new privacy concerns. It is easy to ping a database and learn about all ones past transactions with a company – this could be good for self reflection and better deals but bad take it to use against us. We are sharing ourselves in new ways online – we can project pieces of ourselves through our blogs, we can show up in Flickr, and online video's. We are all “a little famous” to others beyond what we could be in ‘just’ a physical world - where once you might have shown up in the local paper just once in your life for winning a science fair – (like I did when I was 12!) – now you show up daily to your friends but also to those who randomly discover you. The old model still has my science fair win locked up in the local paper in a microfiche in my home town library. The new model has me and anyone else distributed, searchable, browsable and discoverable across the globe.

The promise of Web 2.0 comes with the distributed web of information by and about me AND by us about us. With an identity layer there exists the potential for products and services to go beyond isolated silos to deeply link together people, events, associations, meaning and media to become more than the sum of what any application could do or be alone. Identifiers that work in the digital realm along with human friendly metaphors and user-interfaces to manage this including one's own privacy are critical for a fully realized vision. These new identity tools to be trusted must protect privacy, reputation and be secure. These are the challenges that must be solved collaboratively by the larger web 2.0 community.

Web 2.0 is only going to work if people trust the web enough to use it. PHRAUD, Phishing, pharming and theft of identity, are destroying user trust and USER TRUST is critical for Web 2.0 to succeed. Kim Cameron, one of the leaders in the Identity community has been tracking fraud statistics and they are staggering. When the Internet was created it was a small community of scientists, hackers and academics who didn't need an identity infrastructure, because they already had (out of band) in the context of their own smaller communities. Web 2.0 creates the opportunity

Ubuntu
en.wikipedia.org/wiki/
Ubuntu_(ideology)

*Information, we observed, is derived from the verb *inform,* which is related to the verb *form*. To *inform* is not to "deliver information", but rather to *form* the other party. If you tell me something I didn't know before, I am changed by that. If I believe you, and value what you say, I have granted you authority. Meaning, I have given you the right to *author* what I know. Therefore, ***we are all authors of each other***. This is a profoundly human condition in any case, but it is an especially important aspect of the open source value system. By forming each other, as we also form useful software, we are making the world. Not merely changing it.*

- Doc Searls IT Garage
www.itgarage.com/node/725

I exist at Blogger, del.icio.us, Flickr, Facebook, Twitter, Reader, and Dodgeball (update frequency / abandonment rate varies).

- Mihai Parparita
blog.persistent.info/

IdentityWoman.net

My blog covers the industry and identity issues more broadly. The sidebar includes upcoming events, resources to learn more about identity and an annotated blogroll.

Identity Commons is a very loose umbrella organization for the range of conversation around technical, social and legal aspects of a digital identity layer.
wiki.idcommons.net

OpenID.net

Kim Cameron's
The Laws of Identity
www.identityblog.com

- 1) Personal control and consent
- 2) Minimal disclosure for limited use: data minimization
- 3) Justifiable parties: "need to know" access
- 4) Directed identity: Protection and accountability
- 5) Pluralism of operators and technologies: minimize surveillance
- 6) The human face: Understanding is key
- 7) Consistent experience across contexts: Enhanced user empowerment and control

for us to 'know' each other again and reweave a fabric of trust on the web through communities. This is a hard problem well beyond the ability of any one person or one community to solve it. In the Identity Commons community some building blocks to solve these issues have emerged but we don't know the answers.

The community has innovated OpenID as a way for individuals to sign-in to sites across the web that support the protocol. Looking ahead are conversations about:

- *datasharing* services so that I can update my information once and it "shows up" in multiple places or not as I desire.
- *personal network portability* where I can take/share/access 'my' network of contacts from one service to another.
- vendor relationship management services so I can manage my relationships with companies I buy from.

All of this is still individually centric and I think the real value opportunity is in communities - communities of people who know each other, care about each other and seek to collaborate together on activities none could really do alone. How do we - show up together in many places? The power of groups to work together and move themselves around from context to context coherently is nearly impossible. The real value is in the WE made of many I's, because people fundamentally see themselves as part(s) of social groups. For web 2.0 this means having tools that support both people AND communities. Success in an interconnected social web means platforms and companies need to begin thinking about designing for "my architecture" this is in the context of *our web*, so they must also begin thinking about designing for "we architecture." I (as a user) am going to use tools that work for me using my identity to hang my relationships on - hooks to me -- if you will. Because I am a social being - I relate to many groups and share many imagined communities and cultures with others. This will unleash a reflective power this gives us as individuals and collectively the ability to make better decisions and act differently. It creates a feedback loop we didn't have before.

Community is about shared meaning, understanding and trust to take action together. When you get down to it trust is crucial for a heart in Web 2.0. This raises the question of how and why do we trust? Is it because you hand me government papers that say you are who you say you are? When do we do that in real life? Only when we are interacting with abstract entities - 'the bank', 'the government', 'the passport control check point.' We generally don't use these to interact with others socially.

Trust, in part, comes from knowledge of past interactions and basis a decision to trust in the present comes from a combination of current context and past interactions. These can be interactions with

- ourselves. *I trust my friend Sally because we have been doing things together for a long time.*
- others we know who vouch for their past experience. *I trust Bill who is Sally's friend because she trusts him.*
- others we don't know who assert successful past interactions. *I don't know Jane but she says Suzie was a good person to do business with.*

Trust is not an algorithm it is a knowing set of instincts we evolved and intuition we develop to survive and thrive in social groups. Each of us individually and each of our communities (the we's) have our own way of balancing our needs for trust as our lives and community dynamics that unfold moment to moment. We make decisions regarding trust based on a range information that we have which we mentally aggregate to form judgments as we need to.

The "how" of all this is not obvious - science is just starting to unpack the deeper roots of our minds and human social behavior around trust instincts and intuition. In our evolutionary past these were tribal groups of around 150 people that you knew for life. A question we must ask our selves is what if our natural ways of discerning about trust don't scale to the size of our social context today whether it is cities of millions or a web of billions? Another question that arises is what happens when our assumptions for social behavior work in a shared culture be it epistemic, geographic or religious but not in another? How do we as an evolving web 2.0 culture develop enough cultural literacy, emotional maturity and helpful tools to overcome these hurdles?

We must think deeper than "5 star ratings" and gesture algorithms to look deeper human at drivers and social processes. Instead of thinking in terms of technology and platform we need to innovate solutions to these difficult problems that are user-centric. And solutions that are rooted in community contexts.

So what do we do today? Where do we start? I believe the place to begin is to start supporting OpenID to become a relying party and if possible an OpenID provider. OpenID gives users the freedom to extend themselves across the web in a way that is under THEIR control.

Internet Identity Workshop
May 14-16, Mountainview
liw.windley.com

Identity Commons
wiki.idcommons.net

OpenID.net
The community portal

OpenID explained
en.wikipedia.org/wiki/OpenID

Part of OpenID

Yadis - www.yadis.org

LID - lid.netmesh.org

i-names - www.inames.net

Sxip - www.sxip.net

Open Source bounty info
IWantMyOpenID.org

Community Blog Hub
planet.opened.net

OpenID Directory
To find enabled sites
OpenIDDirectory.com

Next, before we can get to good answers, we need to determine good questions. I invite you to join the conversation at Identity Commons and the Internet Identity Workshop about how group identities along with individual identities should be supported in a living web, the new web for all of us - Web 2.0.

Web 2.0 provides us with a fabulous new set of engines that have made Wikipedia possible created live search and many others we learning about here. So the big question is what kind of new engines can Web 2.0 provide us to enhance IDENTITY and TRUST to form a distributed social fabric. What can YOU do with Web 2.0 to create a trustable social web? That's my question to all of you building and participating in Web 2.0.

OpenID - Open Standard for Web Wide Distributed Single-Sign-On

The story behind OpenID is quite remarkable. In 2005 when myself, Doc Searls and others formed the ad-hoc "Identity Gang", it became clear there were several companies and standards efforts with similar goals - an open standard for web-wide distributed single-sign-on. The first Internet Identity Workshop (IIW) in the fall of 2005 in Berkeley brought eighty people together to collaborate and share the work that was happening within the identity space. Since then, IIW has turned into a semi-annual event attracting over one-hundred-and-fifty attendees to participate in an open space format. What is truly remarkable about OpenID is not the technology itself, but rather the people that were able to bring competing technologies and views together so that a new market could be created where everyone could compete not on the technology, but on value that can be brought to users and services.

Originally, OpenID Authentication was an innovation by Brad Fitzpatrick (Chief Architect at Six Apart) to give LiveJournal users the ability to login with their Blog URL at other LiveJournal clones. Johannes Ernst (CEO of NetMesh) had also created Light Weight Identity (LID), which also used URLs to accomplish the same task though with different technology under the hood. Ernst, Fitzpatrick, and David Recordon (Software Engineer at Six Apart at the time) decided to collaborate to create an interoperable version which combined the best pieces of LID and OpenID. While this hybrid protocol was never actually developed, this effort spurred the development of the Yadis discovery protocol.

In the community there was a service discovery protocol as part of the XRI (eXtensible Resource Identifier) technology at OASIS. At the first IIW, a conversation was started to reuse the discovery document from the XRI technology within Yadis. In January of 2006, Recordon hosted a technology summit where version 1.0 of Yadis was ratified and is now being widely used throughout OpenID deployments.

The summer of 2006 marked the next wave of convergence within the user-centric identity community. In July, the i-names (based upon XRI) providers made the decision to switch from using SAML to OpenID for authentication and were able to do so easily due to the OpenID community already using Yadis which took advantage of XRI technology. In August, Sxip Identity decided to weave its work into OpenID and joined the community as a part of the IWantMyOpenID.org developer bounty program announced at OSCON. In the end, it was agreed that the community would use OpenID to describe this overall standard and community effort.

OpenID is thriving as a community and is seeing significant adoption:

- [Every](#) AOL screen name is also an OpenID
- Many Web 2.0 companies are supporting OpenID, or have announced they will be: Digg, Netvibes, Six Apart, Magnolia.com, 37signals, Zoomr
- Plugins, or native support, for many Open Source projects like Drupal, Plone, Joomla, Wordpress, MediaWiki, Ruby on Rails.

How does it work? The end-user goes to a website they want to login to - the relying party. They see it accepts OpenID. They enter their identifier into the login box on the relying party site and they are redirected by the relying part to their OpenID provider. At their provider they are prompted to authenticate using a password or some other form of stronger authentication. Once the provider is satisfied with the authentication, the end-user is redirected back to the relying party they are logging into.

OpenID is not a trust system and is architected to solve small but useful pieces of the digital identity problem. The idea is that trust first requires identity, which OpenID provides. From there, it is up to all of you to take advantage of finally having global identity on the Internet and to build cool applications with it.

Kim Cameron's Blog
www.Identityblog.com

Microsoft on Cardspace
cardspace.netfx3.com/

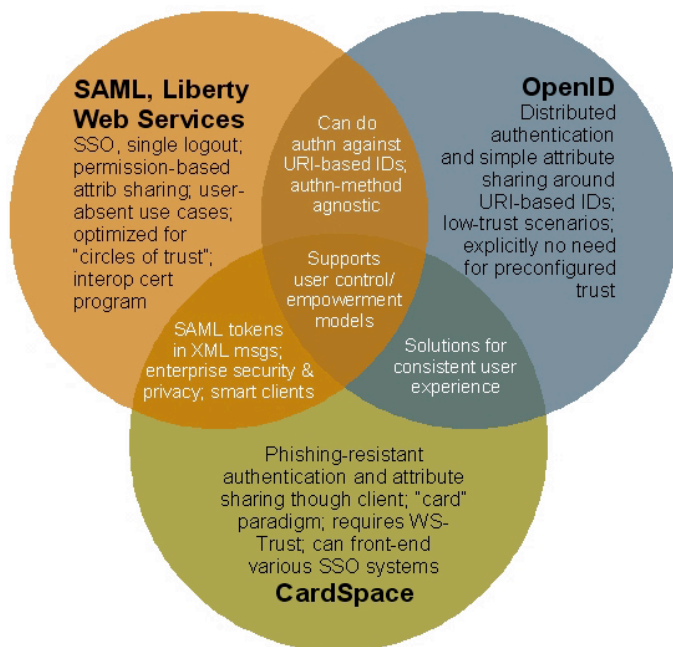
Wikipedia on CardSpace
en.wikipedia.org/wiki/CardSpace

Higgins
www.eclipse.org/higgins/

Microsoft

Kim Cameron is the chief Identity Architect for Microsoft. In 2005 he published the *Laws of Identity*, many of which were built upon the learning of Passport, that technical systems should follow. Cameron received extensive feedback from the Identity Commons community and has been working with them at events such as IIW, fostering good communication. Microsoft has innovated CardSpace (shipped with Windows Vista) to support secure sign-on to websites in a password free manner. One of the main goals of CardSpace is protecting the user from phishing attacks.

Announced by Bill Gates and Criag Mundie at RSA this year, there is an agreement between members of the OpenID community and Microsoft to cooperate. The announcement included support of CardSpace as a technique to help control phishing at some OpenID Providers as well as OpenID being embraced and supported within Microsoft technologies. Microsoft has licensed the intellectual property behind CardSpace in a way that allows others to develop similar tools for other platforms. One group working on this is the Higgins project which is a part of Eclipse another open source effort is Bandit lead by Novell.



The Venn of Identity by Eve Maler

www.xmlgrll.com/blog/archives/2007/03/28/the-venn-of-identity/

also derived from work by Paul Madsen connectid.blogspot.com/ AND Johannes Ernst http://netmesh.info/jernst/Digital_Identity/Updating-three-standards.html

Liberty Alliance

The Liberty Alliance is a vendor consortium that also includes businesses, government agencies and nonprofit organizations. Their outputs solve many of the enterprise related single-sign-on and data sharing problems. Through OASIS, they've developed SAML (Security Assertion Markup Language) which is optimized for "human-to-application" interaction has wide adoption. Many of the assumptions that were made designing for the enterprise and because of this it has yet to take root within the open Internet. They are currently working on Liberty Web Services (ID-WSF and ID-SIS), that are optimized for "application-to-application interaction" and the People Service, a "groups and roles definition" service that can bridge different identity ecosystems.

OSIS

OSIS brings together many identity-related open-source projects, and synchronizes and harmonizes the construction of an interoperable identity layer for the internet from open-source parts. Its first deliverable is interoperability with Microsoft CardSpace, although OSIS also encompasses alternate technologies such as OpenID and SAML.

Liberty Alliance
Projectliberty.org

SAML - Security Assertion
Markup Language
en.wikipedia.org/wiki/SAML

OSIS
osis.netmesh.org/

Identity Commons
Wiki.idcommons.net

Identity Commons

This is the loose umbrella organization forming to help all these identity efforts coordinate and collaborate. *The purpose of Identity is to support, facilitate, and promote the creation of an open identity layer for the Internet, one that maximizes control, convenience, and privacy for the individual while encouraging the development of healthy, interoperable communities.*

The organization has evolved to its current form after several years. There are 15 working groups including: *The Identity Gang* with a mailing list and community lexicon. *Identity Rights Agreements* for better EULA (end-user license agreements) in the identity layer. *Identity Schema's* to develop shared schema's across identity systems.

The main community gathering is the Internet Identity Workshop the next one is May 14-16, 2007 in Mountainveiw. We welcome you to join the conversation.