

Empowering Individuals with Tools to Manage Their Personal Data for the Identity in the Browser

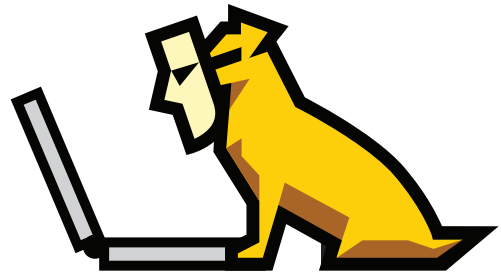
By: The Personal Data Ecosystem Consortium

Kaliya Hamlin, Executive Director, Personal Data Ecosystem Collaborative Consortium
director@personaldataecosystem.org @identitywoman Mobile: 510-472-9069

Mary Hodder, Chairman, Personal Data Ecosystem Collaborative Consortium
mary@personaldataecosystem.org Mobile: 510-701-1975

Introduction

I convene the [Internet Identity Workshop](#) the main gathering of Identity Commons. It has met every six months since the fall of 2005. This collaborative industry event brings together independent developers, major web companies, companies who sell identity solutions to businesses. The focus is user-centric digital identity technologies are focused on making individuals/ end-users/ citizens empowered with their own identity online - to have it be persistent, autonomous, be under their control.



Many of you doubtless have recognized in our logo the allusion to the [famous New Yorker cartoon](#), “On the Internet, nobody knows you’re a dog”

To me our logo symbolizes three human rights which we believe are worth fighting for:

1. The Freedom to be who you want to be online, i.e., the right to anonymity.
2. The Right to curate the information about yourself that can be found online.
3. The ability to express verified claims about yourself and share detailed information when you want with people and organizations.

We are keen to see tools in the browser that support these rights and freedoms we believe in. I am ultimately an end-user advocate rather than a technologist building particular tools. This paper outlines some of the questions we have and talks about emerging developments in our field.

Personal Data

The Personal Data Ecosystem Consortium represents a community of end-user advocates and technology innovators focused on individual rights and access to individuals' own personal data, and the business and innovation opportunity that this new user-management and control.

The “bread crumbs” of data that people leave as they move around the web is one kind of “personal data” that our consortium is focused on. Other types of data include transaction histories, utility logs, geo logs, phone call logs, instant message logs, logs from medical devices or wellness trackers.



The young woman running is leaving a whole trail of data as moves through her life. Cover of the World Economic Forum Report on Personal Data.

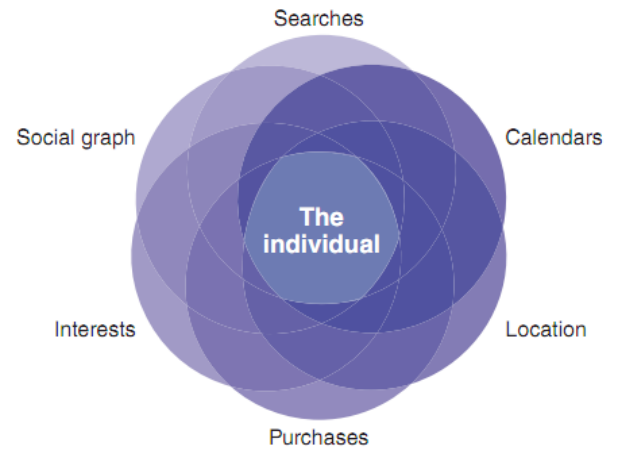
An individual's click stream and web browsing history is very personal.

How it is protected and how the user is given choice about how it is stored, used and access is critical?

Having a free society depends on people being able to explore and access ideas without fear that this will be tracked in their explorations. That their viewing and reading habits will be used to make inferences about their political or religious beliefs or personal habits. It has been a social norm that library loan histories are not shared. Higher education uses an identity interoperability standard called Shibboleth that provides for login across university library systems without exactly which student or professor is accessing the system.

The reason that personal data is so interesting is that it gives deep insight into people. When streams from multiple digital mediums across contexts are integrated they give an even more detailed picture.

We think that individuals are the only ethical integrators of all of their data streams. Putting the individual at the center of their own data stream integration is also a key idea put forward in the World Economic Forum Report Personal Data: The Emergence of a New Asset Class.



Personal Data: The Emergence of a New Asset Class. Page 9. Source: Davis, Marc, Ron Martinez and Chris Kalaboukis. "Rethinking Personal Information – Workshop. Pre-read." Invention Arts and World Economic Forum, June 2010.

How can Identity management tools in the browser support the user integrating multiple data streams?

How do these tools work with personal data stores and services that might be in the cloud?

Now is a good time to make a distinctions in a few fundamental concepts.

Being SEEN is an act of mutual social recognition - I see you, you see me, we see each other seeing each other - we are seen.

Being WATCHED is uni-directional. It is done without the subject – I may say “the victim’s” knowledge.

Being STALKED is what happens to someone when the watching activity is *aggregated*, that is when someone is followed through time and space without their awareness.

The behavioral marketing, advertising and search industries are stalking people all over the web - collecting information about them and their activities without their awareness. The status quo is highly invasive of people’s privacy, linking their activities across contexts they wish to keep separate or private if they chose to do so. In addition, decisions about people's lives are increasingly made from such data, and they are not aware of it, though the consequences can be quite severe. Economic value is derived, but at the expense of the basic dignity and privacy rights (ie personal control) of the individual.

How can the tools that are put forward for identity management in the browser support individuals being able to manage and put forward different personae depending on the context they are seeking?

How do identity management tools in the browser interact with an individuals personal data store on their own server or in the cloud?

How can the information that is shared via browser based identity tools help individuals understand more about how others see them?

Personal Data should be treated like Personal Money

Individuals must be able to move data between service providers, as they can move money between banks, retaining its value. However, with user's data, it's the user that is the provider, but there must still be many takers because of open data formats, activity streaming, and clear identity models that are also portable and separate from the data bank.

End-user choice and the right to transfer data from one service provider to another is key to this model. Just as our money does not become worthless when we move it from one bank to another, the same needs to hold true for individuals' data.

What is the role of identity management tools in the browser managing the transfer and movement of information between data stores.

Personae Management

In the physical world individuals manage their identities across contexts. They choose what information to share where depending on the how they want to be seen and what is contextually appropriate. One of the things that we have learned in the last several years of engagement with user-centric identity and women in technology communities (the co-authors are also the founders of She's Geeky a women's only technology unconference that has happened 8 times across the country in the last 4 years) is that women are more frequent users of personae to separate life contexts.

Examples of where women are separating their persona's out include

- Professional Life - if as a "licensed professional" or hiding one's gender while participating on technical mailing lists
- Gaming Life - Handles in Game
- Personal Life - Dating and Sex
- Personal Life - Parenting
- Personal Life - Sexual Preferences
- Health & Wellness - sharing about disease and other issues.
- Religious Life
- Hobby Life - Quilting
- Sporting Life - teams one belongs to.

These issues of personae management are not just face by women but also by sexual minorities (Lesbians, Gay Men, Transgendered, Bisexual and Queer identified people), religious minorities (think buddhist in the rural south), ethnic minorities (who don't want to have their color be known in online contexts).

How can identity management tools in the browser (and operating system) help individuals manage multiple personae in a way that helps them keep life contexts separate.

NSTIC

The White House in March released the National Strategy for Trusted Identities in Cyberspace. It calls for constituent centric and user-centric identity management tools. It outlines a broad vision for how individuals can manage their identities with fewer user-names and passwords.

How does the development of identity in the browser tools work with the vision outlined in the NSTIC document?