Web 3.0 CONFERENCE & EXPO

Designing For Privacy

Safe Data Sharing, via Semantic Web Architecture (a sketch)

Sandro Hawke, W3C

October 17, 2008 – Santa Clara, CA

W3C® WORLD WIDE WEB consortium

W3C (Web Standards)

- Helping create industry standards
- ~50 WGs, ~500 participants, ~50 staff
- HTML, CSS, XML (etc), SOAP, P3P
- RDF, OWL, SPARQL, GRDDL, RIF
- “Semantic Web”, “Linked Data”
- ... so much more to do!

Data Sharing: Business Risks (Opportunities)

- amazing possibilities
- amazing dangers
- we need a solid approach
- the Web gives us a good model

So Much Information

- Imagine what your cell phone could know:
  - it hears everything going on around you
  - it knows where you are
  - it knows the motion of your body
  - it sees what's in front of it
  - it knows your contacts
  - it hears your phone calls

What Could We Do With It?

- ... I'm not even going to try to guess.
- (but I know it'll be wild)

Requirements: No Surprises

- A clear, robust, simple-as-possible model
- Based on consensus rights and responsibilities
- Make everything predictable for all parties
- No Risk? No. But like a normal business venture.

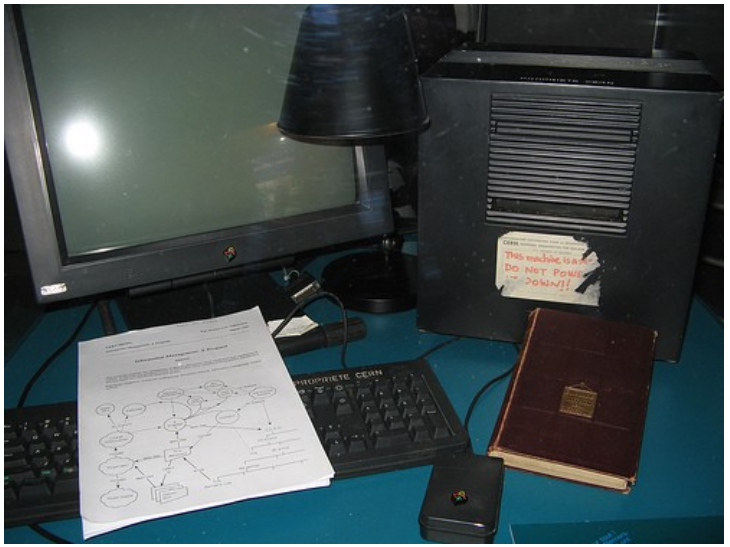
Suggestion: Leverage the Web

- Information origin == web server
- Shared control by originating parties
  - if the information originates from a transaction, all parties ought to have a prior arrangement about control

Example: My-Location Website

- Websites provide information
- Your cell phone has lots and lots

=



Example: Phone-Location Website

- Different pages (APIs) for different uses:
  - Raw data, current and past
  - Geocoding, On-Map, Various Merges
  - "blurred" (eg only city information)
  - purpose-centric (eg location when I'm on the job)
- HTML, RDF, XML, whatever

Grant Access to Person

- List the specific people (agents) for access to specific pages
  - spouse – full location access
  - fellow-traveler during trip – full location access
  - child – city access

Grant Access by Filter

- Roles
  - co-worker
  - “friend” in social network
- Location
  - friends near me
- etc....

Access for a Purpose

- cc-non-commercial
- HIPPA "we may disclose your health information to a healthcare provider who is providing treatment to you"
- Law Enforcement (automating what court orders allow)