The Care and Feeding of Online Relationships

Eve Maler
Principal Engineer
Sun Microsystems, Inc.
The Venn of human/application relationships

- Identity management
- Vendor relationship management
- Personalized, access-controlled app behavior based on data sharing
- Social networking
What is VRM?
http://projectvr.org

• VRM is about empowering users in interactions with online vendors
• Seminal use case: propagating a change of address to authorized online partners automatically
• Other key use cases:
  > Issuing personal RFPs
  > Expressing tolerance for customer support wait times
The design of everyday identity: a cautionary tale

“human-centered design”

“design is an act of communication”

“the difference between pleasure and frustration”
What human tendencies might inform our approach to solutions?
New-relationship energy

Willingness to expend energy on "overhead" app behavior

Trust and register
Configure, customize
Add policies
Use and customize advanced features
Don't bother me... just work!

Time

High-value (fun or productive)
Low-value
The efficiency imperative

Reactions:
- Frustration
- Anxiety
- Impatience
- Annoyance

Strategies:
- Avoidance
- Lying
- Rote behavior

Impatience quotient

Number of clicks, steps, dialog boxes, or required fields
The self-revelation imperative

A friend has invited you to try Pandora.

I wanted to let you know about Pandora, a free internet radio site based on the Music Genome Project. It helps you discover and listen to great music.

Just tell Pandora the name of your favorite song or artist, and it will create a radio station that plays songs with similar musical attributes.

Here's a link to my profile page. From this page, you can listen to my stations and check out new music I've found on Pandora:

Cell phones' nude pictures now part of teen dating, experts say

Published on Sunday Apr 13, 2008

Forget about passing notes in study hall; some teens are now using their cell phones to flirt and send nude pictures of themselves.
Some general lessons we can draw

1. Make “do the right thing” the easiest thing to do
   - Privacy, selectivity

2. Try to make what people want to do possible
   - Connect, share

3. Respect and balance all parties' needs
   - Users, providers
Some implications for today's identity interactions

Make sign-on as seamless as you can
Make a little shared data go a long way
Make consent more meaningful
Requirement: Rescue login time from routine consent-gathering

Does “Yes, dear” mean “Yes”?

Everyday activities must usually be done relatively quickly, often simultaneously with other activities. .... Much human behavior is done subconsciously, without conscious awareness and not available to inspection. .... Subconscious thought is biased toward regularity and structure, and it is limited in formal power. It may not be capable of symbolic manipulation, of careful reasoning through a sequence of steps.

– Don Norman
Requirement: Allow people to impose policies back on websites

Why buy the cow (that's you!) when sites can get the milk for free?

1. Golfer attempts to reserve tee time
2. Site indicates claims it wants, including required claims
3. Selector figures out which cards meet the requirements
4. Golfer selects a managed card out of those presented, and possibly indicates optional claims to send
5. Selector asks provider to supply a token with suitable claims

Public golf course website
Managed card provider
Requirement: Loosely couple all data and relationship-policy events

Four hearts beating as...four

- Paper magazine gets mailed to my home address
- I visit the mag’s website to get special content
- I move to a new house and update my (single) address record
- I decide to change the magazine’s rights to use my data

Thanks to Paul Madsen for the example!
A unified solution needs...

- Asynchronous data access
  - Lots of models possible, e.g. publish/subscribe
  - Data delivered to each app may have many sources
  - Delivery of data to all apps needs to be auditable

- System for expressing your policies for each data usage and further sharing
  - With accountability by legal, social, or economic means

- Dedicated relationship management component
  - Interface for forging and modifying relationship terms, and terminating them entirely
  - Likely also to be the hub for a “personal data store”
Asynchronous data access option: Liberty ID-WSF

1. I register to use ShipThis

2. ShipThis registers with my Discovery service

3. On my approval, ShipThis associates itself to my identity at my Discovery service

4. I visit Books4U and order a book

5. Books4U discovers how to interact with my shipping service

6. Books4U invokes ShipThis to ship out my book

The bookseller offers to ship in a privacy-enabled way

IdP and Discovery service run by my ISP... or my phone!
Asynchronous data access option: “feed-based VRM”

- Personal data store with address and other data – might be kept at, e.g., your blog
- You create shared-secret URLs pointing to custom Atom feeds for vendors as part of registration
- They subscribe and pull data just-in-time
- You can cut off feeds at will
- Pub/sub model works well even without Atom (e.g. iCal)
Some options for user policy

Mary Rundle research on Creative Commons-like icons for privacy and data usage policies

- You agree not to use this data for marketing purposes.
- You agree not to trade or sell this data.
- You agree to submit to a third-party audit program on data use; if government has requested access to my data, you agree to involve my governmental ombudsman.
- You agree to make available to me the data that you have on me without my having to pay for it at a minimal charge.
- You allow me to address inaccuracies in the data and request its removal.
- You agree to take reasonable steps to keep my data secure.
- You agree to arrange with X organization to help resolve any disputes we have over your treatment of this data. [The seal / name of the entity follows.]

Identity Rights Agreements discussion

<table>
<thead>
<tr>
<th>Accessible by Local Community No Sharing Allowed</th>
<th>Accessible by Federated Communities</th>
<th>Accessible by Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Once and Delete</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>May Cache for Duration of Session</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>May Cache and Must Refresh until Deletion Requested</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>May Store Locally until Deletion Requested</td>
<td></td>
<td>n/a</td>
</tr>
</tbody>
</table>

Liberty ID-Governance (CARML and AAPML) and Privacy Constraints work

Request
- Requirements
- Attributes & Properties
- Promises
- Legal Reference

Response
- Assertions
- Obligations
- Exceptions
- Consent
- Legal Reference

Consumer

Attribute Authority
An option for “extraordinary” real-time consent

1. Books4U needs permission to see my list of already-owned books, so it asks where my Interaction service is.
2. Books4U learns that I prefer SMS for permission requests.
3. Books4U asks, and I answer "Yes"...

Liberty ID-WSF Interaction Service for gathering consent/data from an otherwise offline individual.
Some options for relationship management component

- Identity selector with “r-card” (Higgins)
- iPage portal (ooTao)
- “The Mine!” (VRMHub)
Does this model empower parties more evenly?

Can it support new social and commercial data-sharing opportunities?
Resources

• These slides: www.xmlgrrl.com/blog (Publications area)
  > This area also offers other stuff you may be interested in
• Project VRM: cyber.law.harvard.edu/projectvrm
• Don Norman usability info: jnd.org
• Privacy icon research:
  http://identityproject.lse.ac.uk/mary.pdf
• R-card: http://wiki.eclipse.org/R-Card
• Feed-based VRM paper:
  http://docs.google.com/Doc?id=df9dfsgj_lghhqgjfq
• Mine! paper:
  http://docs.google.com/Doc?id=dgc23h2k_397cgqg3xgh
Thanks for your kind attention!

Eve Maler
eve.maler@sun.com
www.xmlgrrl.com/blog