

Open Source Privacy Challenges

7 February 2008

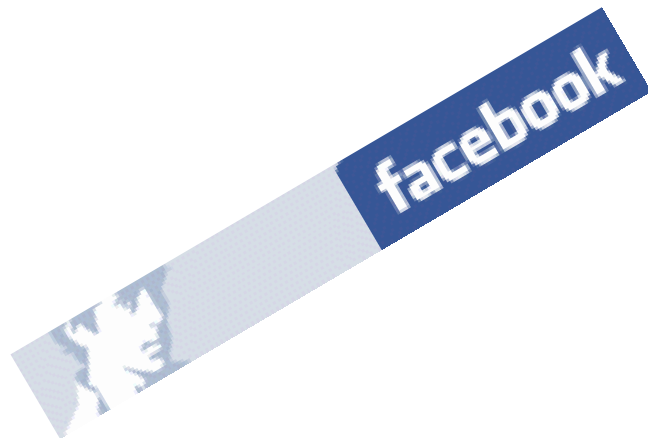
Daniel J. Weitzner <djweitzner@csail.mit.edu>
MIT Decentralized Information Group



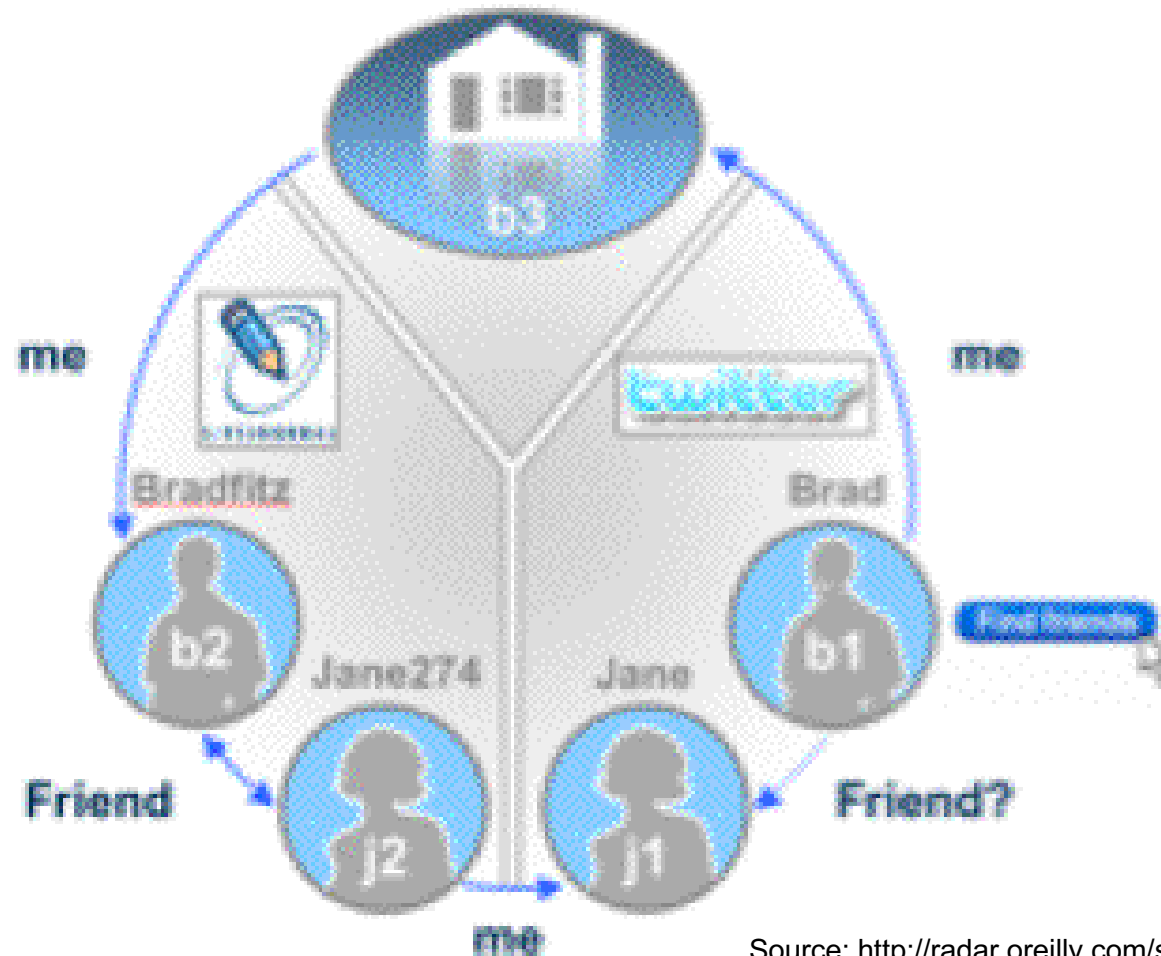
**Can collective intelligence about
privacy save the Web from
collective destruction of privacy?**



Social networks: from walled gardens...



... to the Giant Global Graph



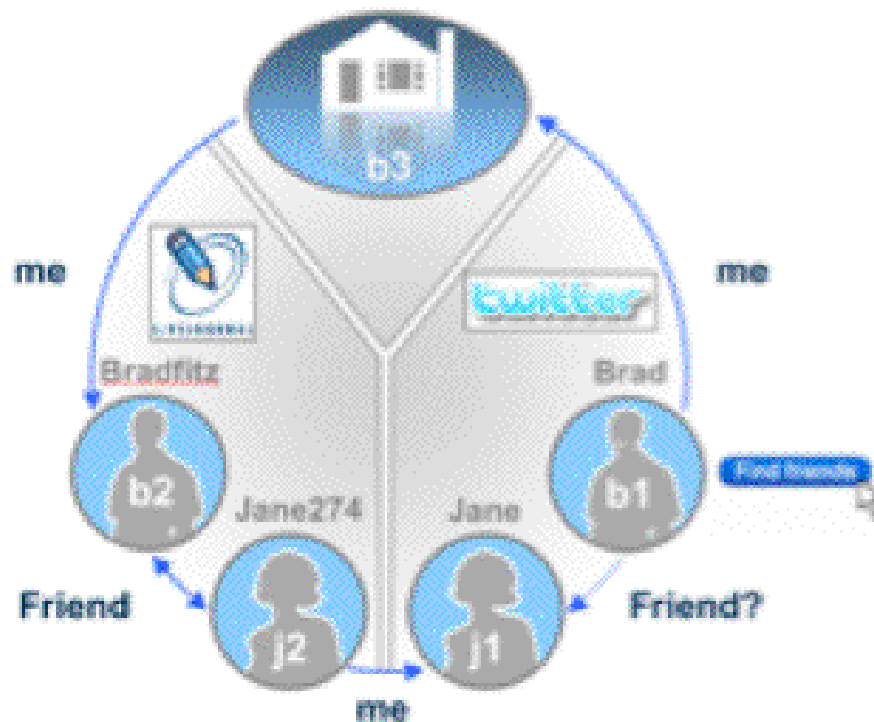
Source: <http://radar.oreilly.com/socialgraph3.png>

Technical Underpinnings of the World Wide Social Network

Open Social API – a common application platform



Social Graph API – access to the social graph the Google creates



Any Privacy Questions?

What can you learn from analyzing a social network?

- From image tags: That the person applying for a job with you spent college drinking
- From looking at images and post: a persons politics, religion, etc., if they do it in public
- *That the person is gay?*



Reactions from the blogosphere

Tim O'Reilly: Radical Transparency

"It's a lot like the evolutionary value of pain," he says.
"Search (searching the social graph) creates feedback loops that allow us to learn from and modify our behavior. A false sense of security helps bad actors more than tools that make information more visible."

Deep Worry

"Being socially exposed is AOK when you hold a lot of privilege, when people cannot hold meaningful power over you, or when you can route around such efforts.... Just because people can profile, stereotype, and label people doesn't mean that they should."



What is Open Source innovation good at?

Leading successes

- Operating Systems: Linux
- Browsers: Firefox
- Servers: Apache (~80% of the Web)

These implement existing designs/standards

- Unix
- HTML
- http



Privacy Design Challenges

- Tools to express their expectations about information access AND usage
- Tools and infrastructure to provide transparency and accountability: assessing when those expectations or relevant laws are broken
- Key Goal: support new social arrangements for privacy in the growing graph of social networks



An Accountability Browser

http://mr-burns.w3.org/cgi-bin/server.cgi.py?logFile=http://dig.csail.mit.edu/TAMI/2007/s9/variation1/log.n3&rulesFile=http://dig.csail.mit.edu/TAMI/2007/s9/variation1/demo-policy.n3

Bettyrejectsbobsreq is non compliant with MA Disability Discrimination Policy

[More Information](#) [Start Over](#)

Because:

Reason for denying Bobsrequest is based on health information. Under the MA Disability Discrimination Law it is inappropriate to use health information to deny a service request.

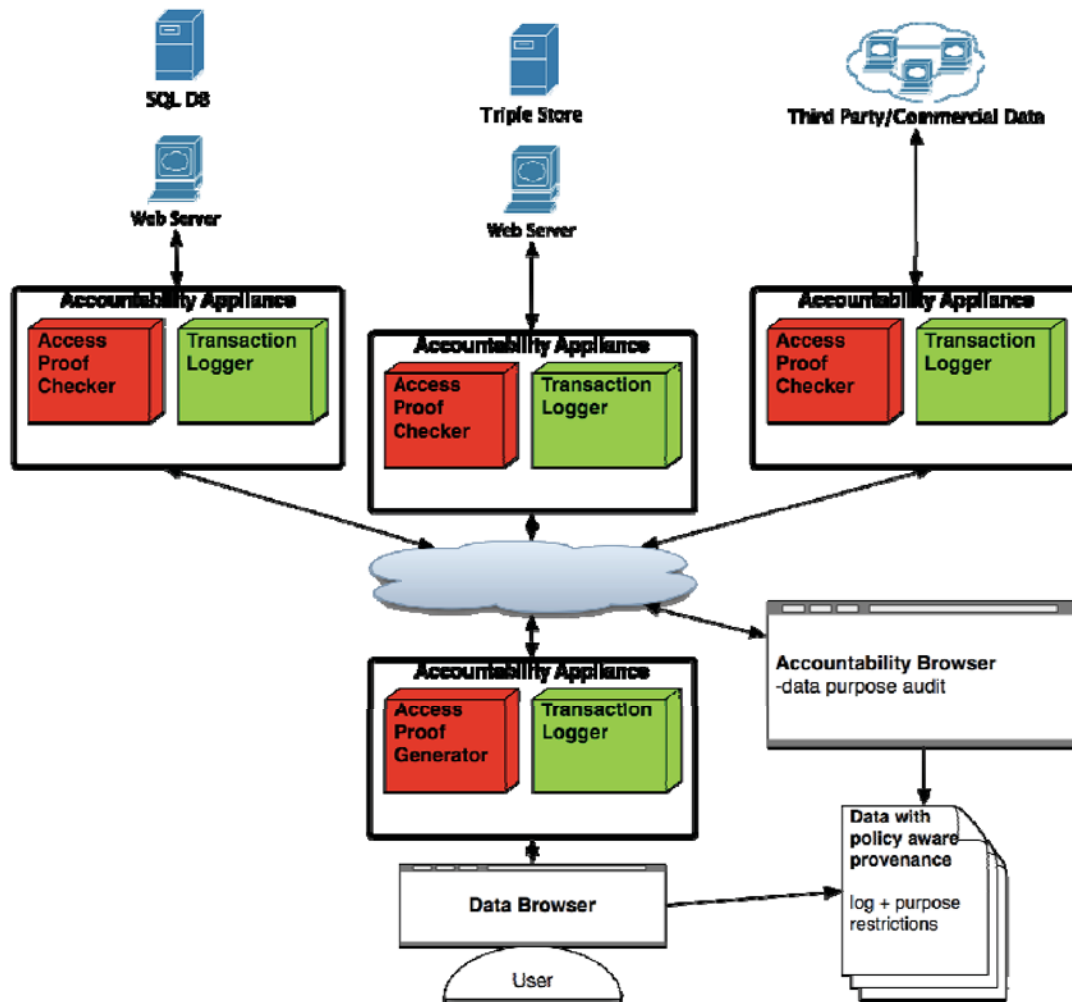
The requester, Bob Same, resides in MA and is covered by the MA Disability Discrimination Law

Bob Same's request, Bobsrequest, was refused because of xphone record 2892

Premises:

Bettyrejectsbobsreq	reason	xphone record 2892
	receiver	customer351
	reply to	Bobsrequest
	type	Refuse Request
customer351	name	Bob Same

Accountability architecture



- Access control through Decentralized Authentication Proofs based on access rules expressed over data semantics
- *Transparent* data usage logging for real-time compliance hints and a *posteriori* accountability
- Engineered as Web architecture components

More Information

- Air specifications:

<http://dig.csail.mit.edu/TAMI/2007/AIR/>

- Paper on AIR submitted to IEEE Policy: [Integrated Policy Explanations via Dependency Tracking](#)

- MIT Transparent Accountable Data Mining Project:
<http://dig.csail.mit.edu/TAMI/>

