The Browser as a Secure Platform

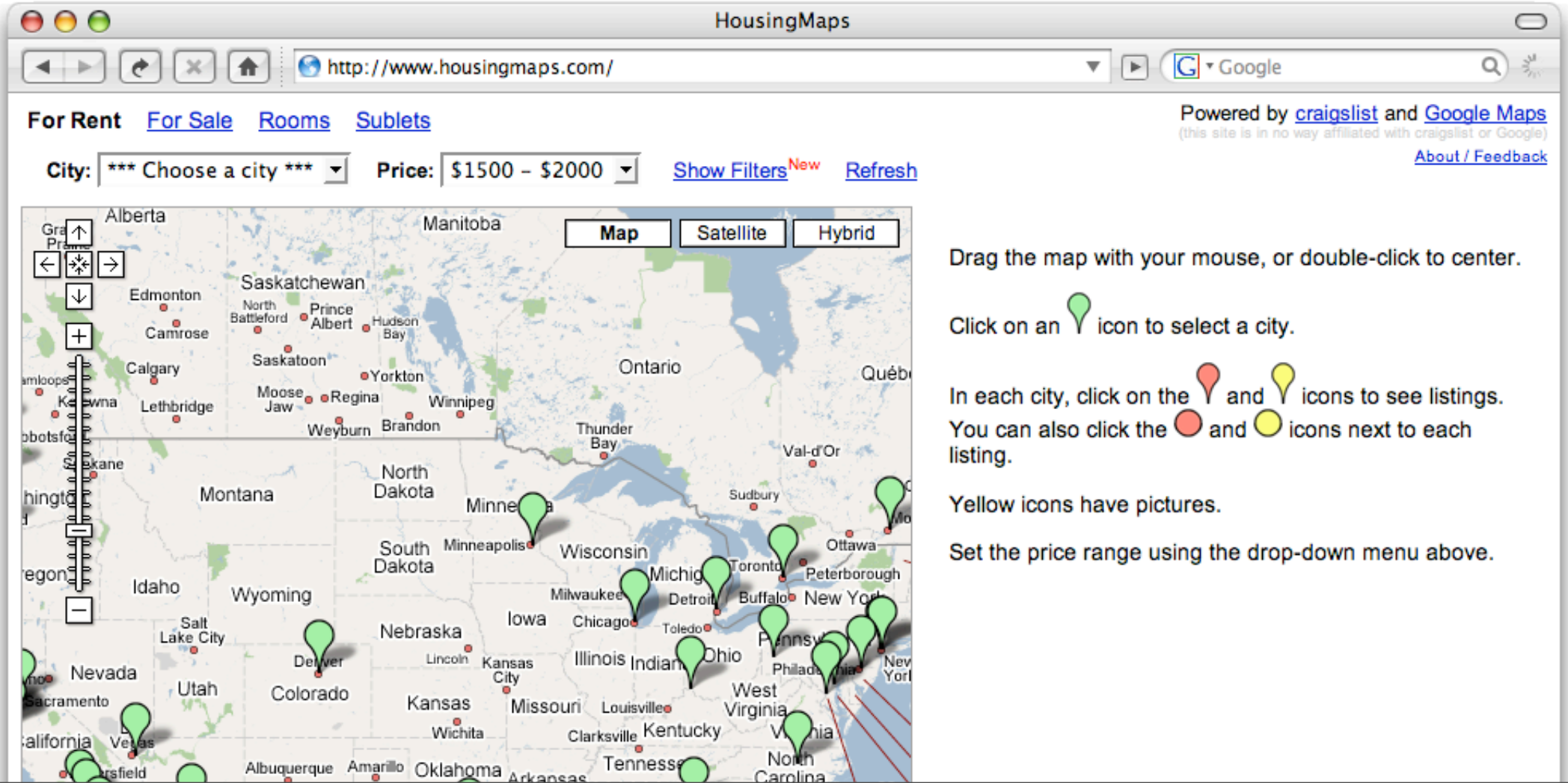
for Loosely Coupled, Private-Data Mashups

Ben Adida
Center for **R**esearch on **C**omputation and **S**ociety
Harvard University

24 May 2007

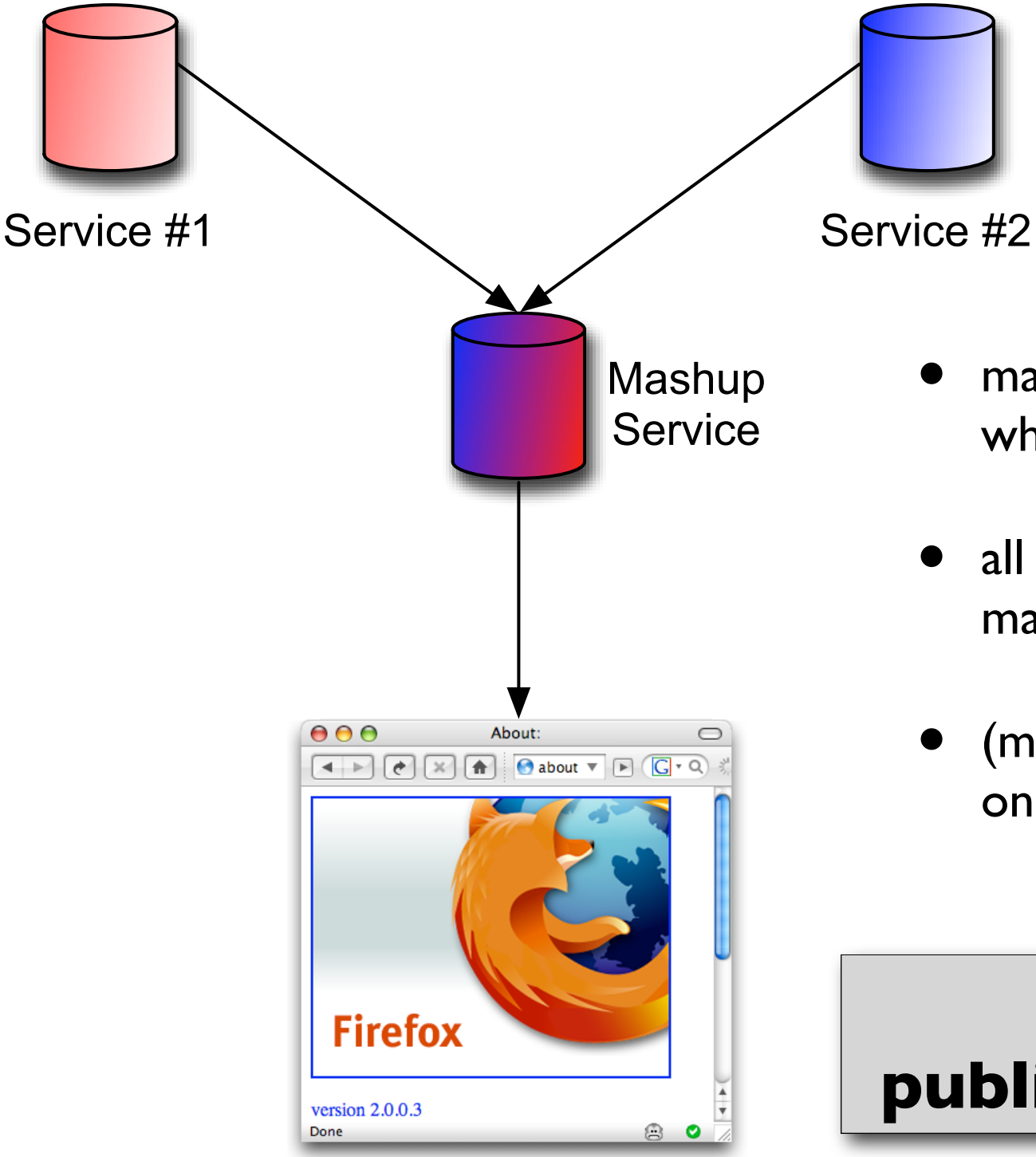
CC BY SA

web mashups: interesting combinations.



Aggressive “web 2.0” development will continue.

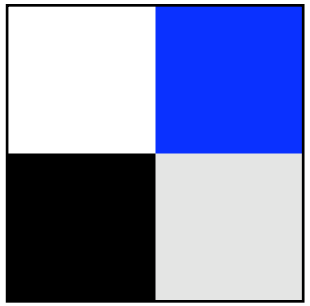
Can we make the browser a better platform?

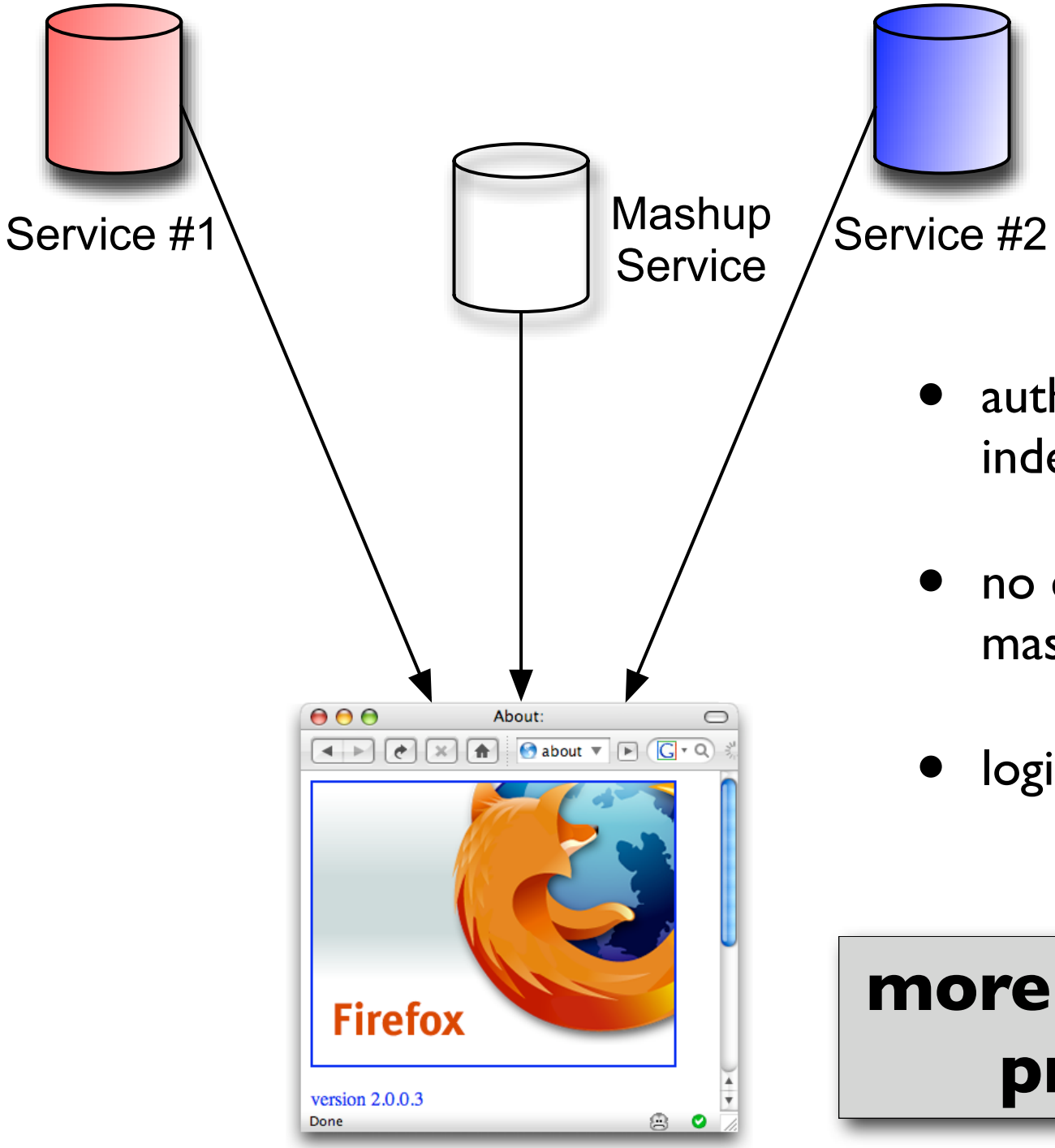


- mashup service selects which sources to combine.
- all data flows through the mashup service.
- (most of) mashup logic on the mashup server.

great for public data services

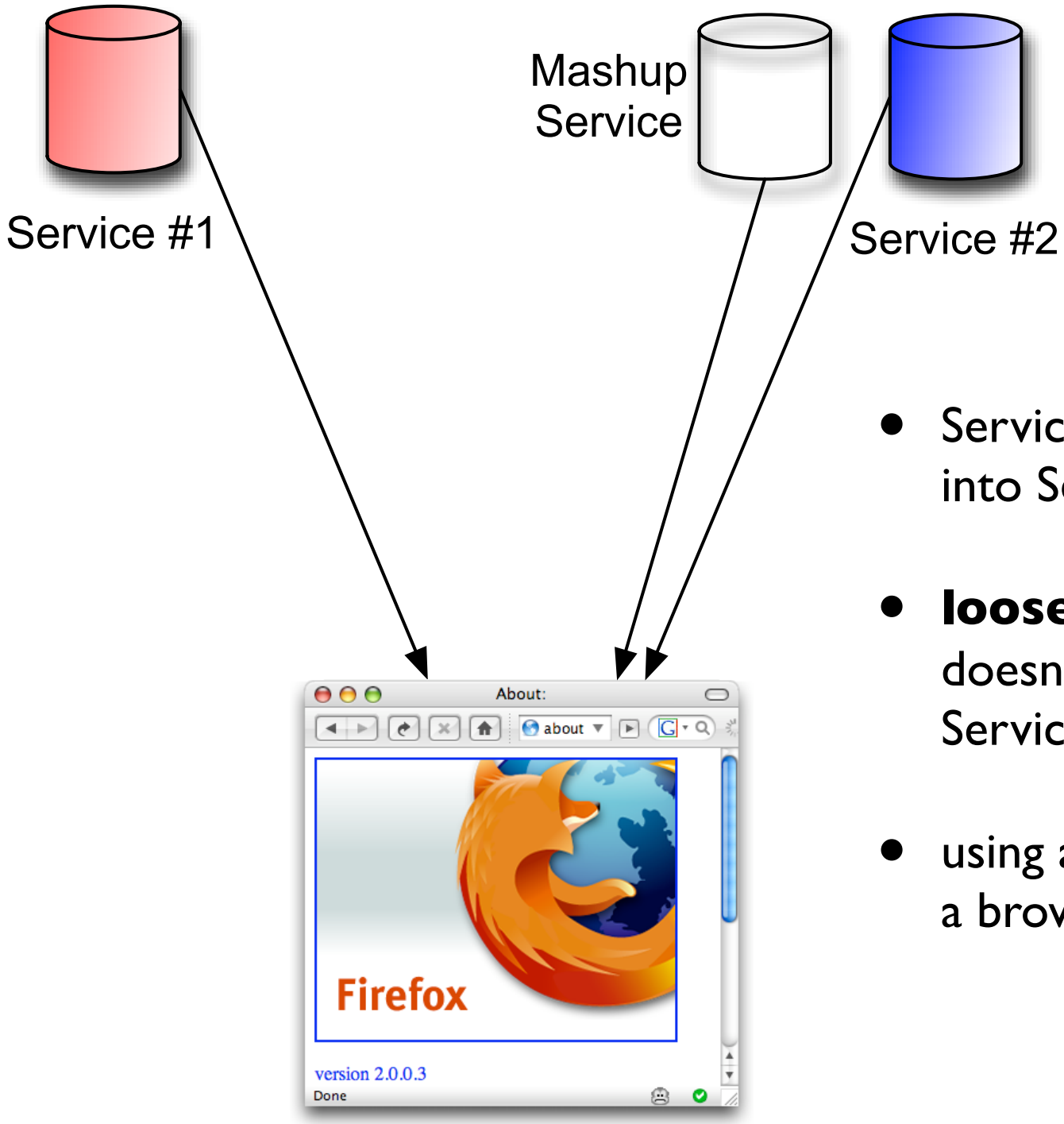
web applications increasingly manage ***private*** data





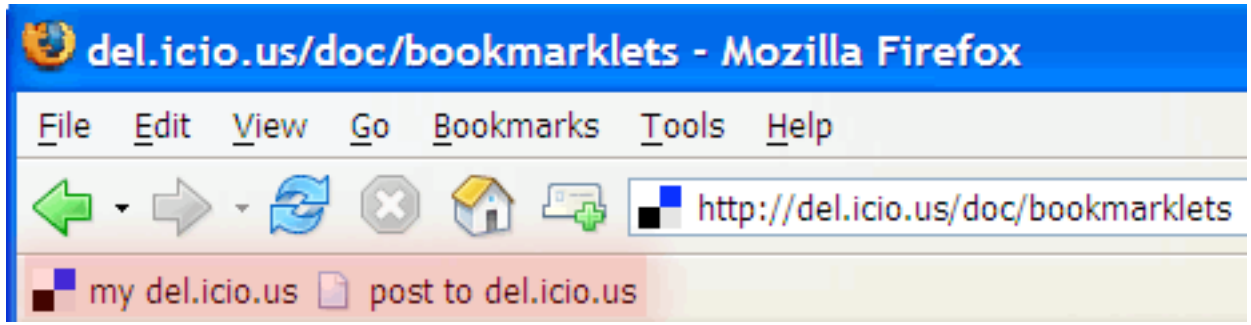
- authentication handled independently by each service
- no data flows through the mashup service
- logic runs in the browser.

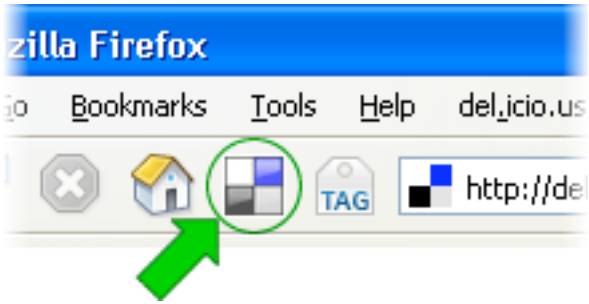
more interesting for private data.



- Service #2 is "injected" into Service #1
- **loose coupling**: Service #2 doesn't necessarily know about Service #1 ahead of time.
- using a bookmarklet or a browser extension

del.icio.us

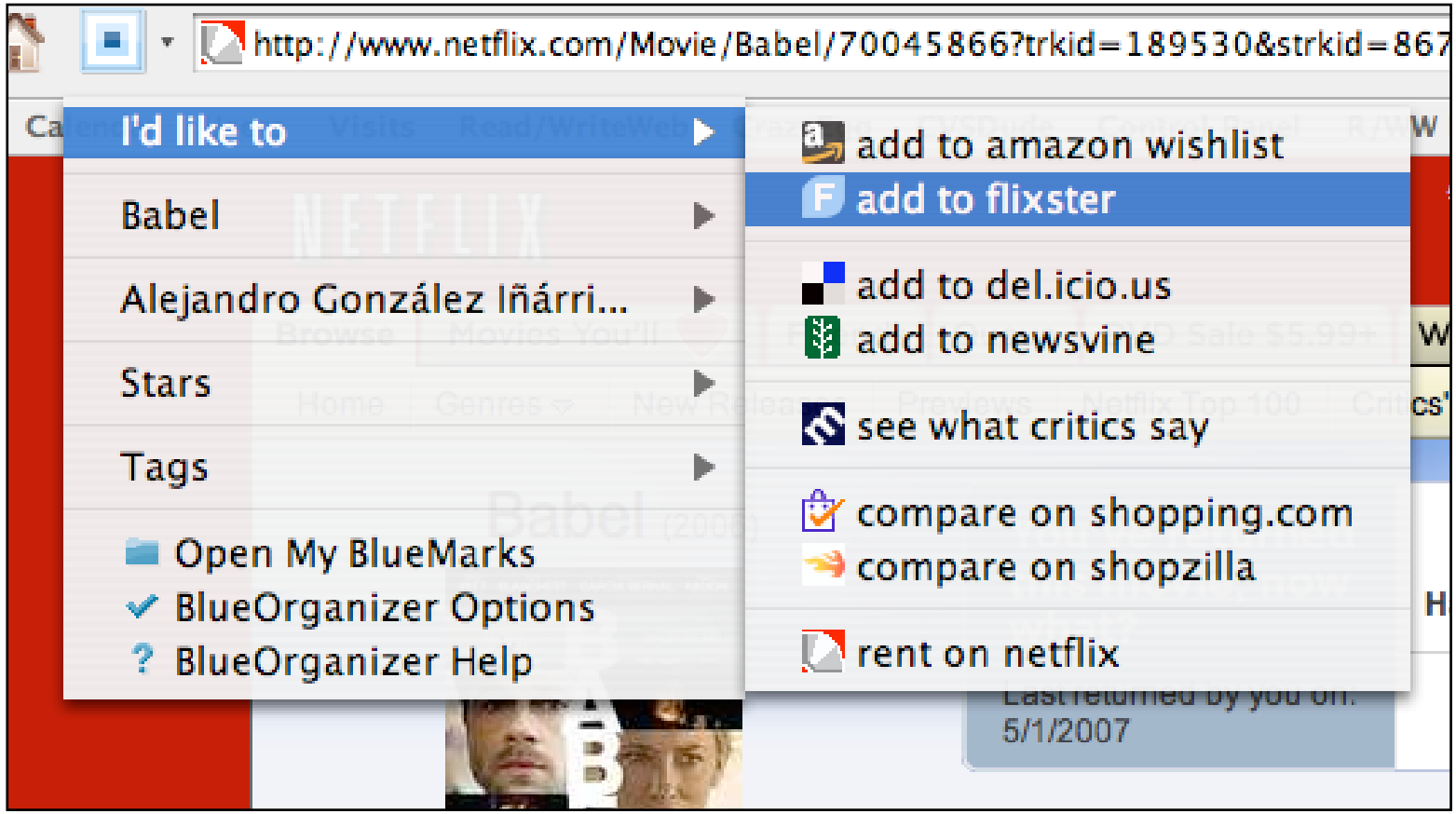

del.icio.us/doc/bookmarklets - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://del.icio.us/doc/bookmarklets
my del.icio.us
post to del.icio.us


zilla Firefox
Bookmarks Tools Help del.icio.us
TAG
http://de

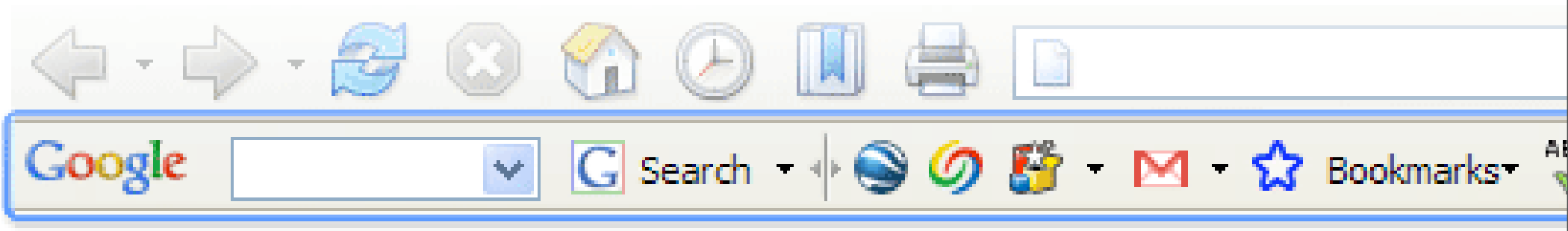
StyleFeeder

AdaptiveBlue

Browse Smarter.



Google Toolbar



Problems

- bookmarklet runs in current page's context
  unstable API - bad for stability and security.
- bookmarklet limited to on-the-fly downloads
  vulnerable to pharming attacks.
- extension has full control over all browsing
  requires significant trust in extension!

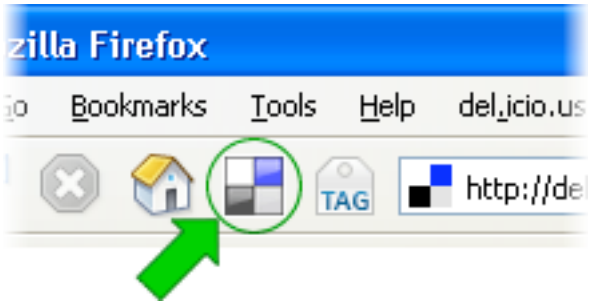
Suggested Enhancements

1. JavaScript Isolation

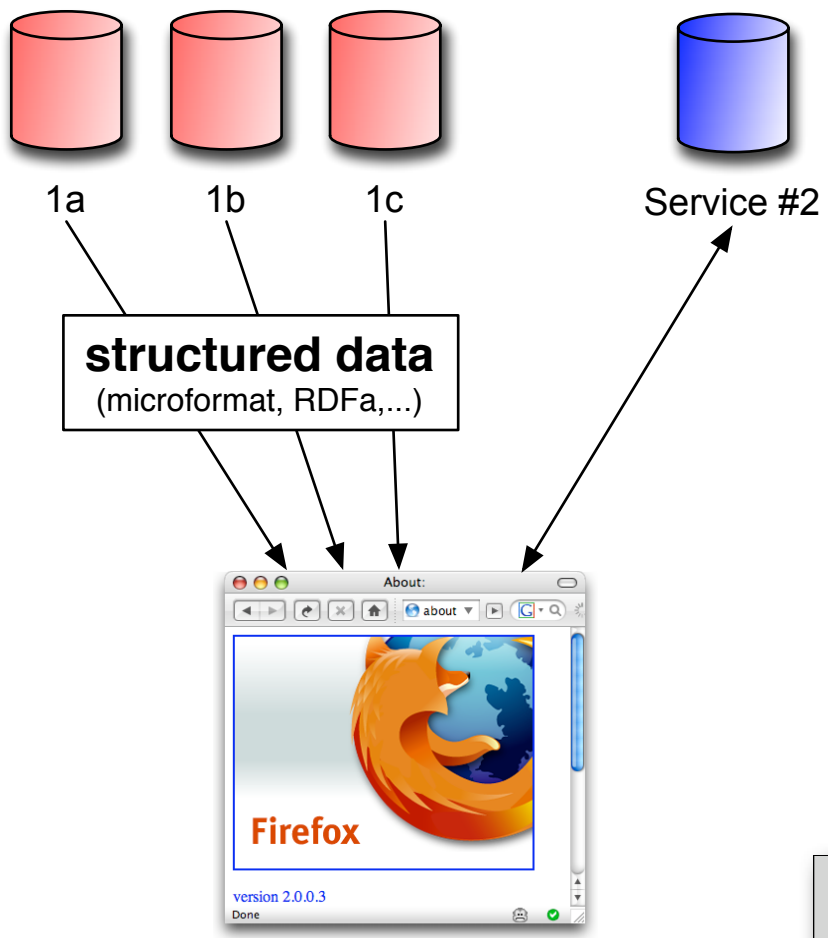
```
with_cleanslate {
  // access DOM

  // call standard JavaScript API

  // ...
}
```

2. Fine-Grained Permissions

- **Limited Awakening:** extension takes control *only* when the user invokes it.
- **Limited Network Access:** extension can access only hosts on which it is invoked.



3. Metadata-Mediated Extensions



- web services contain structured data.
- the data type triggers the appropriate extension.
- the extension can contact its own web-based service.
- (extension may not even need to contact 1a, 1b, 1c.)

watch for the Operator FF Extension

Browser = Platform

- **Isolation**
- **Fine-Grained Permissions**
- **Structured Data for Inter-Application Communication**

Enhancements are backwards-compatible with today's web

http://flickr.com/photos/hollywoodpoodle/373053089/

Questions?

http://ben.adida.net/presentations/