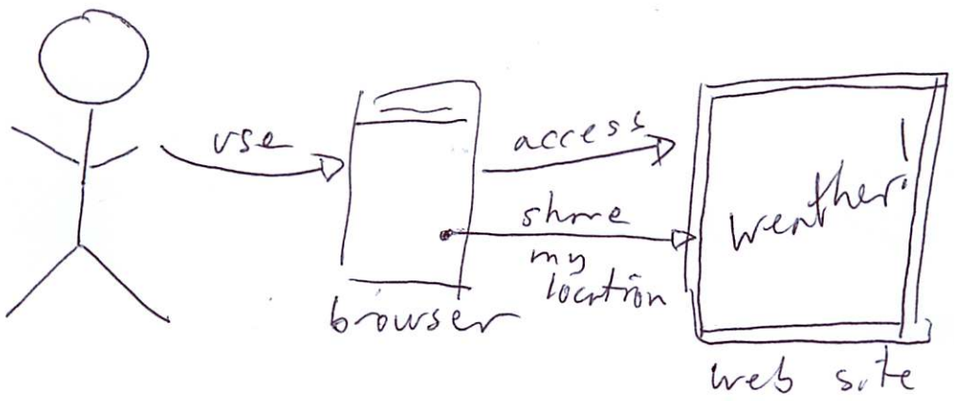
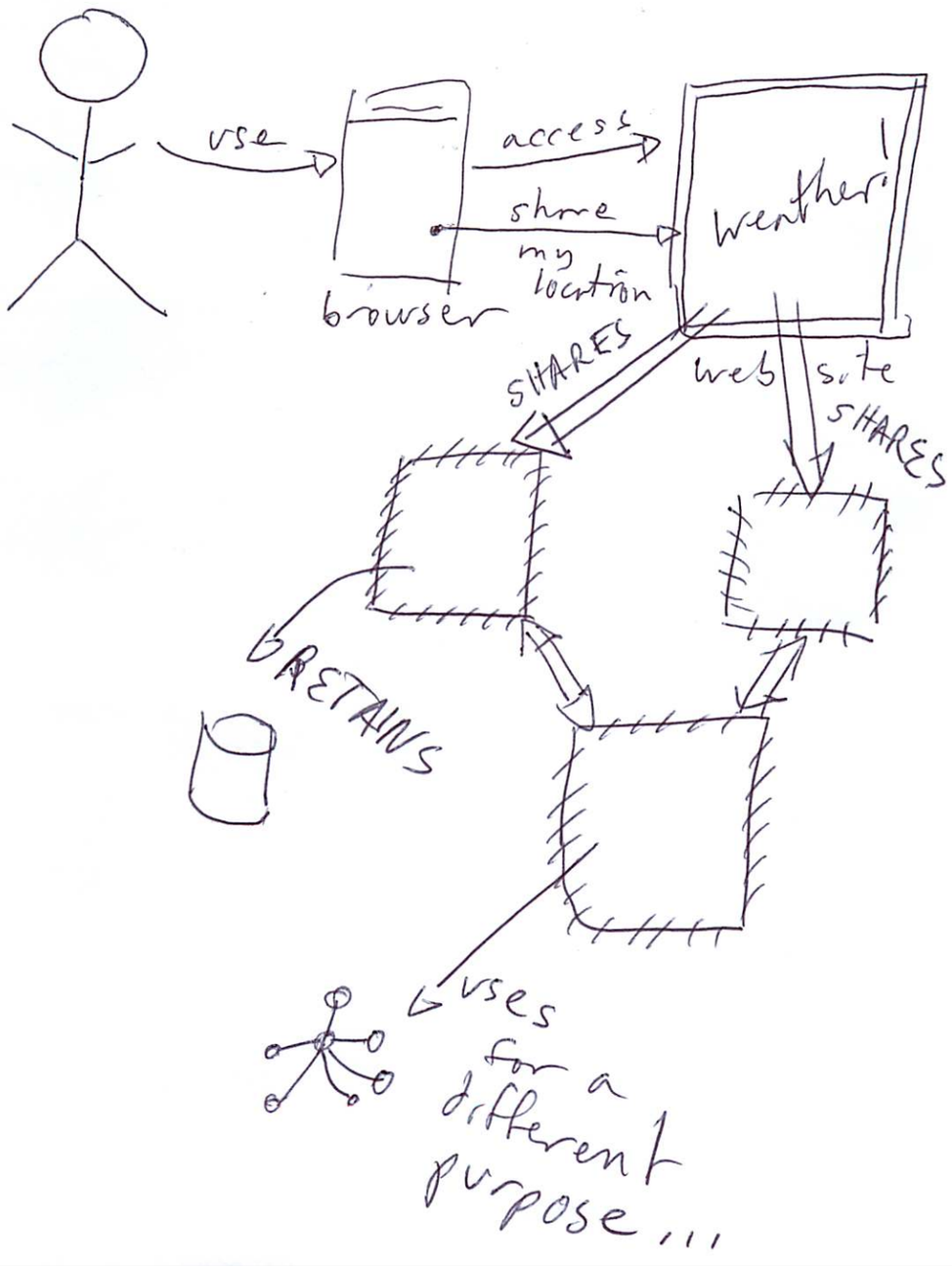
“User choice vs. Protecting users by default"

Frederick Hirsch, Nokia, @fjhirsch
Chair W3C Device APIs WG
20 November 2014

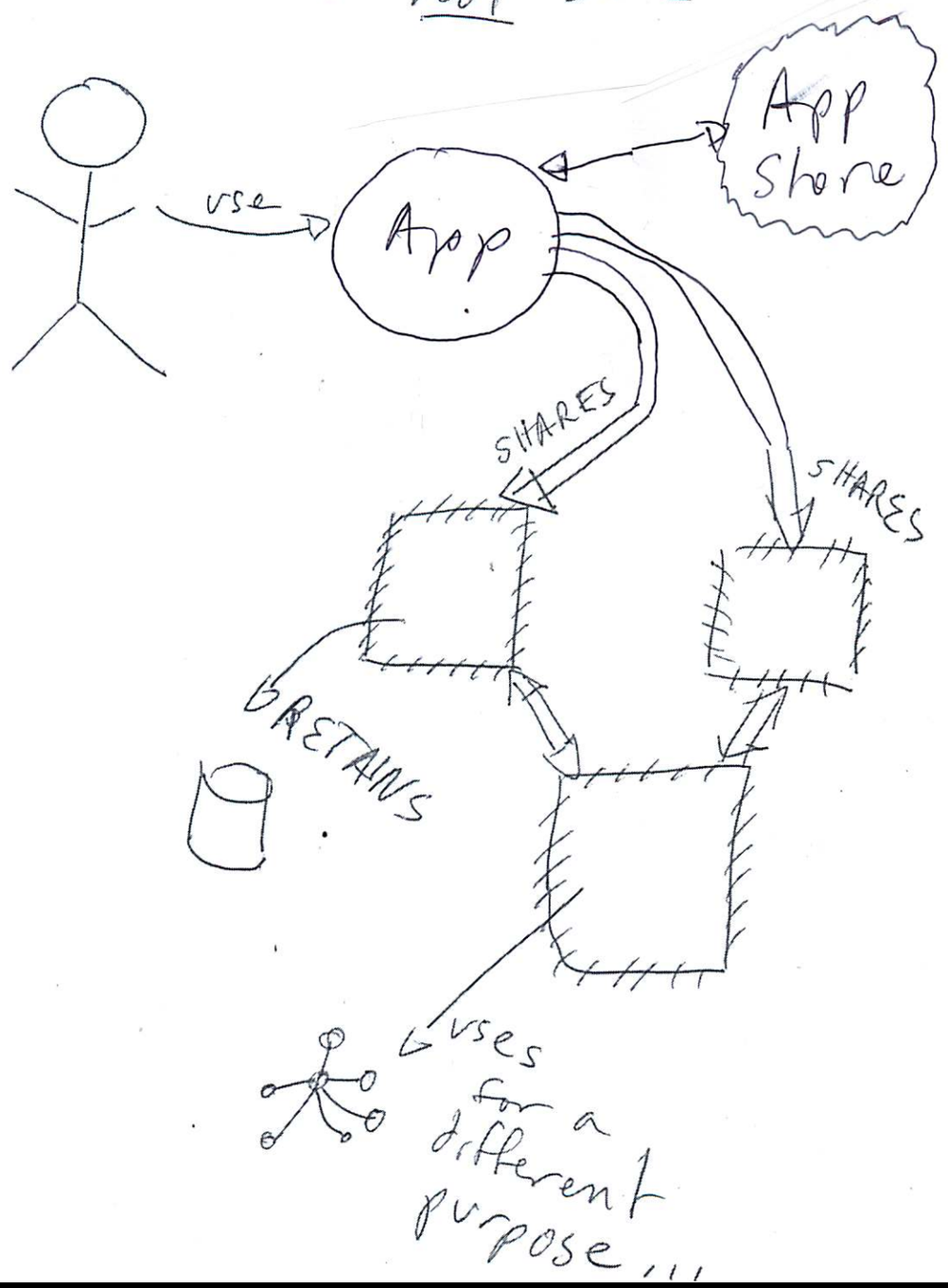
what the "user" sees

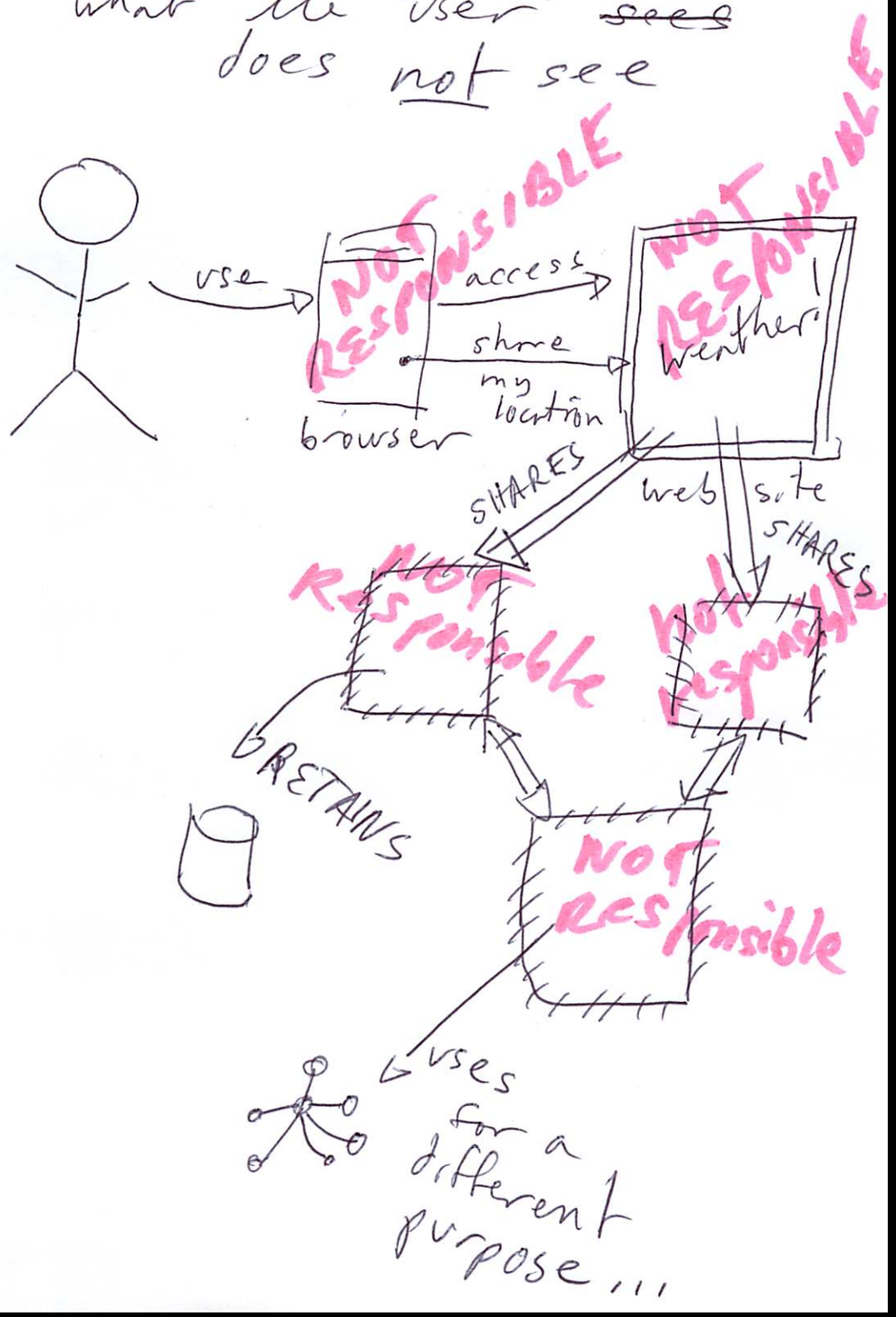


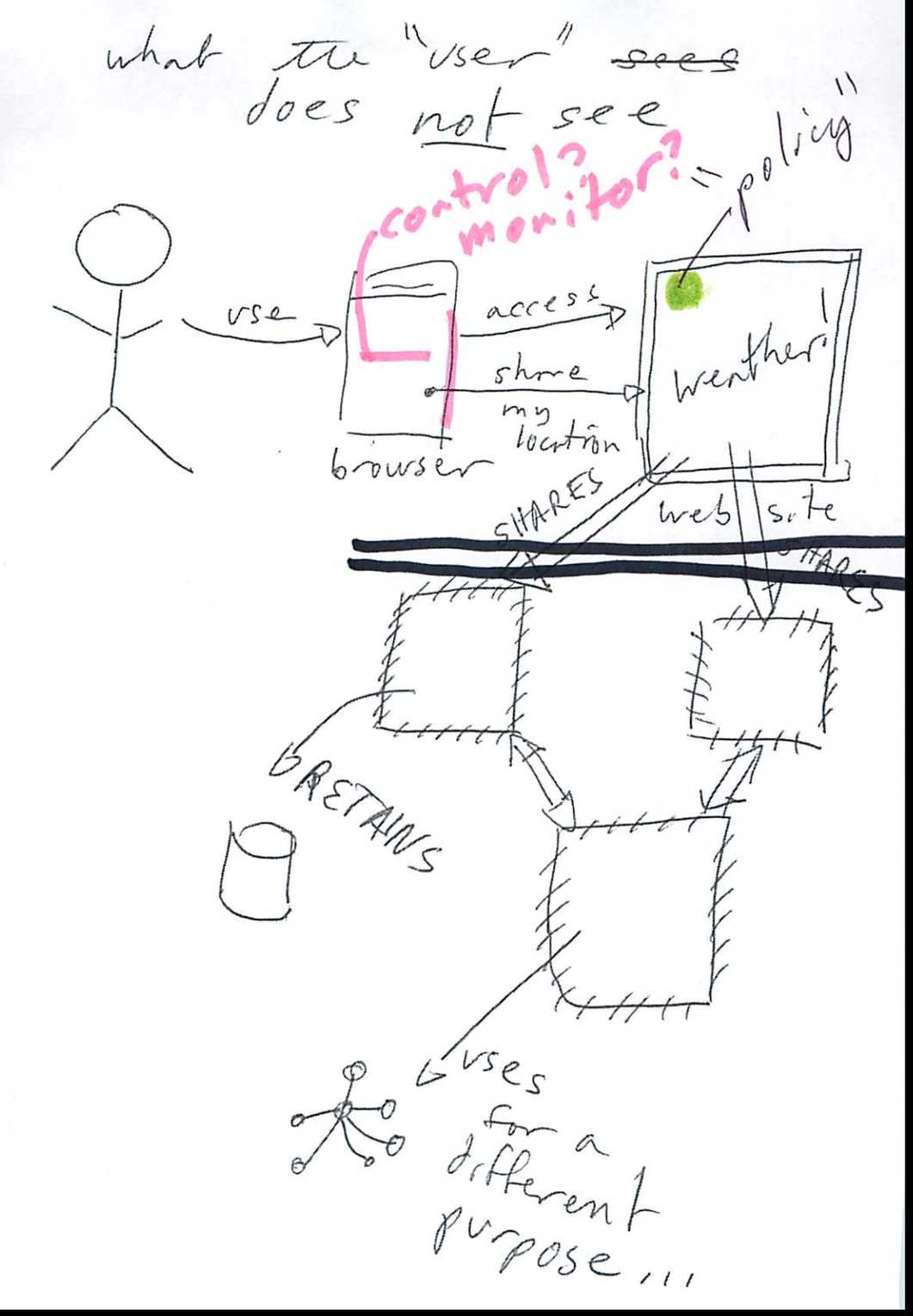
what the "user" ~~sees~~
does not see



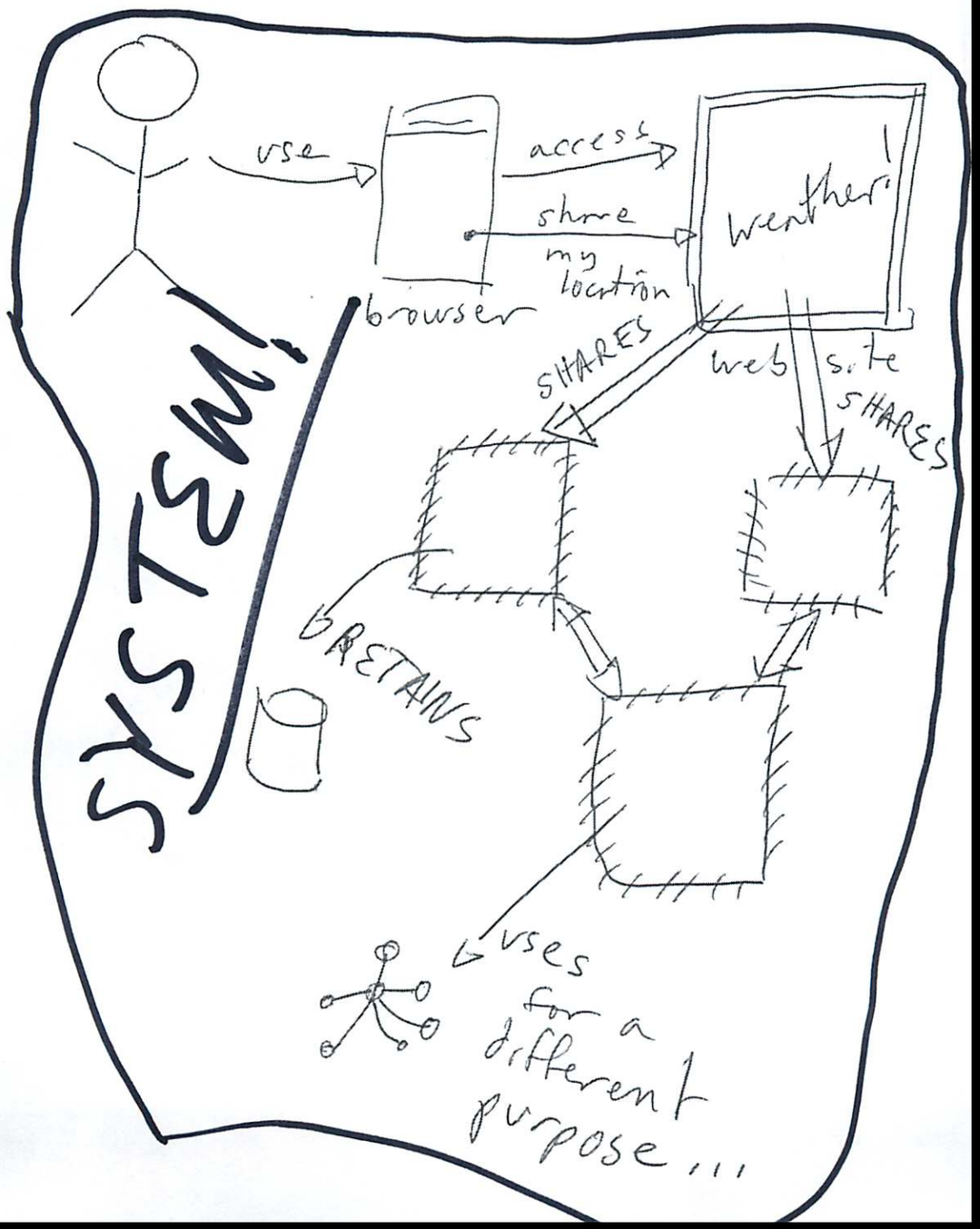
what the "user" ~~sees~~
does not see



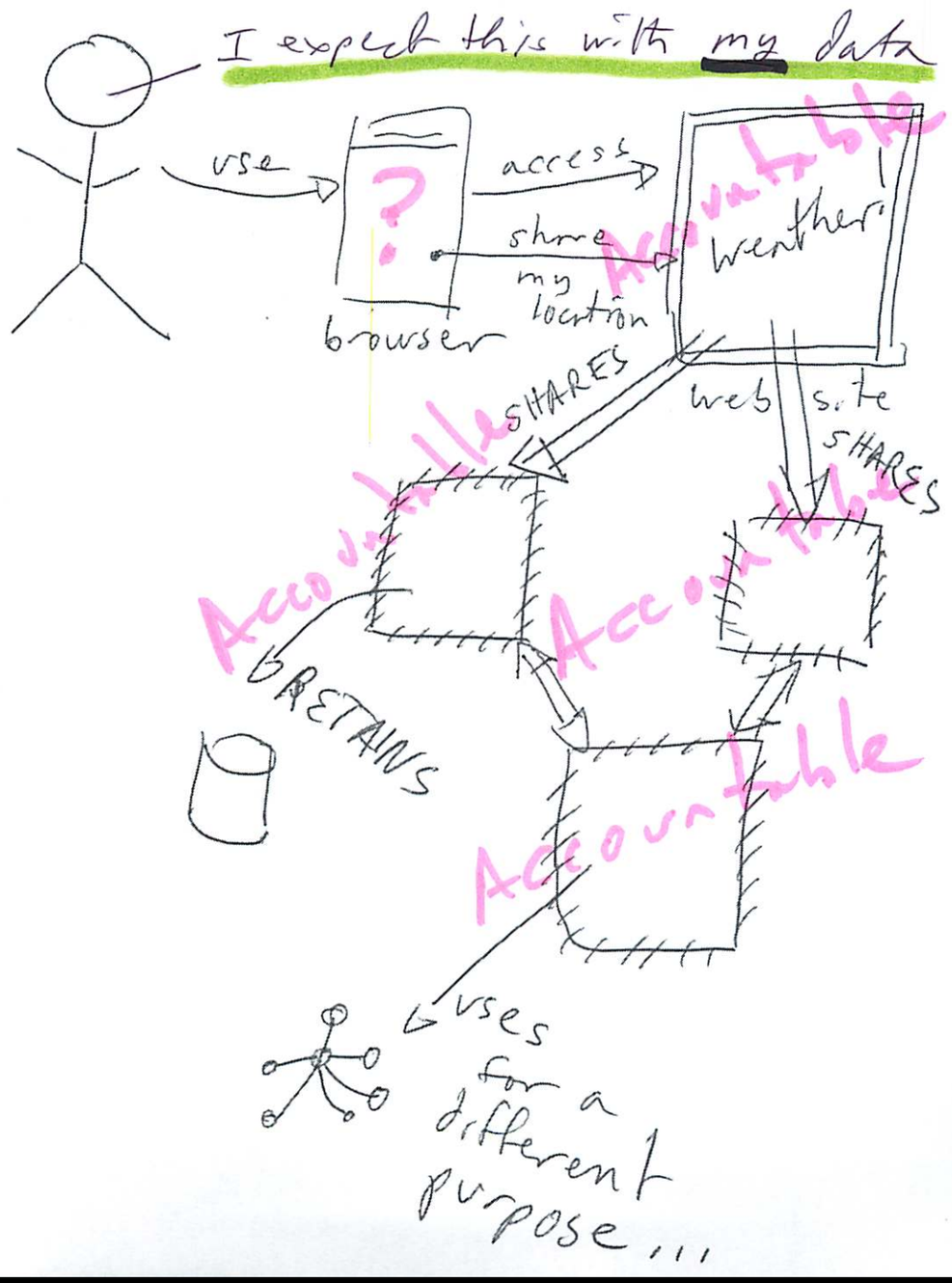

what the "user" ~~sees~~
does not see
use
access
share
my location
browser
weather
web site
SHARES
SHARES
RETAINS
uses for a different purpose...
NOT RESPONSIBLE
NOT RESPONSIBLE
NOT RESPONSIBLE
not responsible
Not Responsible


what the "user" ~~sees~~
does not see
control? monitor? = policy
use
access
share my location
browser
weather
SHARES
web site
SHARES
BRETAINS
uses for a different purpose...

what the "user" ~~sees~~
does not see



what the "user" ~~sees~~
does not see

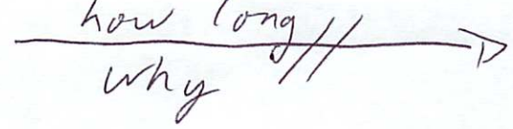


- App, Operating System
- Browser, Web Application
- App Store, Search/Discovery
- Network
- Service Providers, Backend Systems

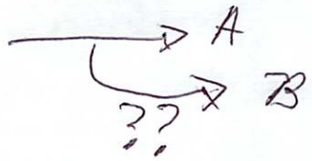
How much?

Minimize 

How long?

Retention 

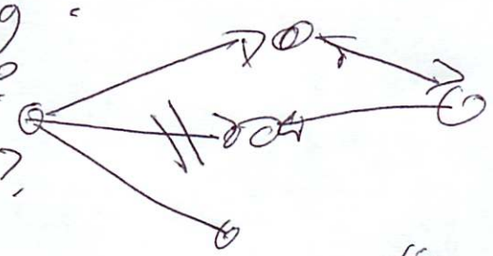
what for?

Secondary Use 

sharing?

Limits?

purpose?



Consent? 

User Desires

Meaningful?

Timely?

Implicit?

Feasible?

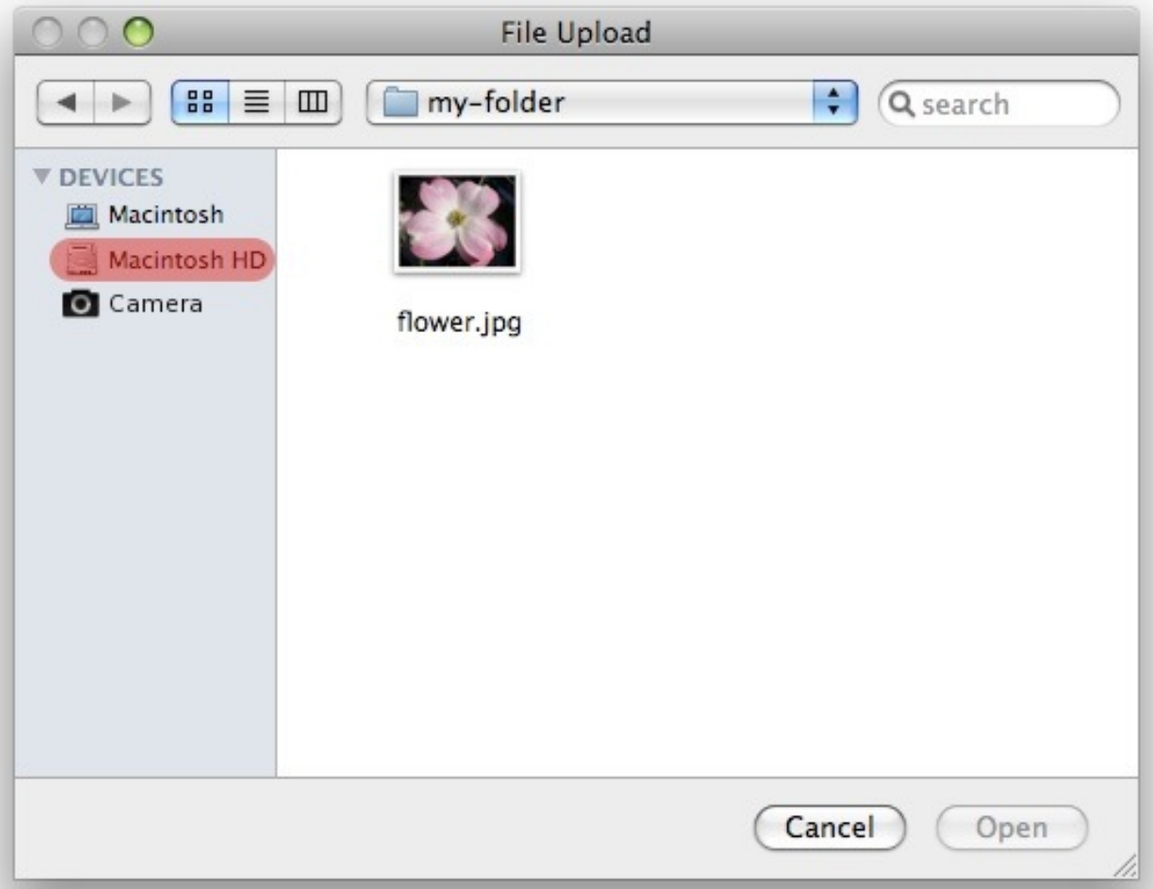
EXAMPLE 1

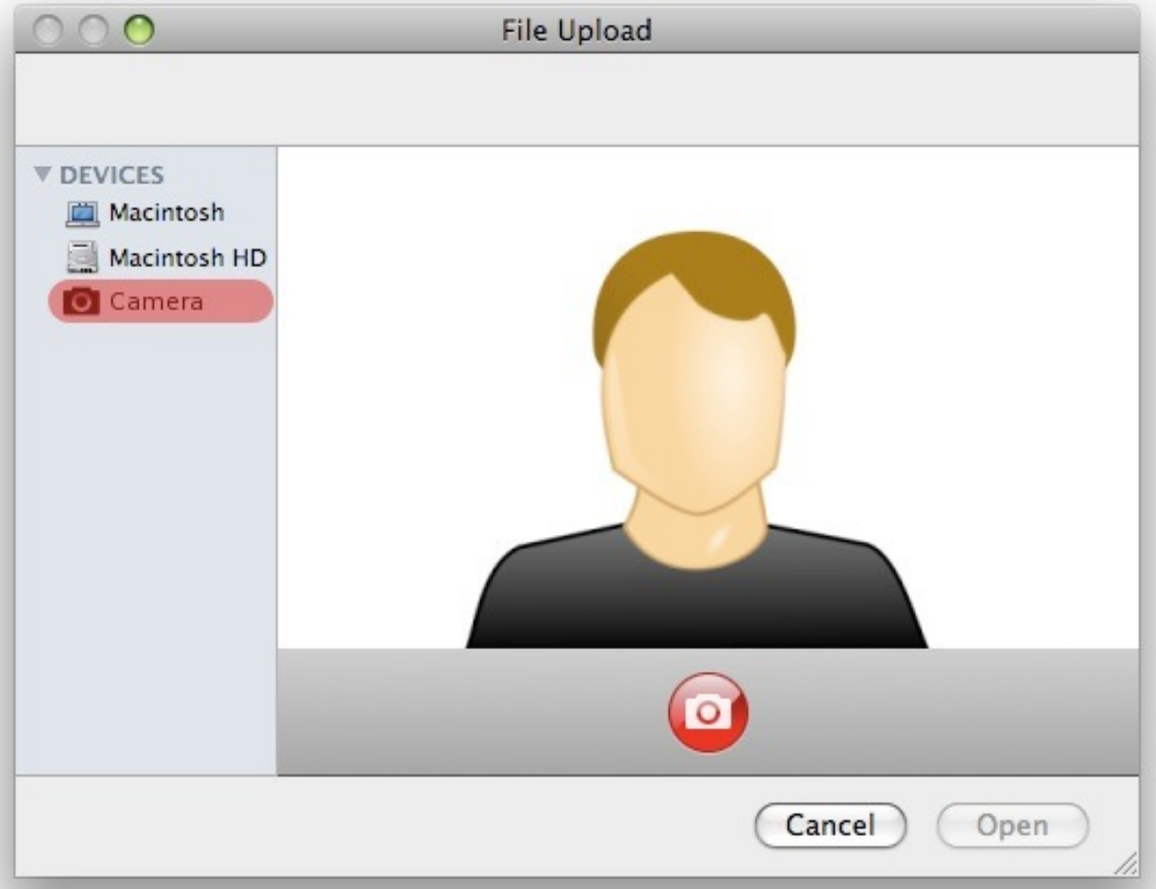
```
<form action="server.cgi" method="post" enctype="multipart/form-data">
  <input type="file" name="image" accept="image/*" capture>
  <input type="submit" value="Upload">
</form>
```

EXAMPLE 4

```
<input type="file" accept="image/*" capture>
<canvas></canvas>
```

When an `input` element's `accept` attribute is set to `image/*` and the `capture` attribute is specified as in the Example 1 or Example 4, the file picker may render as presented on the right side. When the attribute is not specified, the file picker may render as represented on the left side.





Least permissive:

```
sharing=internal
secondary-use=contextual
retention=no
```

The least permissive ruleset says that the user wants her data shared only internally by the data collector and organizations that help the data collector deliver the service, only used for contextual purposes (which includes contextual advertising), and not retained beyond the baseline period.

Internal customization/personalization:

```
sharing=internal
secondary-use=customization
retention=short
```

Some users may want to permit their data to be used internally by the data collector to do individualized analytics or provide some personalization based on recent activity, but not for marketing purposes. This ruleset, which allows data to be retained for a limited period and used for customization but not shared, corresponds to that set of preferences.

Profile-based advertising:

```
sharing=internal
secondary-use=marketing-or-profiling
retention=long
```

If users want to allow the data collector to use their data in profiles that are later used to target ads back to them, this ruleset would allow for that, with sharing still limited for internal use but with marketing, profiling, and retention allowed.

Public:

```
sharing=public
secondary-use=contextual
retention=long
```

This ruleset lets users express their permission to have their data shared publicly, but not used by the data collector for non-contextual purposes.

Most permissive:

```
sharing=internal
sharing=affiliates
sharing=unrelated-companies
secondary-use=contextual
secondary-use=customization
secondary-use=marketing-or-profiling
retention=long
```

The most permissive ruleset allows all three kinds of sharing, all three kinds of secondary use, and indefinite retention.

“User choice vs. Protecting users by default”

what is the right question?

Additional information

Device API Privacy Requirements , Alissa Cooper, Frederick Hirsch, John Morris
http://www.w3.org/TR/2010/NOTE-dap-privacy-reqs-20100629/

Web Application Privacy Best Practices, Frederick Hirsch
http://www.w3.org/TR/2012/NOTE-app-privacy-bp-20120703/

Privacy Rulesets, Alissa Cooper, John Morris, Erica Newland
http://dev.w3.org/2009/dap/privacy-rulesets/

Privacy Workshop Position Paper - The DAP Perspective, Robin Berjon, Frederick Hirsch
http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-11.html

Position Paper: Privacy And Policy In The DAP Wg A Dap Perspective,
Frederick Hirsch, Robin Berjon
http://www.w3.org/2010/policy-ws/papers/14-Hirsch-Berjon-DAP.html

HTML Media Capture, Anssi Kostiainen
http://www.w3.org/TR/2014/CR-html-media-capture-20140909/

W3C Device APIs Working Group
http://www.w3.org/2009/dap/