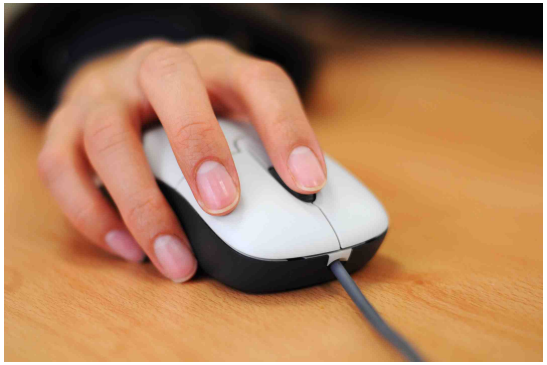
Privacy concerns of implicit secondary factors for web authentication

Joseph Bonneau
Edward Felten
Prateek Mittal
Arvind Narayanan

WAY Workshop 2014

Passwords +…



Behavioral/soft biometrics

Passwords +...

191.255.255.255

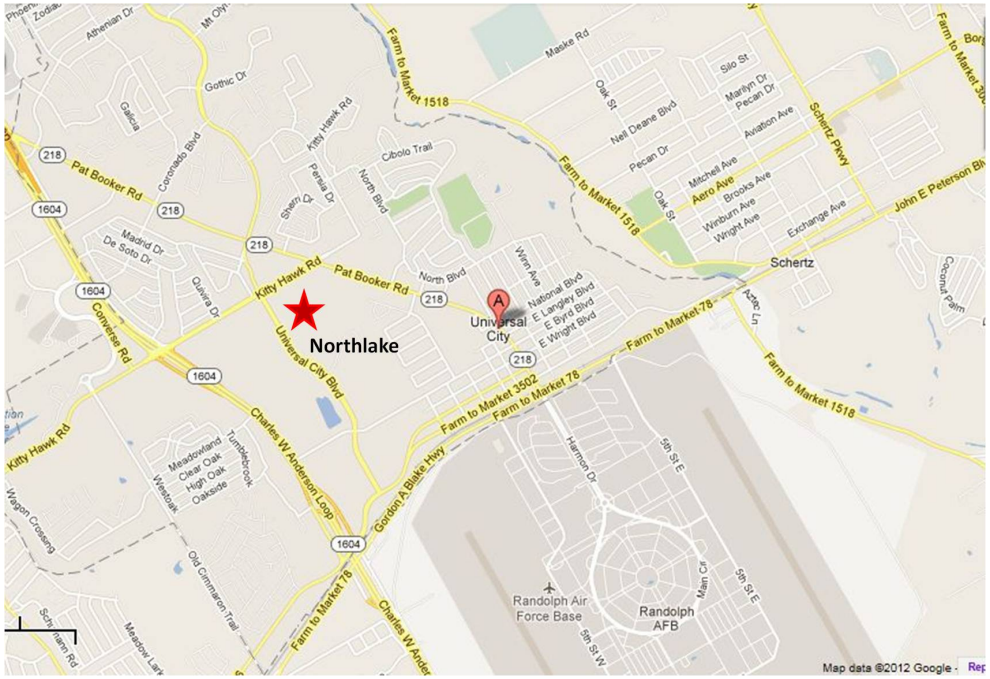
Mozilla/5.0 (iPad; U; CPU OS 3_2_1 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Mobile/7B405

Set-Cookie:
id=0x987fe1;
Expires=Wed,
09 Jun 2021
10:18:14 GMT

```
var x = window.screen.availWidth;
var y  = window.screen.availHeight;
```

User agent information

Passwords +...



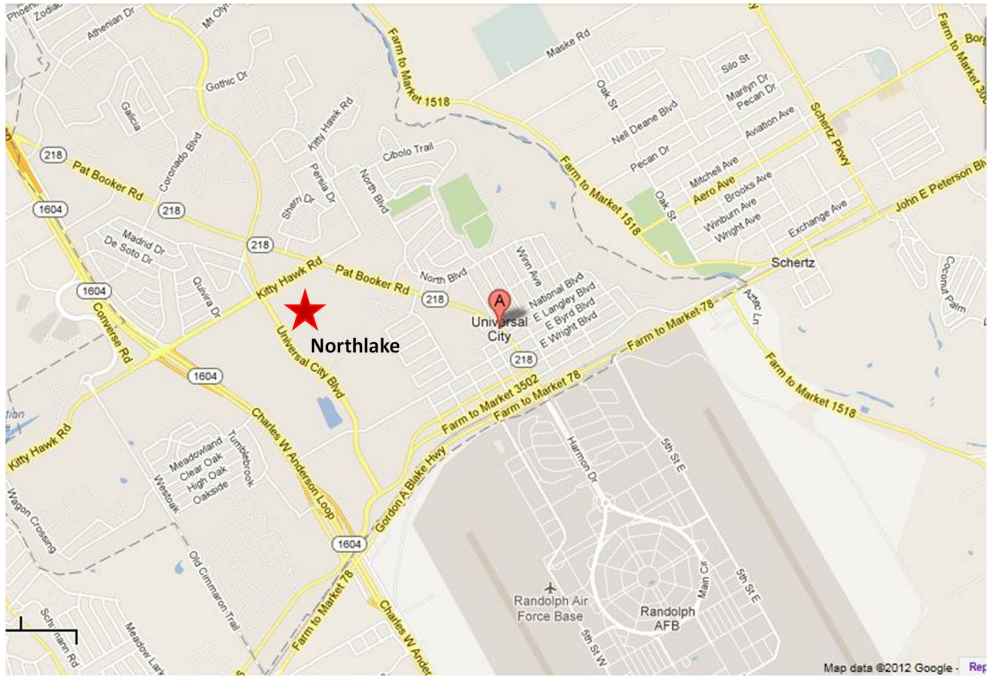
Usage patterns

Three privacy(ish) effects

I. Data permanence
II. Inherent sensitivity
III. Legitimate secondary uses

Data permanence

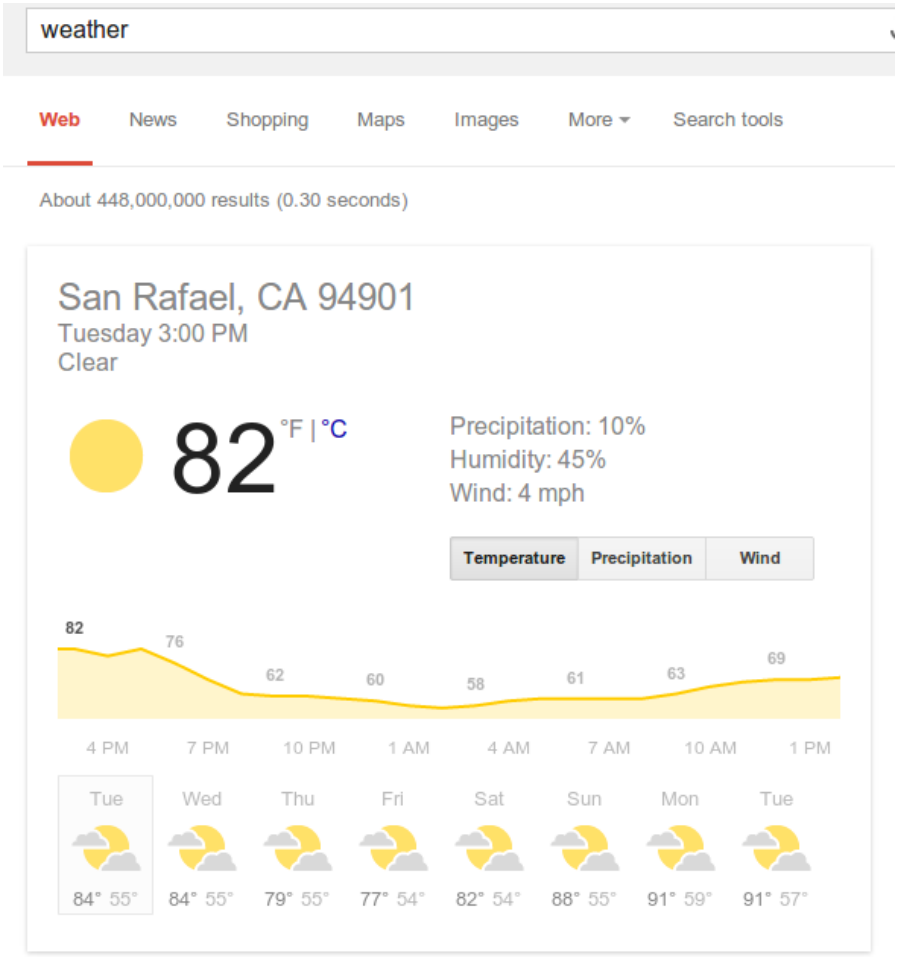
Inherent sensitivity

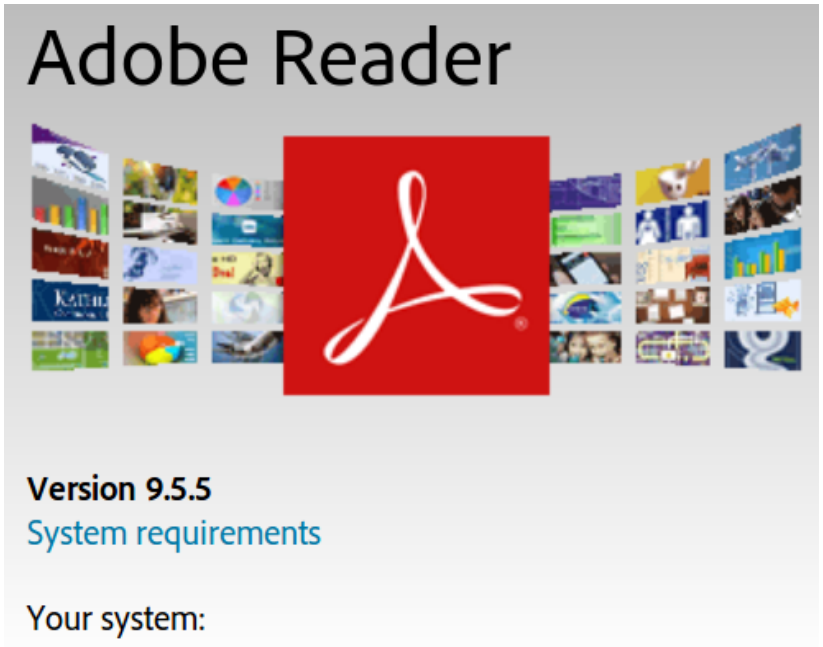


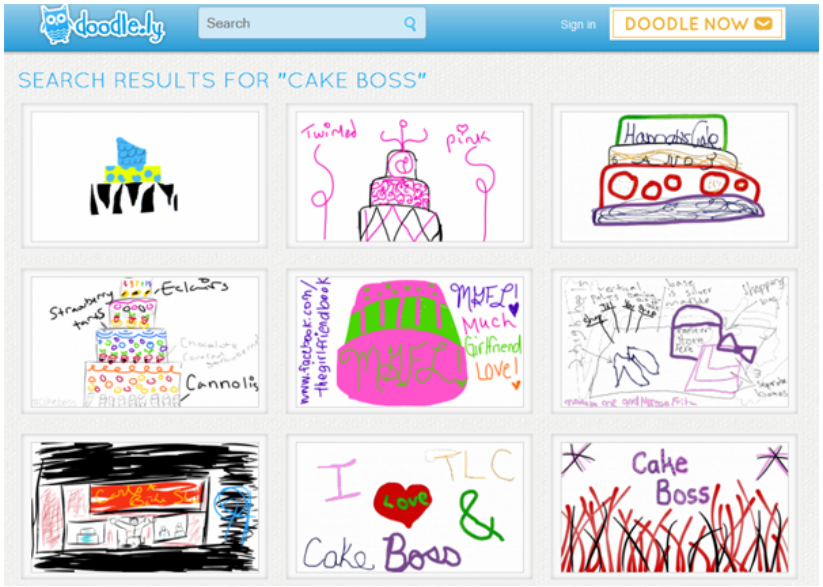
Your Recent Activity

Date	Event	Location
Jun 15	Signed in from Chrome (Nexus 5)	Philadelphia, PA, USA
Jun 12	Signed in from Chrome (Linux)	New York NY, New Jersey, USA
Jun 12	Created a new app password	Franklin Township, NJ, USA
Jun 12	Signed in from Chrome (Linux)	New York NY, New Jersey, USA

Legitimate uses







Research challenges

Signal extraction

➔ How fast can a game learn your typing/swiping/clicking style?

➔ Do we need more permissions?

Privacy-preserving authentication

- ➔ Privacy-preserving machine learning exists already
- ➔ Can we adapt it for authentication?
- ➔ Data minimization?

Returns to centralization

- ➔ Data already collected
- ➔ Data collected *frequently*
- ➔ Third party logins are a signal, too

- ➔ Are small services doomed?

Thank you!

jbonneau@princeton.edu
felten@cs.princeton.edu
pmittal@princeton.edu
arvindn@princeton.edu