Privacy Design Patterns and Anti-Patterns

Patterns Misapplied and Unintended Consequences

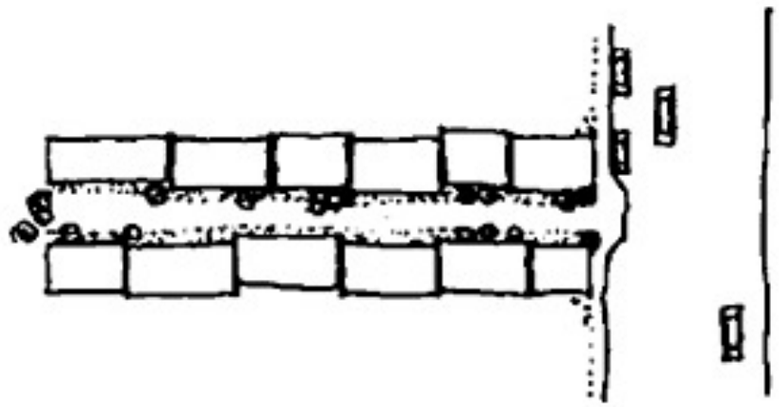
Nick Doty & Mohit Gupta
UC Berkeley, School of Information

Privacy-by-Design
... *in practice*

- for designers and developers of technologies
- document and share techniques, rather than normative requirements

✣ ✣ ✣

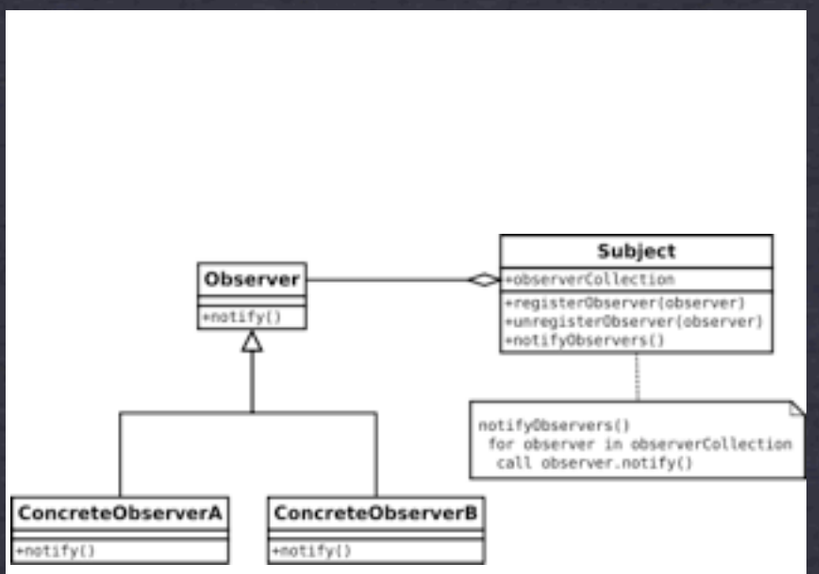
Mark the neighborhood, above all, by gateways wherever main paths enter it—MAIN GATEWAYS (53)—and by modest boundaries of non-residential land between the neighborhoods—NEIGHBORHOOD BOUNDARY (15). Keep major roads within these boundaries —PARALLEL ROADS (23); give the neighborhood a visible center, perhaps a common or a green—ACCESSIBLE GREEN (60)—or a SMALL PUBLIC SQUARE (61); and arrange houses and workshops

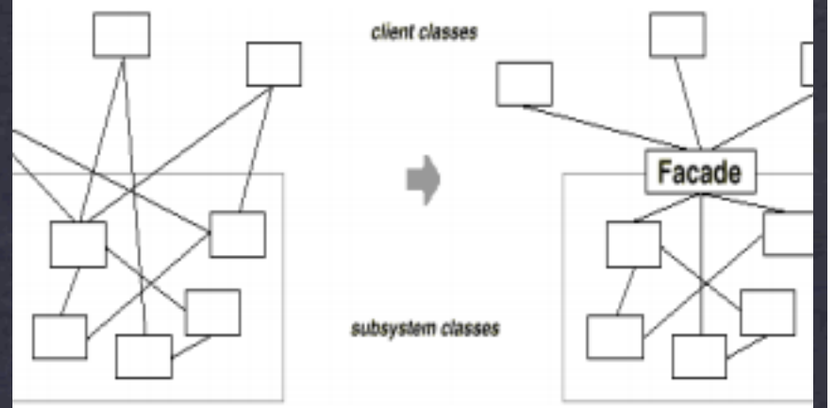


Houses long and thin along the path.

✣ ✣ ✣

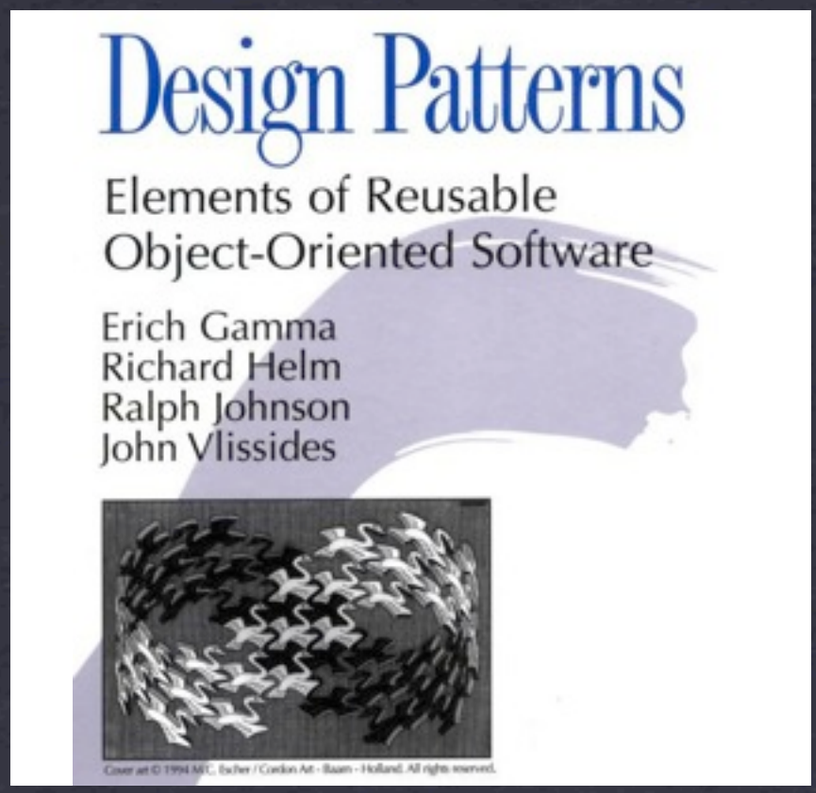
And again, make the house an individual piece of territor
th its own garden, no matter how small—YOUR OWN HOM
9); make the main room essentially a kind of farmhouse kitch
FARMHOUSE KITCHEN (139), with alcoves opening off it f
ing, working, bathing, sleeping, dressing—BATHING ROO
44), WINDOW PLACE (180), WORKSPACE ENCLOSURE (183
D ALCOVE (188), DRESSING ROOM (189); if the house is mea
an old person, or for someone very young, shape it also a
ding to the pattern for OLD AGE COTTAGE (155) or TEE
ER'S COTTAGE (154). . . .





Java

The Facade Pattern
3



PRIVACY DESIGN PATTERNS

http://privacypatterns.org


privacypatterns.org

Asynchronous notice

Intent

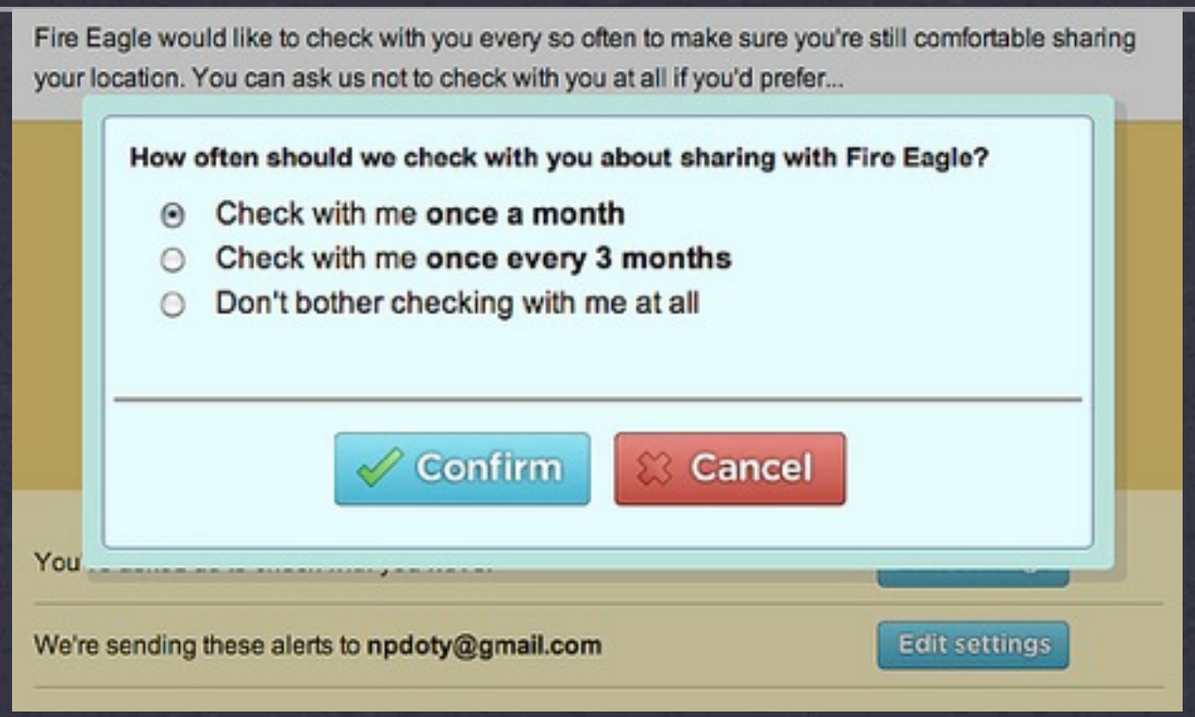
Context

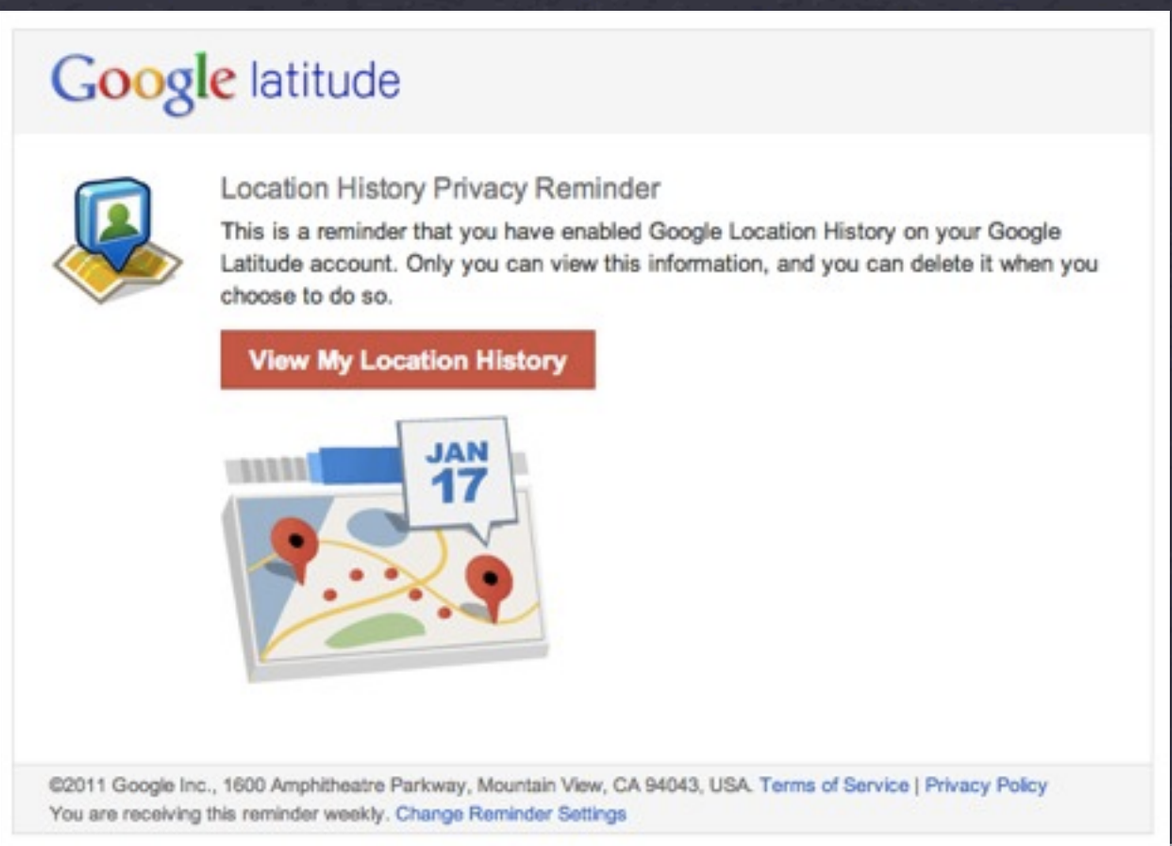
Problem

Solution

Examples

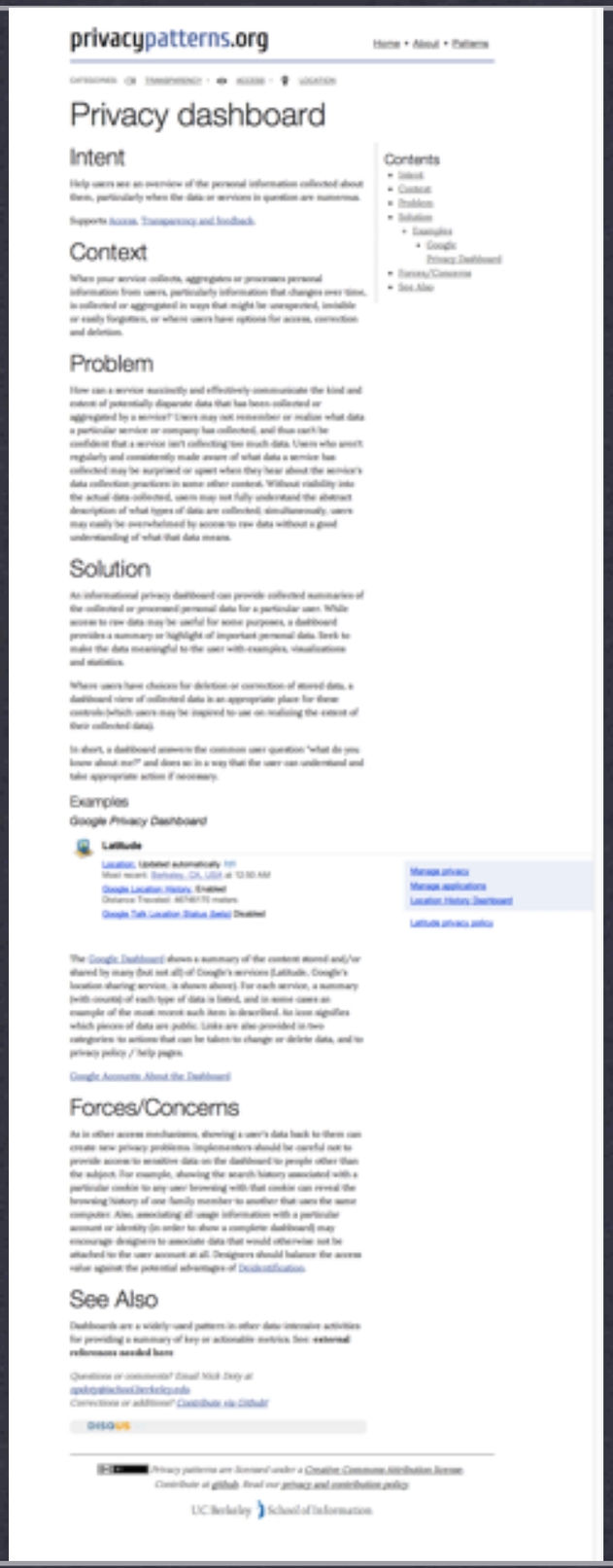
Forces/Concerns





ASYNCHRONOUS NOTICE

http://privacypatterns.org/patterns/Asynchronous-notice


privacypatterns.org

Home • About • Patterns

Privacy dashboard

Intent

Help users see an overview of the personal information collected about them, particularly when the data or services in question are numerous.

Supports Access, Transparency and Feedback.

Contents

- Intent
- Context
- Problem
- Solution
- Examples
  - Google
    Privacy Dashboard
- Forces/Concerns
- See Also

Context

When your service collects, aggregates or processes personal information from users, particularly information that changes over time, is collected or aggregated in ways that might be unexpected, invisible or easily forgotten, or where users have options for access, correction and deletion.

Problem

How can a service succinctly and effectively communicate the kind and extent of potentially disparate data that has been collected or aggregated by a service? Users may not remember or realize what data a particular service or company has collected, and thus can't be confident that a service isn't collecting too much data. Users who aren't regularly and consistently made aware of what data a service has collected may be surprised or upset when they hear about the service's data collection practices in some other context. Without visibility into the actual data collected, users may not fully understand the abstract description of what types of data are collected; simultaneously, users may easily be overwhelmed by access to raw data without a good understanding of what that data means.

Solution

An informational privacy dashboard can provide collected summaries of the collected or processed personal data for a particular user. While access to raw data may be useful for some purposes, a dashboard provides a summary or highlight of important personal data. Seek to make the data meaningful to the user with examples, visualizations and statistics.

Where users have choices for deletion or correction of stored data, a dashboard view of collected data is an appropriate place for these controls (which users may be inspired to use on realizing the extent of their collected data).

In short, a dashboard answers the common user question "what do you know about me?" and does so in a way that the user can understand and take appropriate action if necessary.

Examples

Google Privacy Dashboard

Latitude

Location: Updated automatically

Most recent: Berkeley, CA, USA at 12:50 AM

Google Location History: Enabled

Distance Traveled: 46746170 meters

Google Talk Location Status (beta): Disabled

Manage privacy

Manage applications

Location History Dashboard

Latitude privacy policy

The Google Dashboard shows a summary of the content stored and/or shared by many (but not all) of Google's services (Latitude, Google's location sharing service, is shown above). For each service, a summary (with counts) of each type of data is listed, and in some cases an example of the most recent such item is described. An icon signifies which pieces of data are public. Links are also provided in two categories: to actions that can be taken to change or delete data, and to privacy policy / help pages.

Google Accounts: About the Dashboard

Forces/Concerns

As in other access mechanisms, showing a user's data back to them can create new privacy problems. Implementers should be careful not to provide access to sensitive data on the dashboard to people other than the subject. For example, showing the search history associated with a particular cookie to any user browsing with that cookie can reveal the browsing history of one family member to another that uses the same computer. Also, associating all usage information with a particular account or identity (in order to show a complete dashboard) may encourage designers to associate data that would otherwise not be attached to the user account at all. Designers should balance the access value against the potential advantages of Deidentification.

See Also

Dashboards are a widely-used pattern in other data-intensive activities for providing a summary of key or actionable metrics. See: **external references needed here**

Questions or comments? Email Nick Doty at npdoty@ischool.berkeley.edu

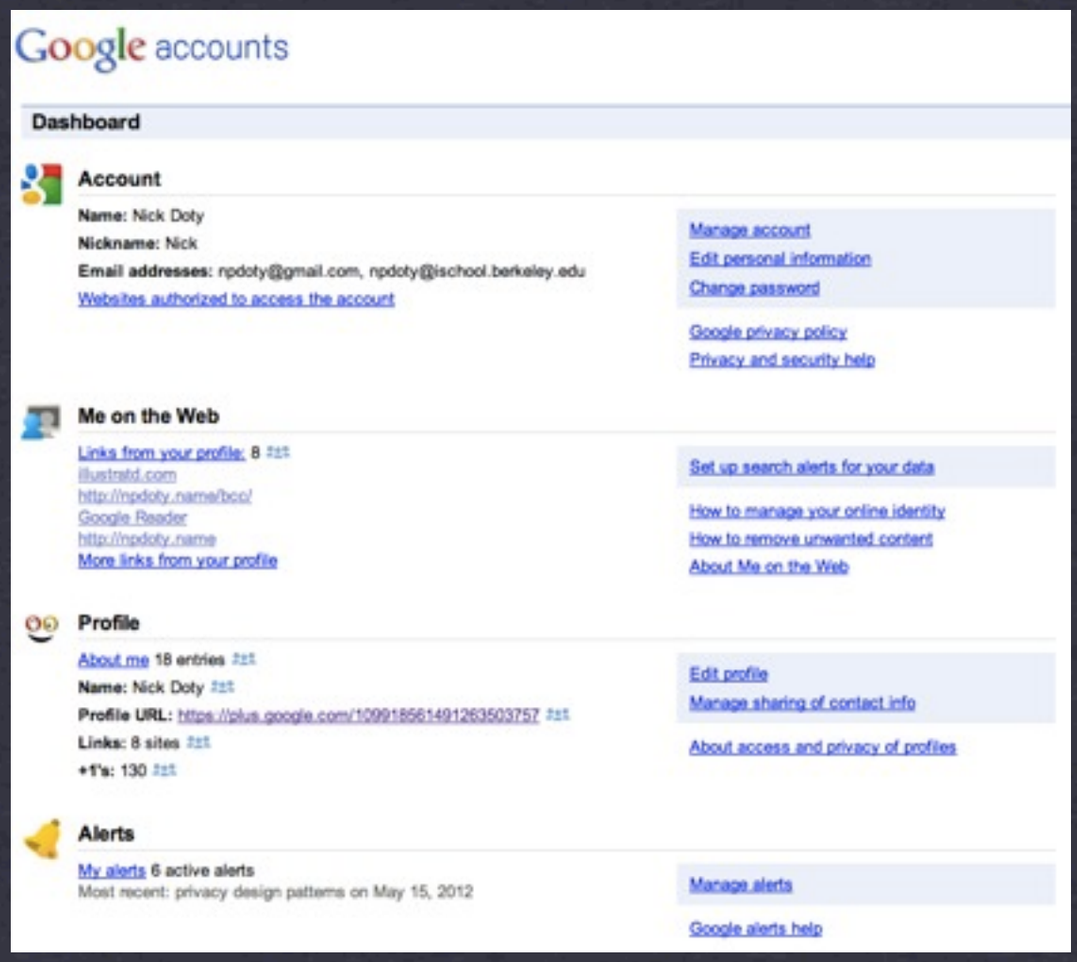
Corrections or additions? Contribute via Github!

DISQUS

Privacy patterns are licensed under a Creative Commons Attribution license

Contribute at github. Read our privacy and contribution policy.

UC Berkeley School of Information


Google accounts

Dashboard

Account

Name: Nick Doty

Nickname: Nick

Email addresses: npdoty@gmail.com, npdoty@ischool.berkeley.edu

Websites authorized to access the account

Manage account

Edit personal information

Change password

Google privacy policy

Privacy and security help

Me on the Web

Links from your profile: 8

@ustratd.com

http://npdoty.name/bcc/

Google Reader

http://npdoty.name

More links from your profile

Set up search alerts for your data

How to manage your online identity

How to remove unwanted content

About Me on the Web

Profile

About me 18 entries

Name: Nick Doty

Profile URL: https://plus.google.com/109918661491263503757

Links: 8 sites

+1's: 130

Edit profile

Manage sharing of contact info

About access and privacy of profiles

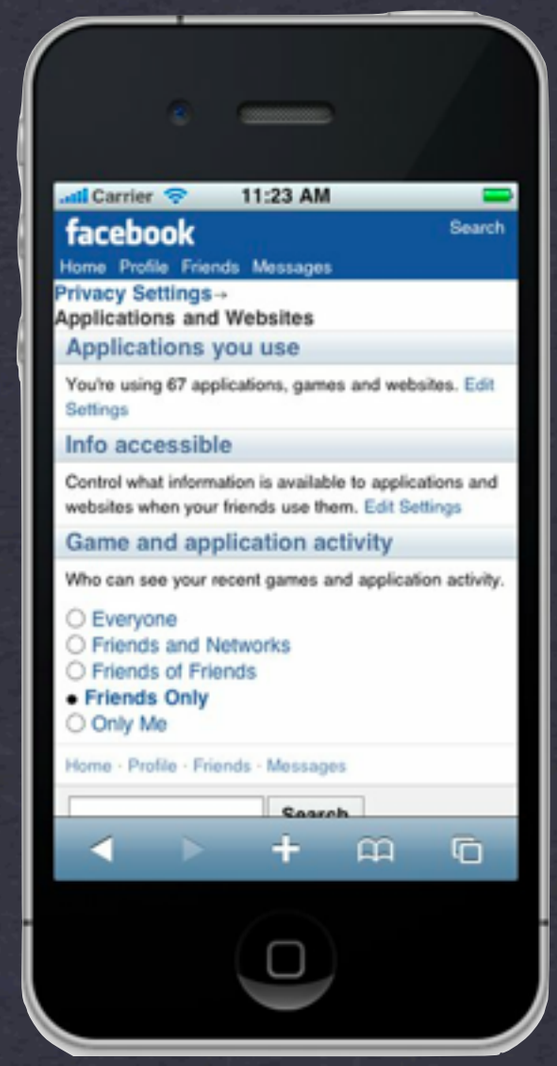
Alerts

My alerts 6 active alerts

Most recent: privacy design patterns on May 15, 2012

Manage alerts

Google alerts help



PRIVACY DASHBOARD

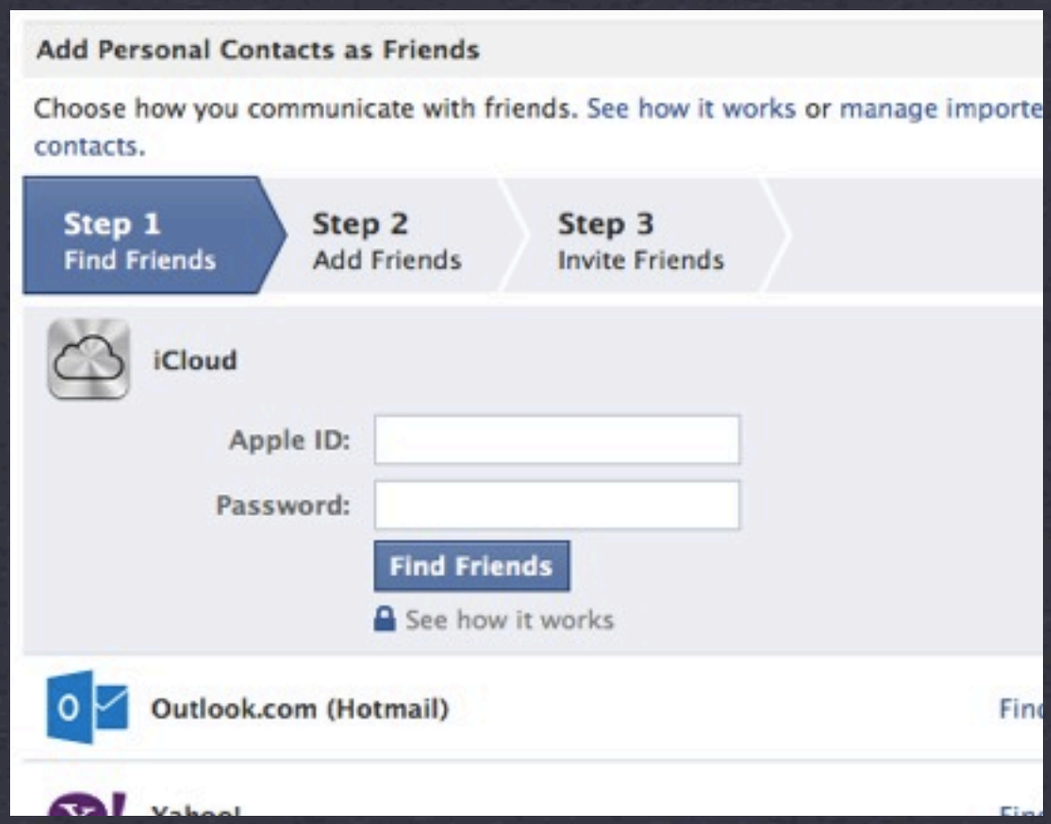
http://privacypatterns.org/patterns/Privacy-dashboard

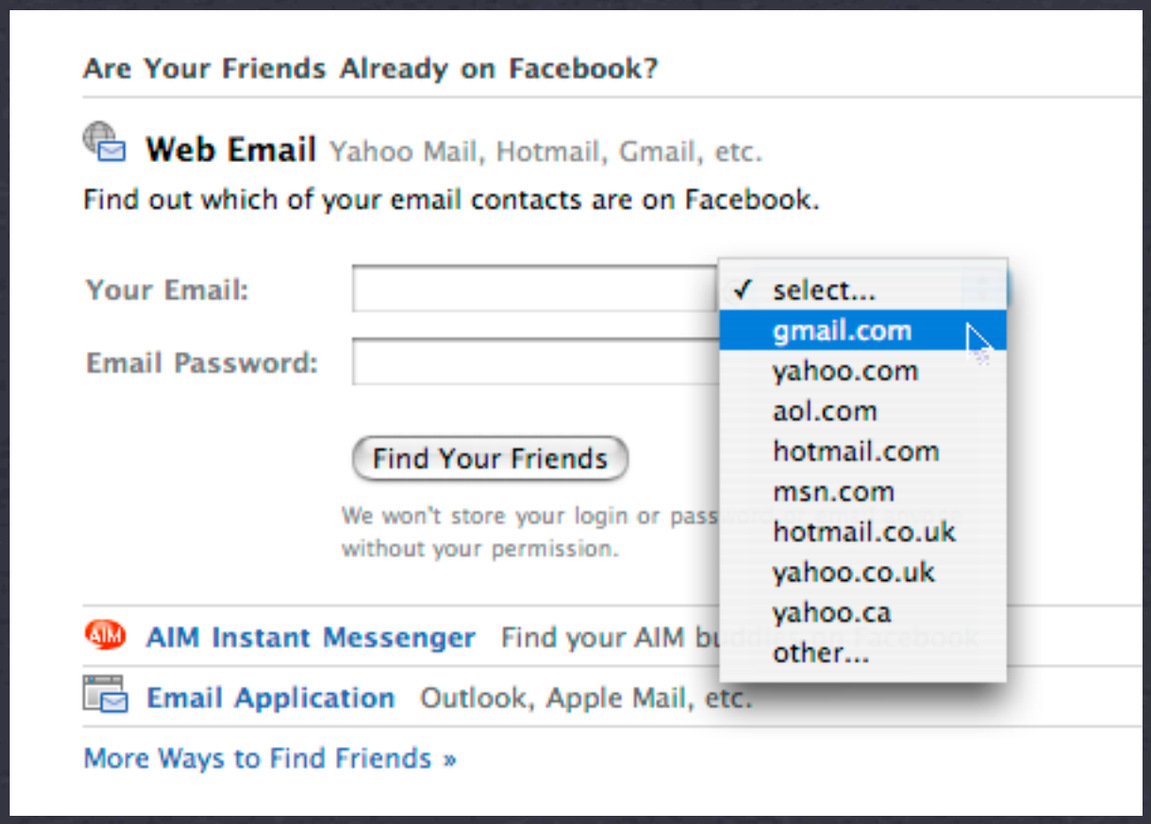
Privacy Patterns — Contribute!

http://privacypatterns.org

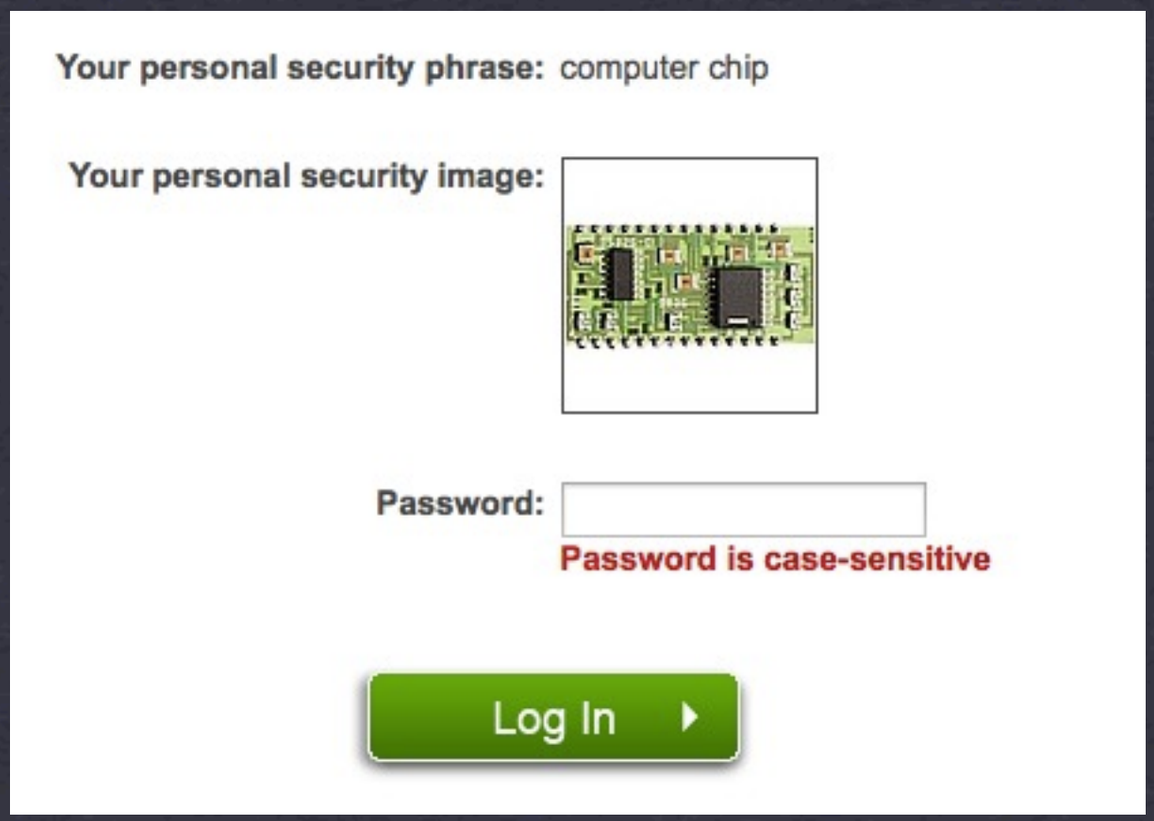
https://github.com/m0hit/privacypatterns

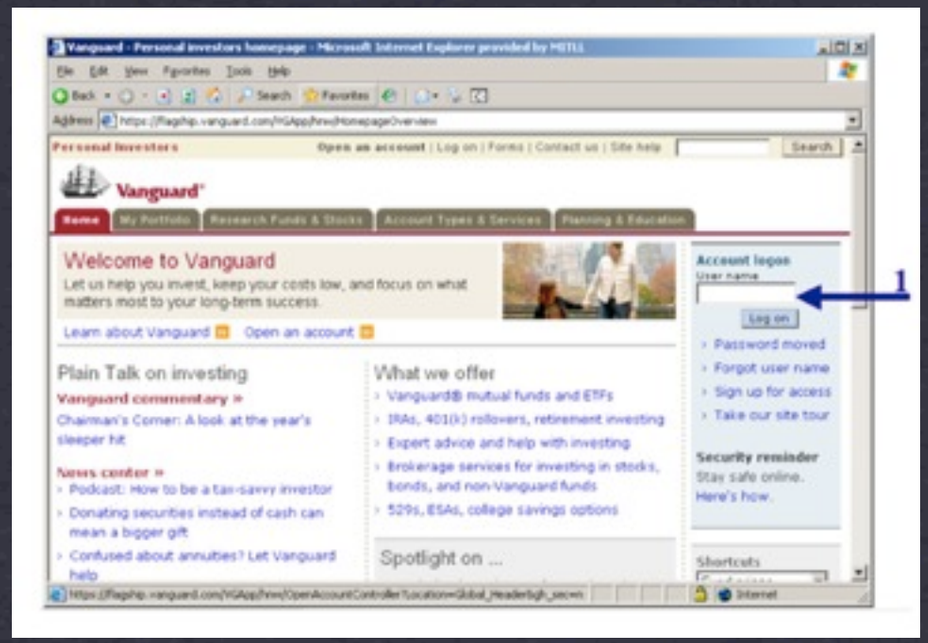
PRIVACY POLICIES

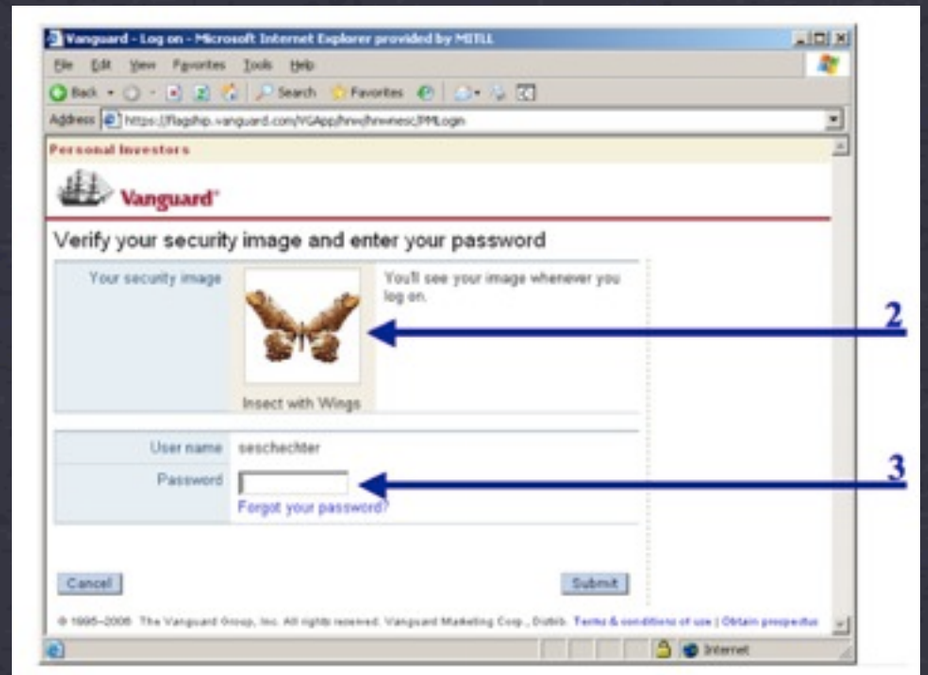




THIRD-PARTY PASSWORDS FOR DELEGATED AUTH







SECURITY IMAGES FOR SITE AUTHENTICATION

Conclusions

Nick Doty
http://npdoty.name
npdoty@ischool.berkeley.edu