

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

max. population of 500



max diameter of 300 yards

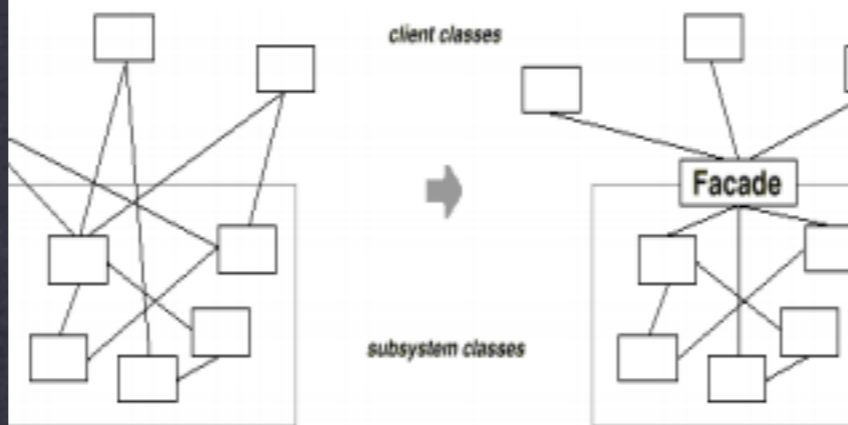
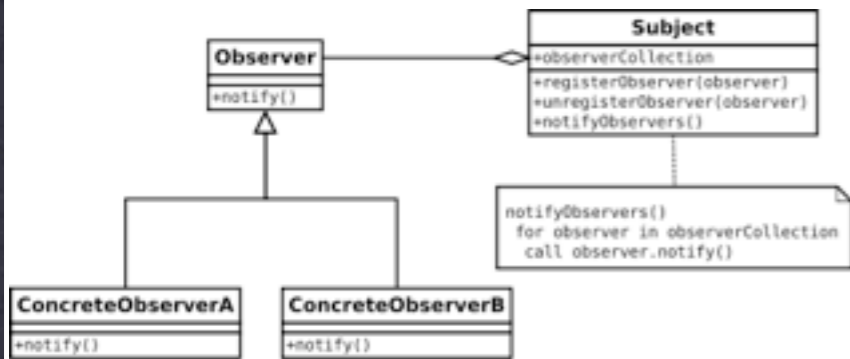
Mark the neighborhood, above all, by gateways wherever main paths enter it—MAIN GATEWAYS (53)—and by modest boundaries of non-residential land between the neighborhoods—NEIGHBORHOOD BOUNDARY (15). Keep major roads within these boundaries—PARALLEL ROADS (23); give the neighborhood a visible center, perhaps 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 territory with its own garden, no matter how small—YOUR OWN HOME (9); make the main room essentially a kind of farmhouse kitchen—FARMHOUSE KITCHEN (139), with alcoves opening off it for dining, working, bathing, sleeping, dressing—BATHING ROOM (144), WINDOW PLACE (180), WORKSPACE ENCLOSURE (183) and ALCOVE (188), DRESSING ROOM (189); if the house is meant for an old person, or for someone very young, shape it also according to the pattern for OLD AGE COTTAGE (155) or TEENAGER'S COTTAGE (154). . . .



in Java

The Facade Pattern

3

Design Patterns

Elements of Reusable Object-Oriented Software

Erich Gamma
Richard Helm
Ralph Johnson
John Vlissides



Cover art © 1994 MIT, Fisher / Corbin Art - Baan - Holland. All rights reserved.

PRIVACY DESIGN PATTERNS

<http://privacypatterns.org>

Fire Eagle would like to check with you every so often to make sure you're still comfortable sharing your location. You can ask us not to check with you at all if you'd prefer...

How often should we check with you about sharing with Fire Eagle?

Check with me once a month

Check with me once every 3 months

Don't bother checking with me at all

You

We're sending these alerts to **npdoty@gmail.com**

[Edit settings](#)

Google latitude

Location History Privacy Reminder

This is a reminder that you have enabled Google Location History on your Google Latitude account. Only you can view this information, and you can delete it when you choose to do so.

[View My Location History](#)

©2011 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. [Terms of Service](#) | [Privacy Policy](#)

You are receiving this reminder weekly. [Change Reminder Settings](#)

ASYNCHRONOUS NOTICE

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

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.

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 learn 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 highlights 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 in 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 101
 Most recent: Berkeley, CA, USA at 12:00 AM
 Google Location History, Email, Distance Traveled: 4574373 meters
 Google Talk Location Status, Data, Deleted

[Manage privacy](#)
[Manage activities](#)
[Location History Dashboard](#)
[Latitude privacy center](#)

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 count) of each type of data is listed, and in some cases an example of the most recent such item is described. In some agencies which pieces of data are public. Links are also provided to new 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 any family members 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 [declassification](#).

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@cs.berkeley.edu
 Corrections or additions? [Contribute via GitHub](#)

DRIOGUS

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
[ilustmtd.com](#)
[http://npdoty.name/bco/](#)
[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

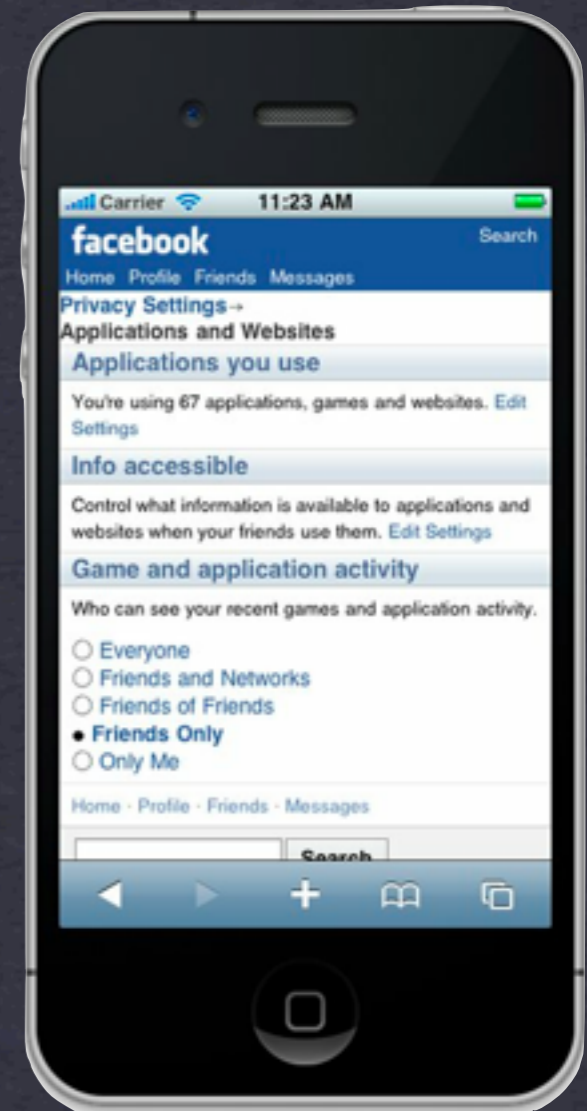
About me: 18 entries
Name: Nick Doty
Profile URL: <https://plus.google.com/109918661491263503757>
Links: 8 sites
+1's: 130

[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](https://github.com/m0hit/privacypatterns)

Our money video series

LOOSE CHANGE
sky news Yahoo!

How to manage your holiday budget
We look at how to ensure a trip with the family doesn't turn into an expensive fiasco.
Yahoo! Personal Finance

YAHOO! SITES Edit

- Mail
- News
- Sport
- Dating
- Lifestyle
- Finance (FTSE 100)
- omg!
- Cars
- Movies
- Shopping
- Games
- Video
- Messenger
- Weather (21°C)
- Answers
- Travel
- Horoscopes

More Yahoo! Sites

MY FAVOURITES Edit

- eBay
- Amazon
- Add Favourite

FEATURED PARTNERS

- Free Bingo

Developing News: Kate Middleton, the Duchess of Cambridge, has given birth to a baby boy. -- More
- Live text blog: All the reaction

Duchess of Cambridge gives birth
The Duchess of Cambridge has given birth to a boy in St Mary's hospital in Paddington, London. World reacts >>
Kate's style gallery - Duchess names ship
Kate looks peachy keen

Go to video

Royal baby boy arrives
Kate's tweet for happy Pete
Celebs tweet royal baby joy
Royal kids through the ages

1 - 4 of 28

NEWS SPORT ENTERTAINMENT FINANCE

Royal baby is born: Coverage on Yahoo!

Follow our live baby blog
So it's a boy - it seems the Duchess got her wish after all
Celebrities react (of course)

- Full coverage of the royal baby
- Well-wishers cheer around the globe

More Royal news

- Royal Baby: Live blog
- Royal Baby: Livestream from outside St Mary's Hospital
- Royal Baby: Boy Joy For Kate And William
- Baby boy for Prince William and wife Kate
- Britain fashes out contested mortgage guarantee scheme
- U.S. and UK fine high-speed trader for manipulation
- Party time in KATE's home village
- Three cheers for royal newborn
- 'Whole country will celebrate' - PM
- UK's oldest person dies aged 115

updated 00:37 More: News | Videos | Weather

NIKKEI: 14,858 **0.47%** **Dow:** 15,545.5 **0.01%** **FTSE100:** 6,823.2 **-0.17%**

Enter stock symbol **Get Quotes**

DONT MISS OUT

Yahoo! Sport
Get the latest football results, news and live coverage.

Gerry Lane (Brad Pitt) is in a race against time to stop a pandemic that threatens to end humanity.

Compare best-selling credit cards on Yahoo! Finance. 0% interest on all balance transfers and purchases

YAHOO! SITES

- Mail
- Answers
- Careers
- Cars
- Dating
- Fantasy Football
- Flickr
- Games
- Lifestyle
- Mobile
- omg!
- Toolbar
- Travel
- TV
- Yahoo! Ireland
- All Yahoo!
- Get Yahoo! on your iPad
- Make Y! your homepage
- Star Wars news
- Latest weather
- Yahoo! Wireless festival
- Career advice
- Britain's Got Talent
- The Hobbit news

FOLLOW YAHOO!
Follow Us

YAHOO! FOR YOUR BUSINESS
Advertise with us

ABOUT YAHOO!
Help | Send Feedback
Press Office | Jobs
Help and advice on Yahoo! Mail security

Copyright © 2013 Yahoo! All rights reserved.
Privacy Policy | About our ads | Terms of Service | Copyright/FP Policy | Safety

YAHOO! PRIVACY CENTRE

At Yahoo! we care about your privacy. We want you to know what we do with your information and how you can control it. This page explains our privacy policy and how you can manage your privacy settings.

How we use your information
We use your information to provide you with the services you request, to improve our services, and to help us understand how our services are used. We may also use your information for marketing purposes, unless you have opted out.

Information collection and use
We collect information from you when you use our services. This information includes your name, email address, and other contact information. We use this information to provide you with our services and to improve our services.

Information sharing and disclosure
We may share your information with our service providers, who use it to provide our services to you. We may also share your information with our parent company, Yahoo! Inc., and its subsidiaries.

Your ability to opt out and control your information
You can control how we use your information by adjusting your privacy settings. You can also opt out of our marketing emails and other promotional offers.

Security and confidentiality
We take steps to protect your information from unauthorized access, disclosure, alteration, and destruction. We use industry-standard security measures to ensure the confidentiality of your information.

Posting on publicly accessible areas
When you post information on our services, you are making it publicly accessible. We are not responsible for the content of any information you post on our services.

Changes to this privacy policy
We may update this privacy policy from time to time. We will post any changes to this policy on this page.

Questions or comments
If you have any questions or comments about our privacy policy, please contact us at privacy@yaho.com.

PRIVACY POLICIES

Add Personal Contacts as Friends

Choose how you communicate with friends. See [how it works](#) or [manage imported contacts](#).

Step 1 Find Friends | **Step 2** Add Friends | **Step 3** Invite Friends

iCloud

Apple ID:

Password:

Find Friends

[See how it works](#)

Outlook.com (Hotmail) Find Friends

Yahoo! Find Friends

Are Your Friends Already on Facebook?

Web Email Yahoo Mail, Hotmail, Gmail, etc.
Find out which of your email contacts are on Facebook.

Your Email:

Email Password:

Find Your Friends

We won't store your login or password without your permission.

AIM Instant Messenger Find your AIM buddies on Facebook

Email Application Outlook, Apple Mail, etc.

[More Ways to Find Friends »](#)

- select...
- gmail.com**
- yahoo.com
- aol.com
- hotmail.com
- msn.com
- hotmail.co.uk
- yahoo.co.uk
- yahoo.ca
- other...

THIRD-PARTY PASSWORDS FOR DELEGATED AUTH

Your personal security phrase: computer chip

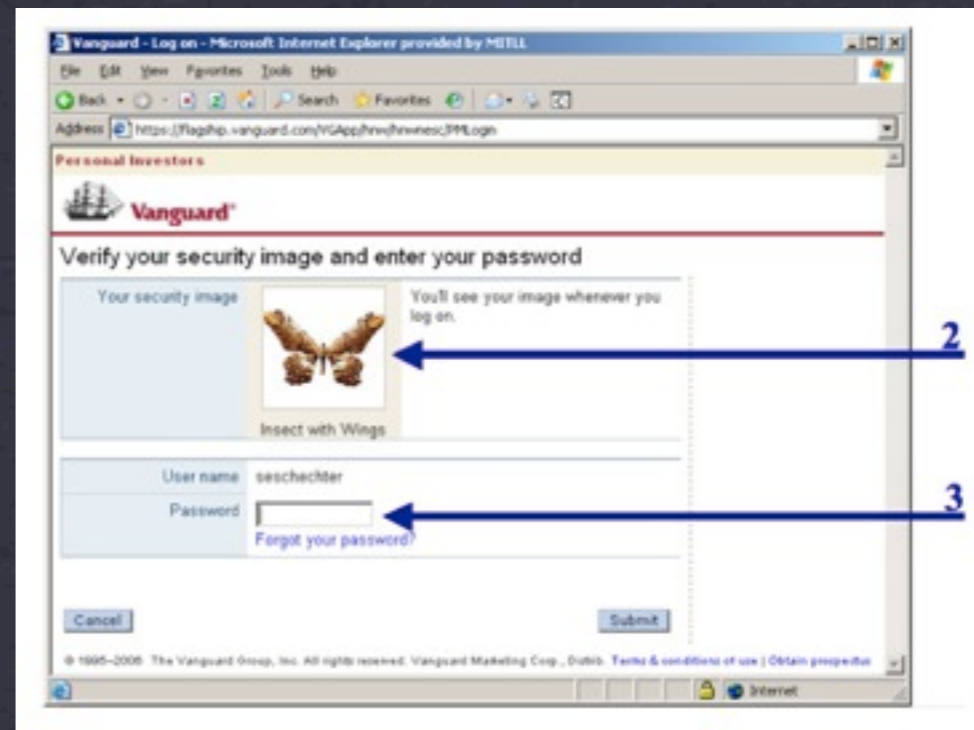
Your personal security image:



Password:

Password is case-sensitive

Log In ▶



SECURITY IMAGES FOR SITE AUTHENTICATION

Conclusions

Nick Doty

<http://npdoty.name>

npdoty@ischool.berkeley.edu