privacy patterns

Nick Doty and Mohit Gupta

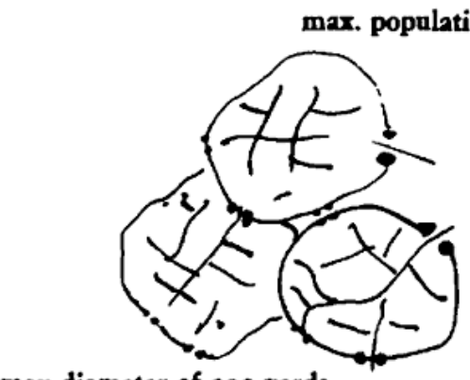
privacy by design

“in practice”

learning design and engineering

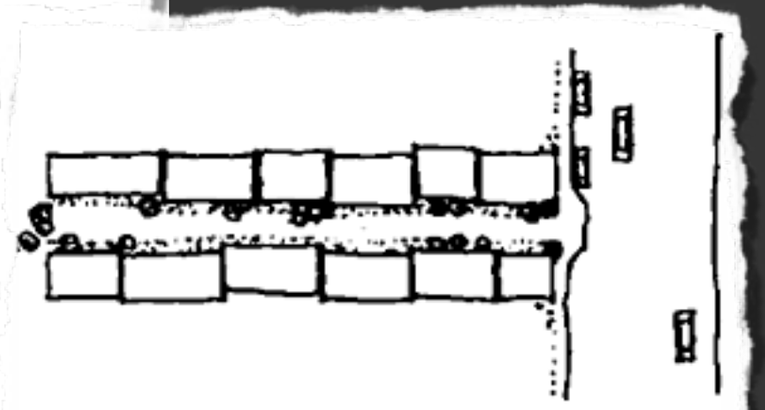
lessons before **disasters.**

why **patterns**



❖ ❖ ❖

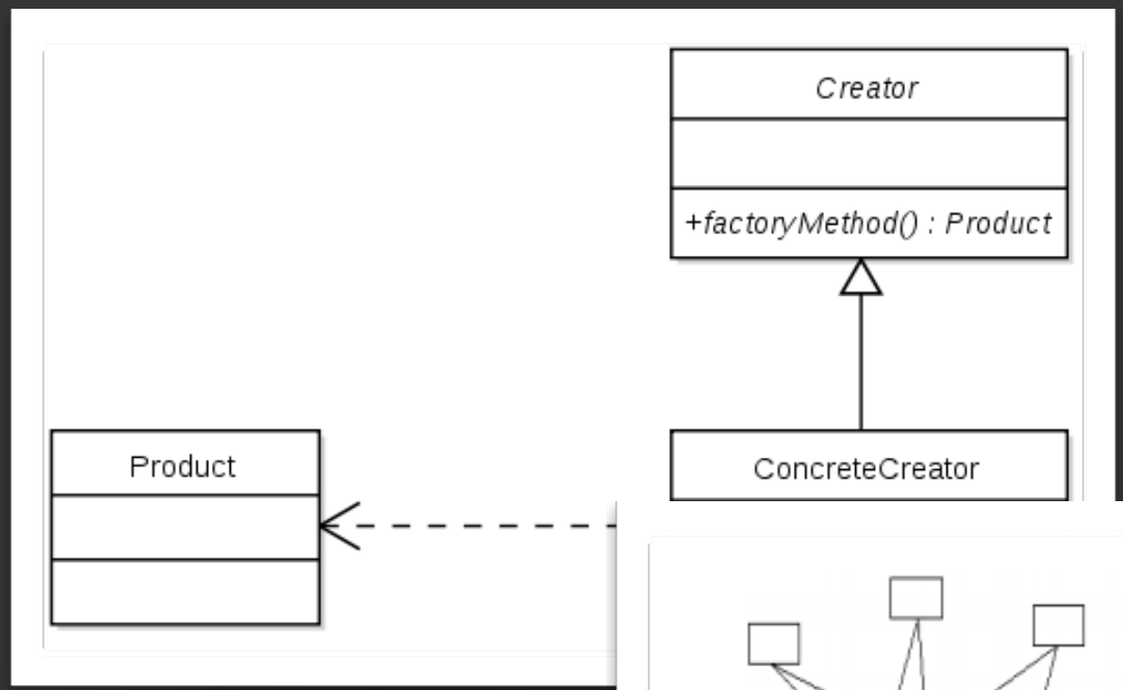
Mark the neighborhood, above all, by gateways wherever main paths enter it—MAIN GATEWAYS (53)—and by modest boundaries of non-residential land between the neighborhoods—NEIGHBORHOOD BOUNDARY (15). Keep major roads within these boundaries —PARALLEL ROADS (23); give the neighborhood a visible center, perhaps a common or a green—ACCESSIBLE GREEN (60)—or a SMALL PUBLIC SQUARE (61); and arrange houses and workshops within the neighborhood in clusters of about a dozen at a time—HOUSE CLUSTER (37), WORK COMMUNITY (41). . . .

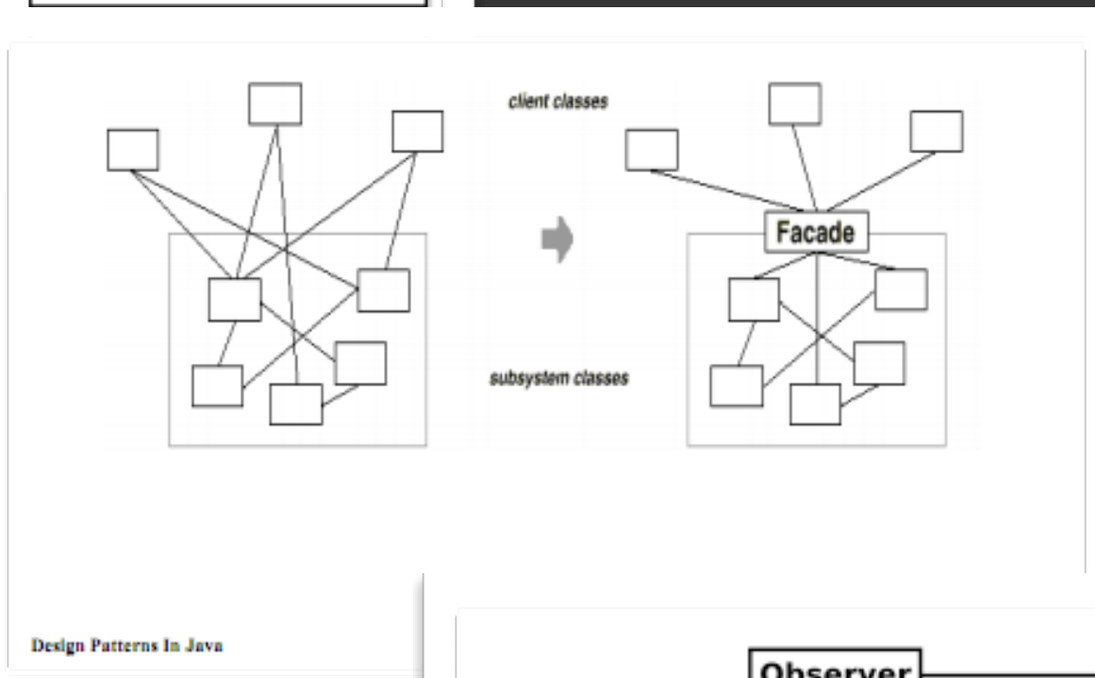


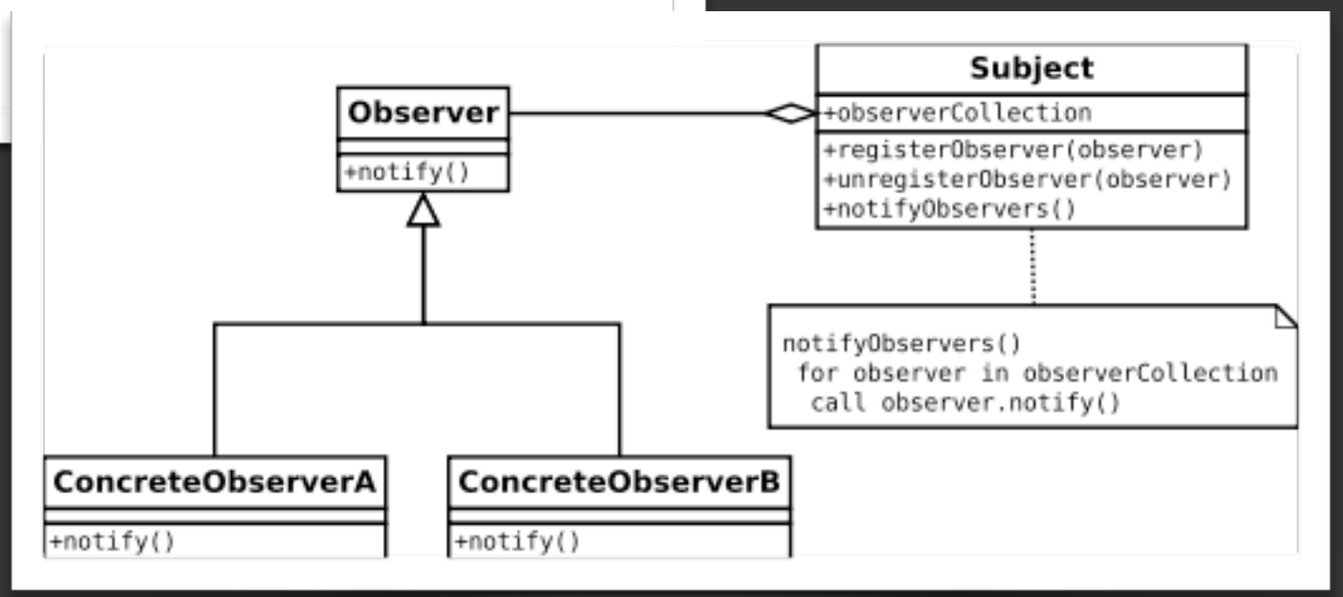
Houses long and thin along the path.

patterns

a pattern is the solution to a problem in a context.

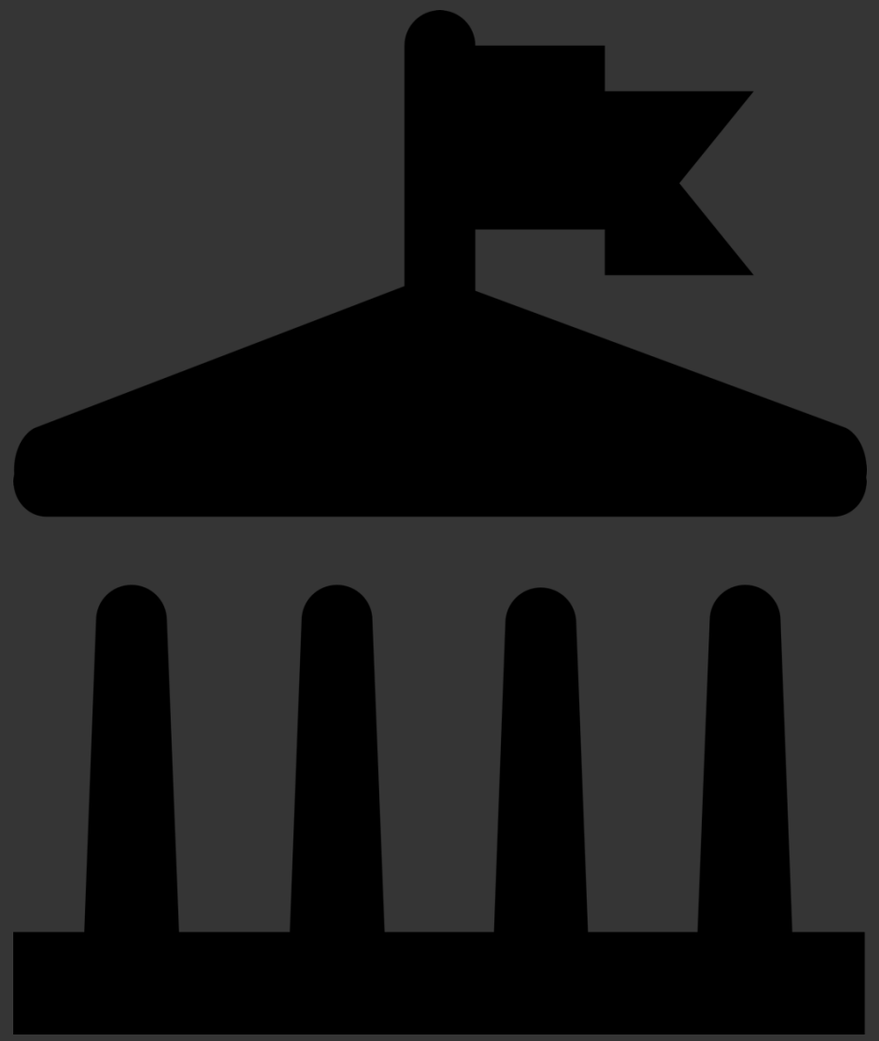

Creator
+factoryMethod() : Product
Product
ConcreteCreator


client classes
Facade
subsystem classes
Design Patterns In Java


Observer
+notify()
Subject
+observerCollection
+registerObserver(observer)
+unregisterObserver(observer)
+notifyObservers()
notifyObservers()
for observer in observerCollection
call observer.notify()
ConcreteObserverA
+notify()
ConcreteObserverB
+notify()

shared

language



institutionalize knowledge

and patterns

allow for collaboration, consistent solutions, and continuous learning

patterns **like...**

ambient notice

Sprint 3G 11:17 AM

know wher ×

/location/

This page is tracking your location.

If you're using a supported browser **(and you are)**, then I ca
precisely determine your location with your permission. I pro
won't store your location or share it with anyone.

Find my location again

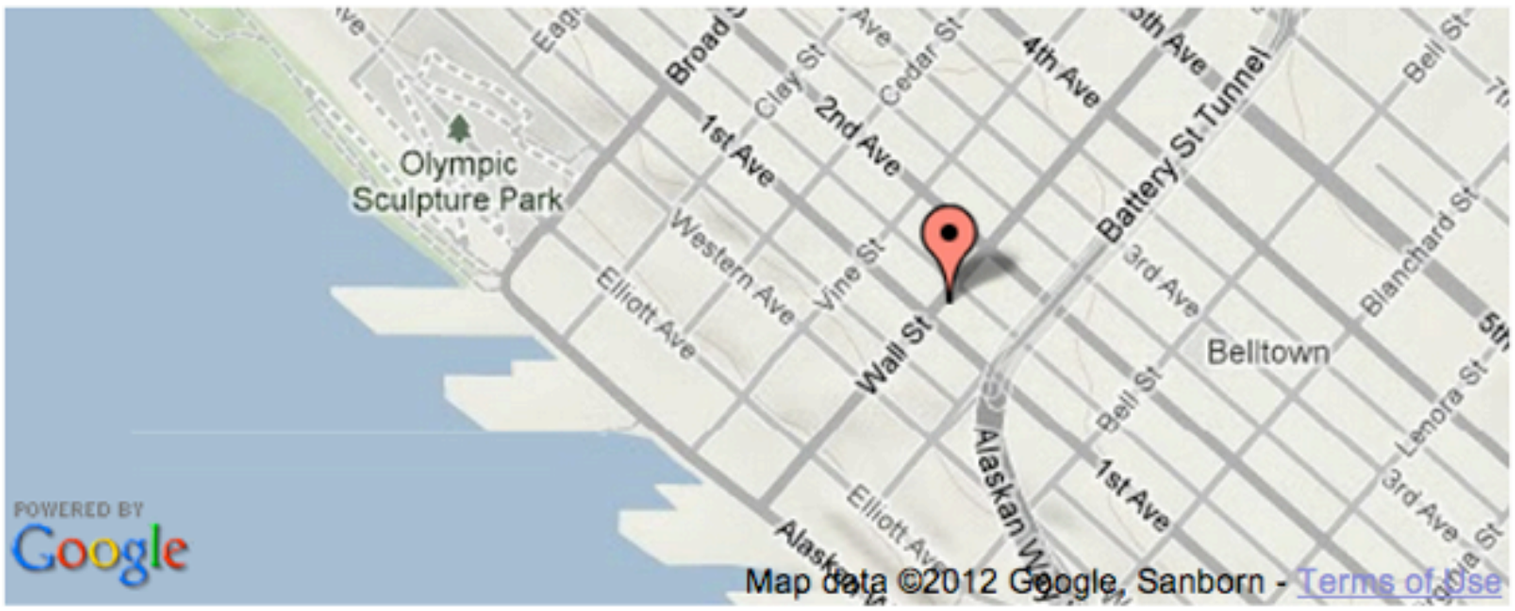
This page contains elements from the following sites that are tracking your location:

npdoty.name

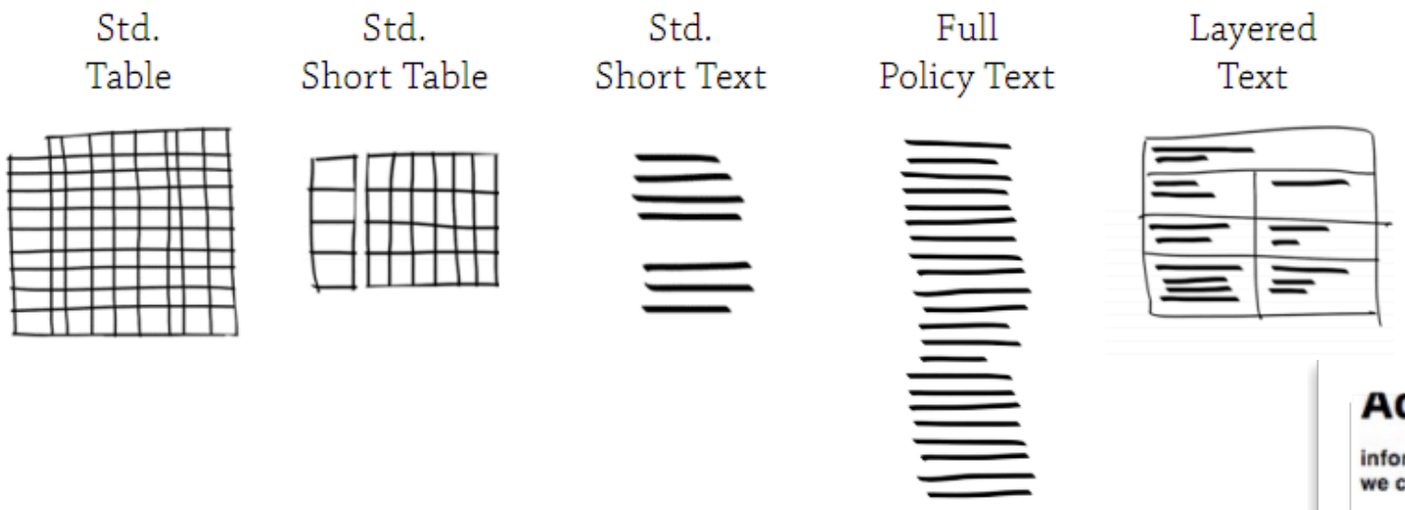
Clear these settings for future visits

Manage location settings... Done

Your browser has reported your coordinates as: **Lat: 47.6147897, Lon: -122.34845, Accuracy: 25 meters**



Five Formats Compared



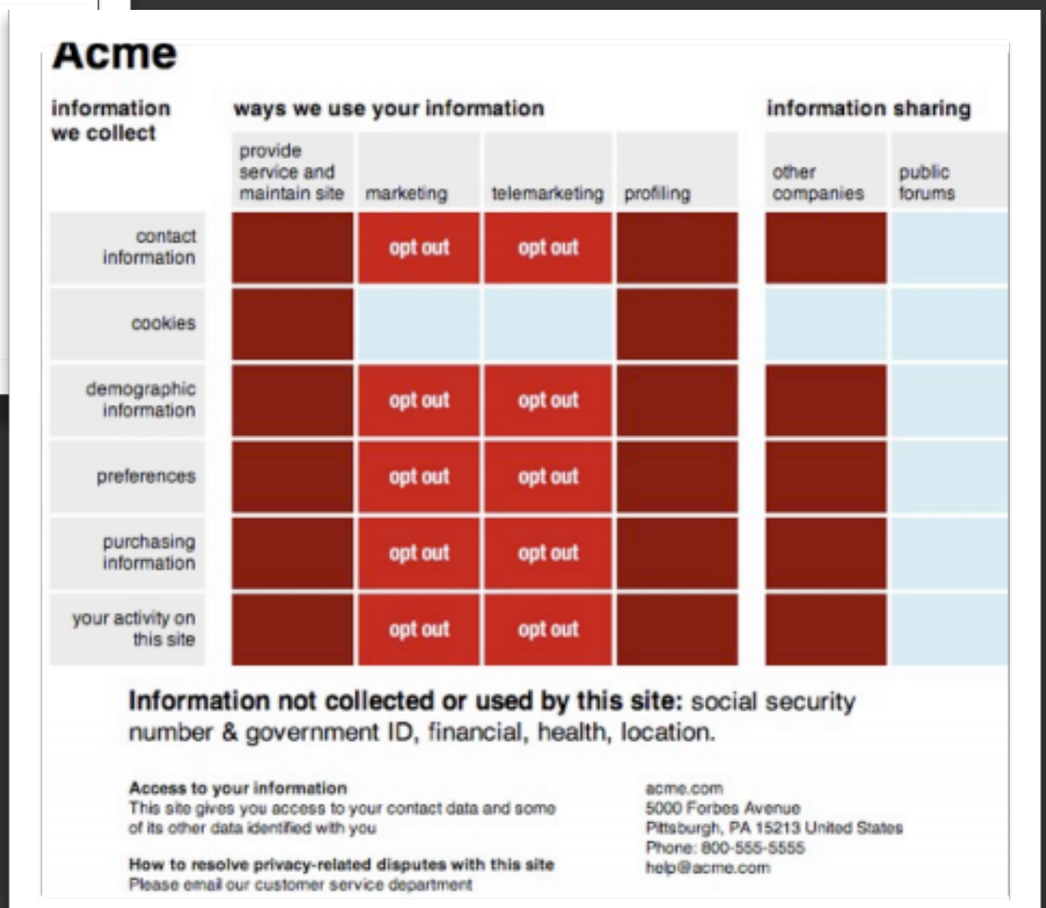
Sharing on foursquare

Last updated: April 18, 2011

We've put together this detailed table of information sharing on foursquare to show our default privacy settings and how they can be adjusted. For the definitions of each of the terms used in the matrix, **see below**.

We invite your **feedback** so we can continue to make your experience on foursquare as positive as possible.

YOUR CHECK-INS					
	Where Displayed	Viewable by foursquare friends		Viewable by the public	
		Default	How to adjust	Default	How to adjust
The location and time of each of your check-ins	Friends tab	Yes	• Check in "off the grid"	No	
	Website homepage	Yes	• Check in "off the grid"	No	
	Who's Here	Yes	• Check in "off the grid"	Yes	• **User Settings** *(can opt out of Who's Here)* • Check in "off the grid"
	Check-in History on Profile page	Yes *(friends can see the five most recent check-ins)*	• Check in "off the grid" • Check in History page *(can delete individual check-ins)*	No	
The location of your shouts	Friends tab	Yes *(the location will be shown to friends as "Nearby" or "Friends in other cities")*	• Users can be selective about sending Shouts	No	



Romanosky, et al.

CATEGORIES: TRANSPARENCY · ACCESS · LOCATION

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 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

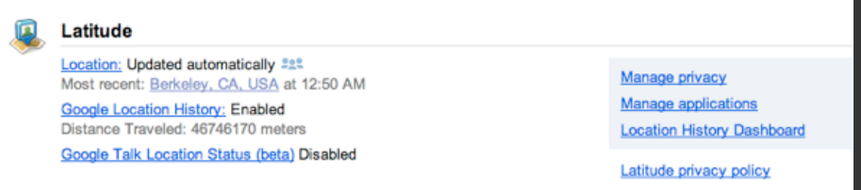
An informational privacy dashboard can provide collected summaries of the collected or processed personal data for a particular user. While access to raw data may be useful for some purposes, a dashboard provides a summary or highlight of important personal data. Seek to make the data meaningful to the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



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**

categories
transparency
location
access

concerns
reveals more data
shared accounts
see *deindentification*

categories
title

intent
context
problem
solution
examples
concerns

structure of a pattern

user control
notice
consent
secondary use
distribution

some principles for privacy

retention
transparency
feedback
aggregation

CATEGORIES: LOCATION · NOTICE · MOBILE

Asynchronous notice

Intent

Support notice of ongoing location tracking.

Supports Notice, User Control, Transparency and feedback

Context

Tracking a person's location over time in an invisible fashion, with or without prior explicit consent. (Particularly useful for background tracking, tracking through devices with limited or no screen space, or tracking repeatedly over long periods of time. For devices with sufficient screen space or other notification affordances, see also ambient notice.)

Problem

How can a service effectively provide notice to a user who gave permission once but whose information is accessed repeatedly (perhaps even continuously) over a long period of time? If a user forgets that they gave access (or who has access) they may later be surprised or upset by the continued flow of personal information. Also, initial consent may have been forged by an attacker or have been provided by another user of a shared device -- if synchronous notice is only provided at the time of consent, a user may inadvertently distribute personal information over a long period of time after having lost control of their device only momentarily.

Solution

Proactively notify the user after the time of consent that information is being tracked, stored or re-distributed. This asynchronous notice could be achieved through an email, text message, on-screen notice or even through non- digital means (by telephone or postal mail, say). The message should inform the user about the ongoing practice, including background context (since the user may well have forgotten) about the service and any opportunities for access and control.

Asynchronous notices may also include a summary of the data recently collected (since the last notice, say) in order to provide clarity (and reminders) to the user about the extent of collection. See also, [Privacy dashboard] (Privacy-dashboard) and Access.

By ensuring that users aren't surprised, asynchronous notice may increase trust in the service and comfort with continued disclosure of information.

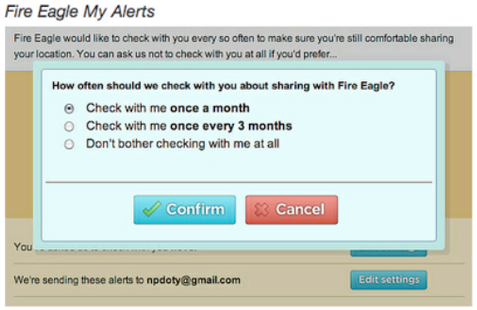
Examples

Google Latitude reminder email

Google Latitude users can configure a reminder email (see below) when their location is being shared with any application, including internal applications like the Location History service.

```
This is a reminder that you are sharing your Latitude location with the following
application(s):

 Google Location History
 You may disable these applications at any time by going to
<https://www.google.com/latitude/apps?hl=en]>

 **Do more with Latitude**
 Go to <https://www.google.com/latitude/apps> on your computer and try the following:

 Google Location History lets you store your history and see a dashboard of
interesting information such as frequently visited places and recent trips.
 Google Talk Location Status lets you post your location in your chat status.
 Google Public Location Badge lets you publish your location on your blog or site.

 You are receiving this reminder once a week. To change your reminder settings, go to:
 <https://www.google.com/latitude/apps?hl=en&tab=privacyreminders>
```

Fire Eagle My Alerts



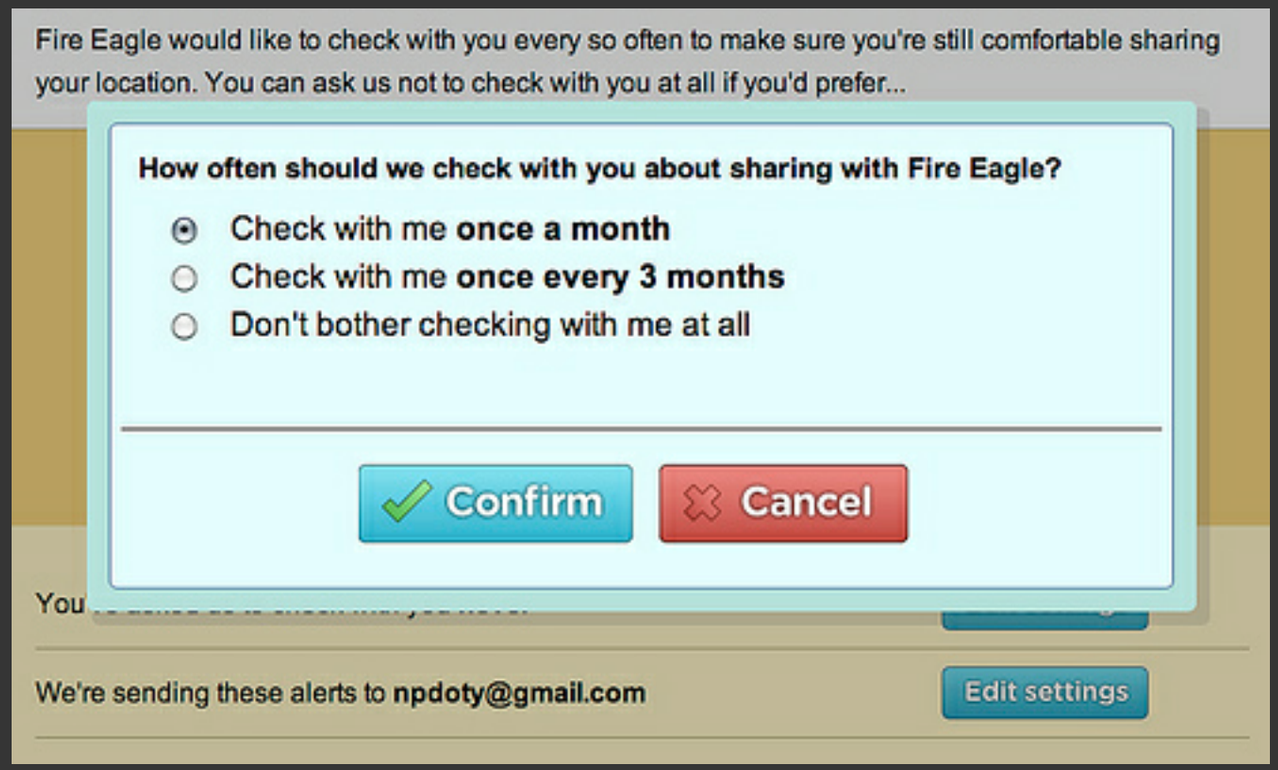
Fire Eagle My Alerts configuration by npdoty, on Flickr

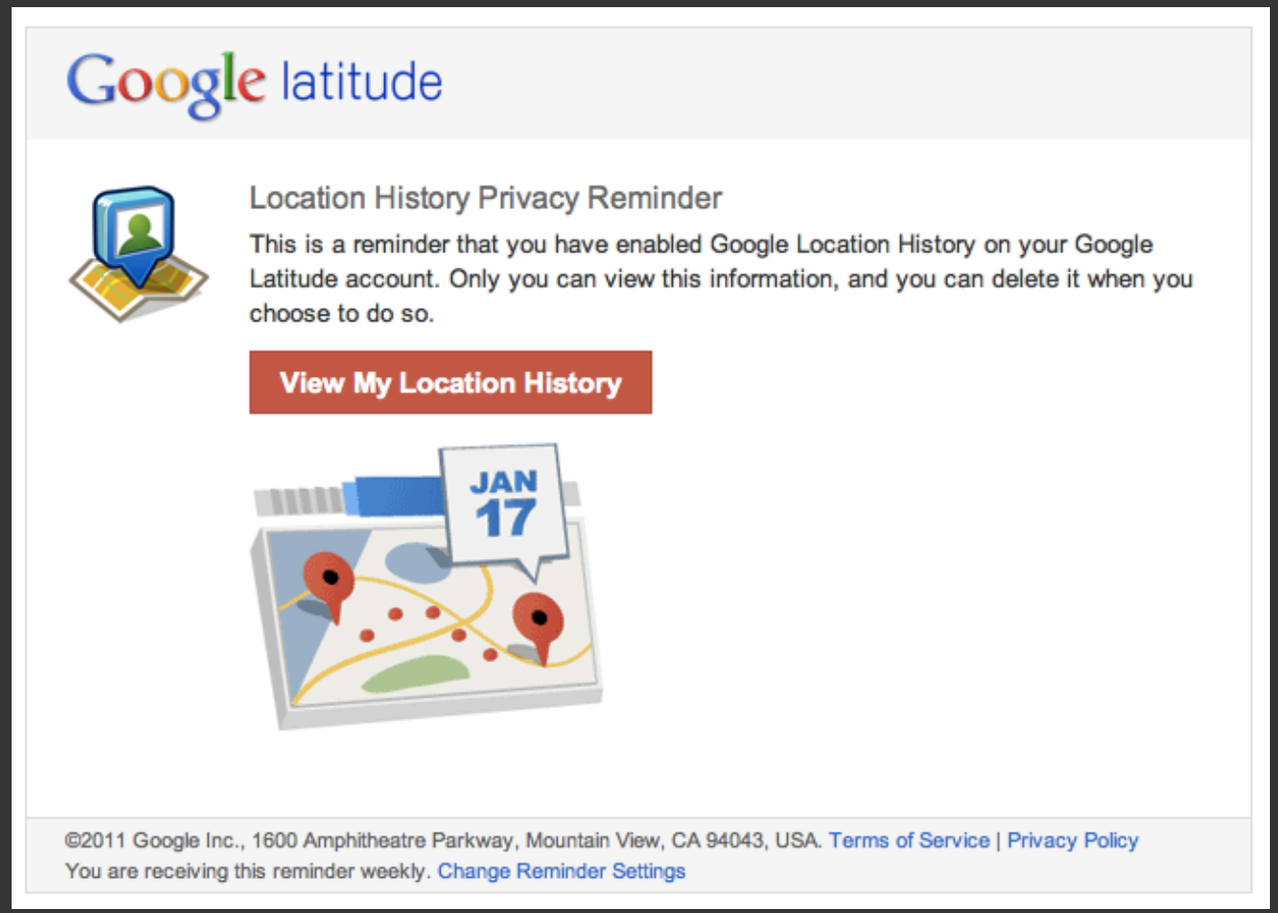
Forces/Concerns

Providing an asynchronous notice requires a reliable mechanism to contact the user (a verified email address or telephone number, for example). Care should be taken to ensure that the mechanism can actually reach the person using the device being tracked. (For example, notifying the owner of the billing credit card may not help the spouse whose location is being surreptitiously tracked.)

In contrast to the common privacy practice of providing consistent and reliable systems, you may wish to provide **random** asynchronous notice. If there is a concern that a malicious user may have opted-in the user without their knowledge, a notice that is sent once a week at the same time each week may allow the attacker to borrow the device at the appointed time and clear the notice.

Many repeated notices may annoy users and eventually inure them to the practice altogether. Take measures to avoid unnecessary notices and some level of configuration for frequency of notices. This must be balanced against the concerns of an attacker's opting the user in without their knowledge.





What is Exif data?

Exif data is a record of the settings a camera used to take a photo or video. This information is embedded into the files the camera saves, and we read and display it here.

Hiding this information

You're currently preventing other people from seeing the Exif data for your photos. You can change this in your Exif privacy settings.

Dates

Taken on	December 26, 2008 at 12.18pm PST (edit)
Posted to Flickr	January 9, 2009 at 10.13PM PDT (edit)

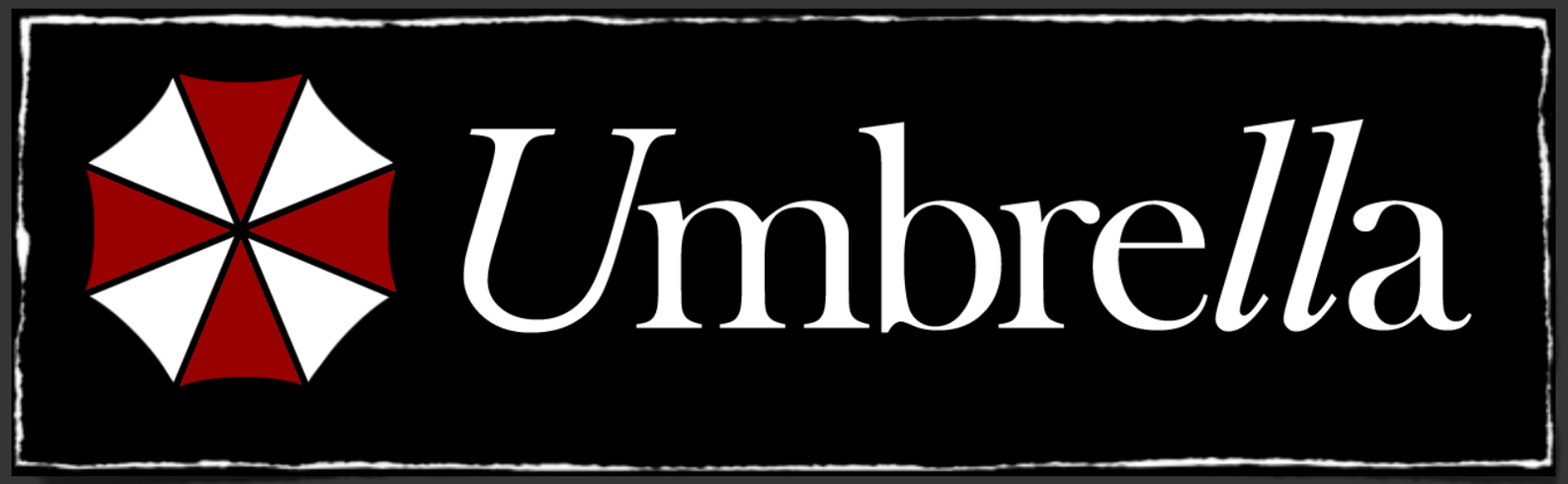
Exif data

Camera	Canon EOS 30D
Exposure	0.003 sec (1/400)
Aperture	f/4
Focal Length	41 mm
ISO Speed	1600
Exposure Bias	-1/3 EV
Flash	Flash did not fire
X-Resolution	240 dpi
Y-Resolution	240 dpi
Date and Time	2008:12:07 1[illegible]9:17
Artist Name	[illegible]known
Exposure Program	[illegible] priority
Date and Time (Original)	2008:12:26 12:18:13
Date and Time (Digitized)	2008:12:26 12:18:13
Shutter Speed	8643856/1000000
Maximum Lens Aperture	4/1
Metering Mode	Pattern

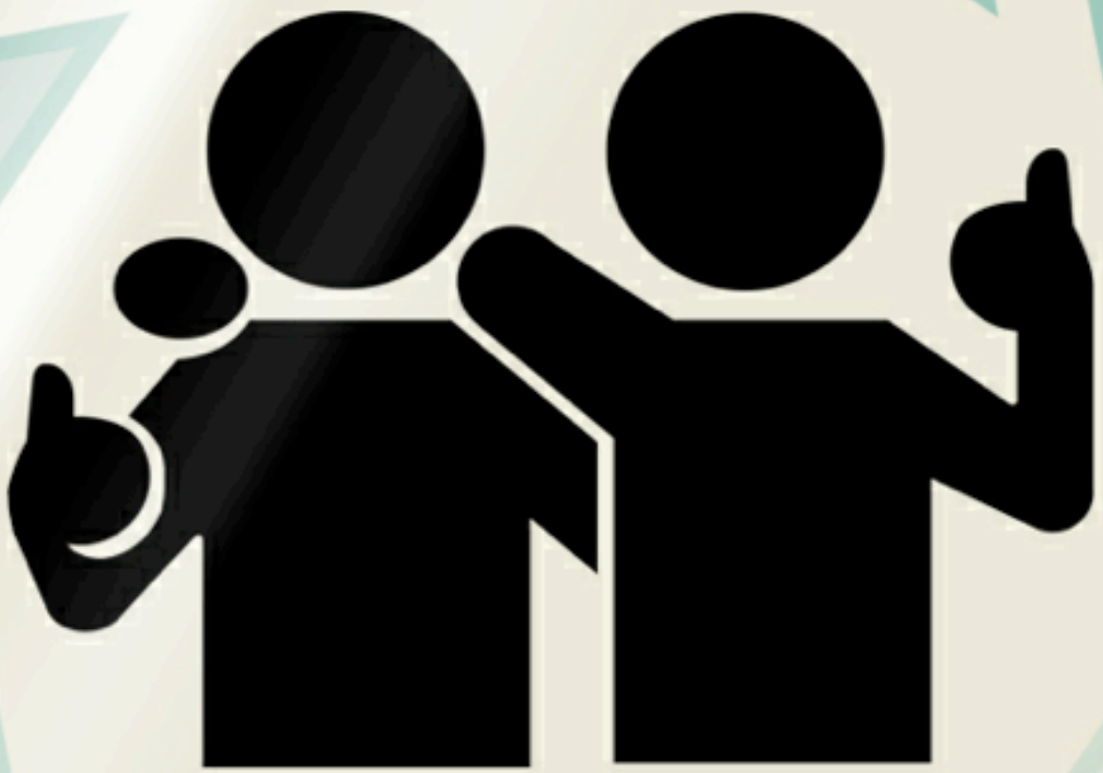
strip invisible metadata

how do privacy patterns help *'me'*

app developers
learn from others



share across teams



A Trusted Friend i ce

in data

APERTURE LABORATORIES

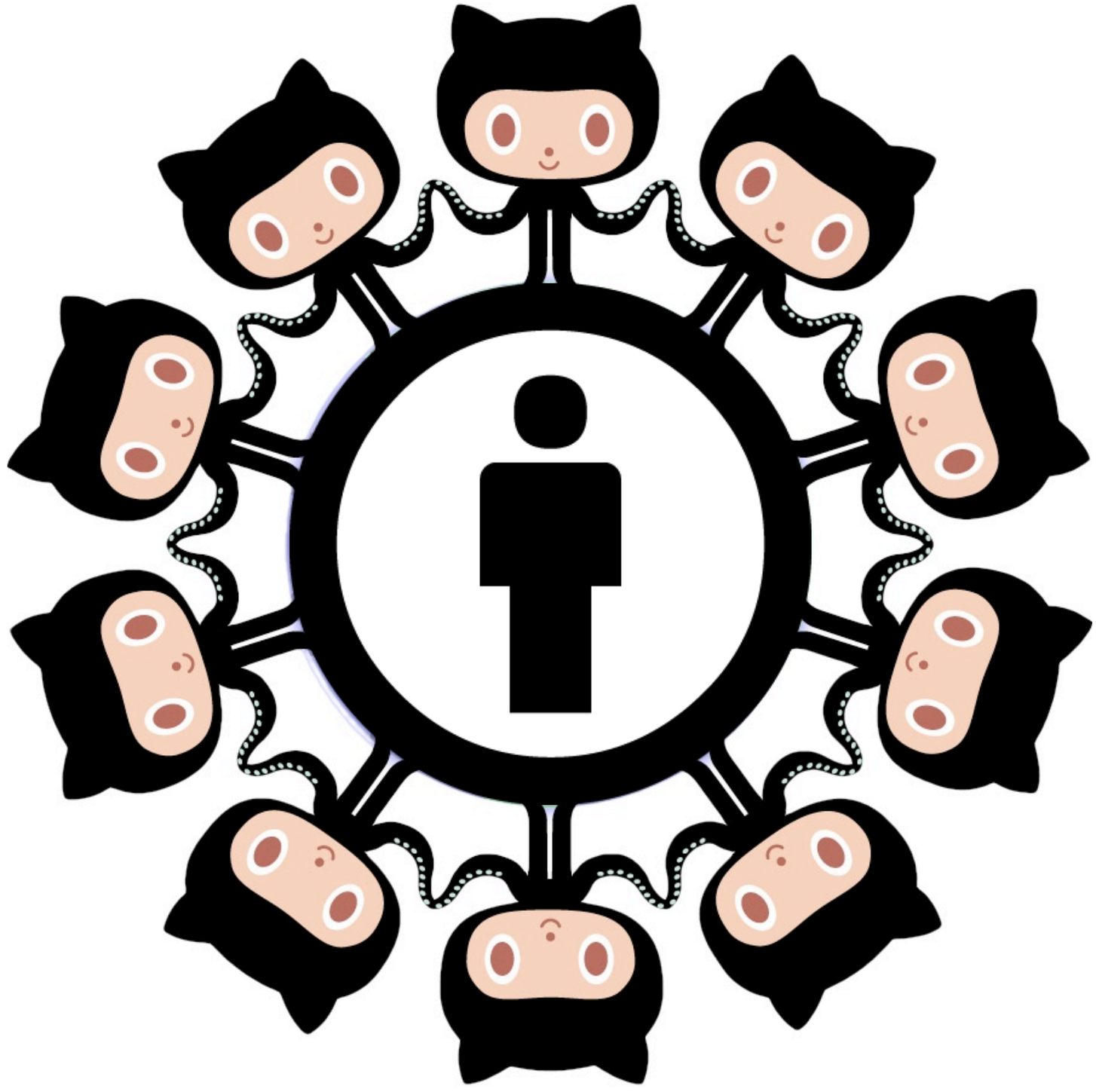
how do privacy patterns help *'me'*

building **trust**

and community

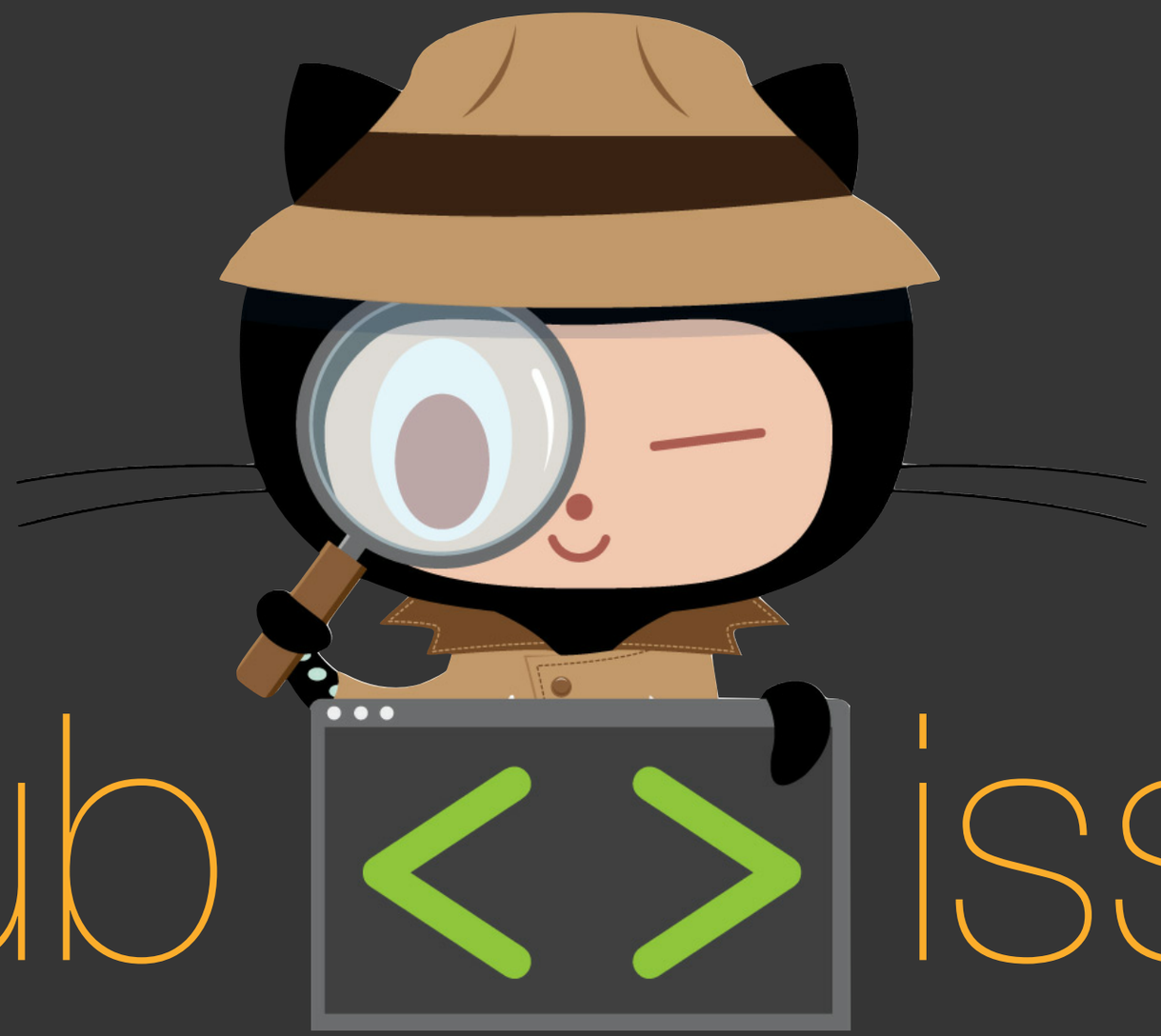

contribute to
privacypatterns.org
E PIKE ST
BROADWAY
Belltown
First Hill
SEATTLE
International
District
Yesler Terrace
YESLER WAY
S JACKSON ST
S DEARBORN ST
JAMES ST
CHERRY ST
PINE ST
PIKE ST
UNION ST
OLIVE WAY
STEWART ST
7TH AVE
6TH AVE
5TH AVE
4TH AVE
3RD AVE
2ND AVE
1ST AVE
ELLIOTT AVE
WESTERN AVE
ALASKAN WAY
ALASKAN WAY VIADUCT
1ST AVE S
4TH AVE S
RAINIER AVE S
EXPRESS LANES
WA 99
15
190

patterns,
drafts,
website,
and discussions



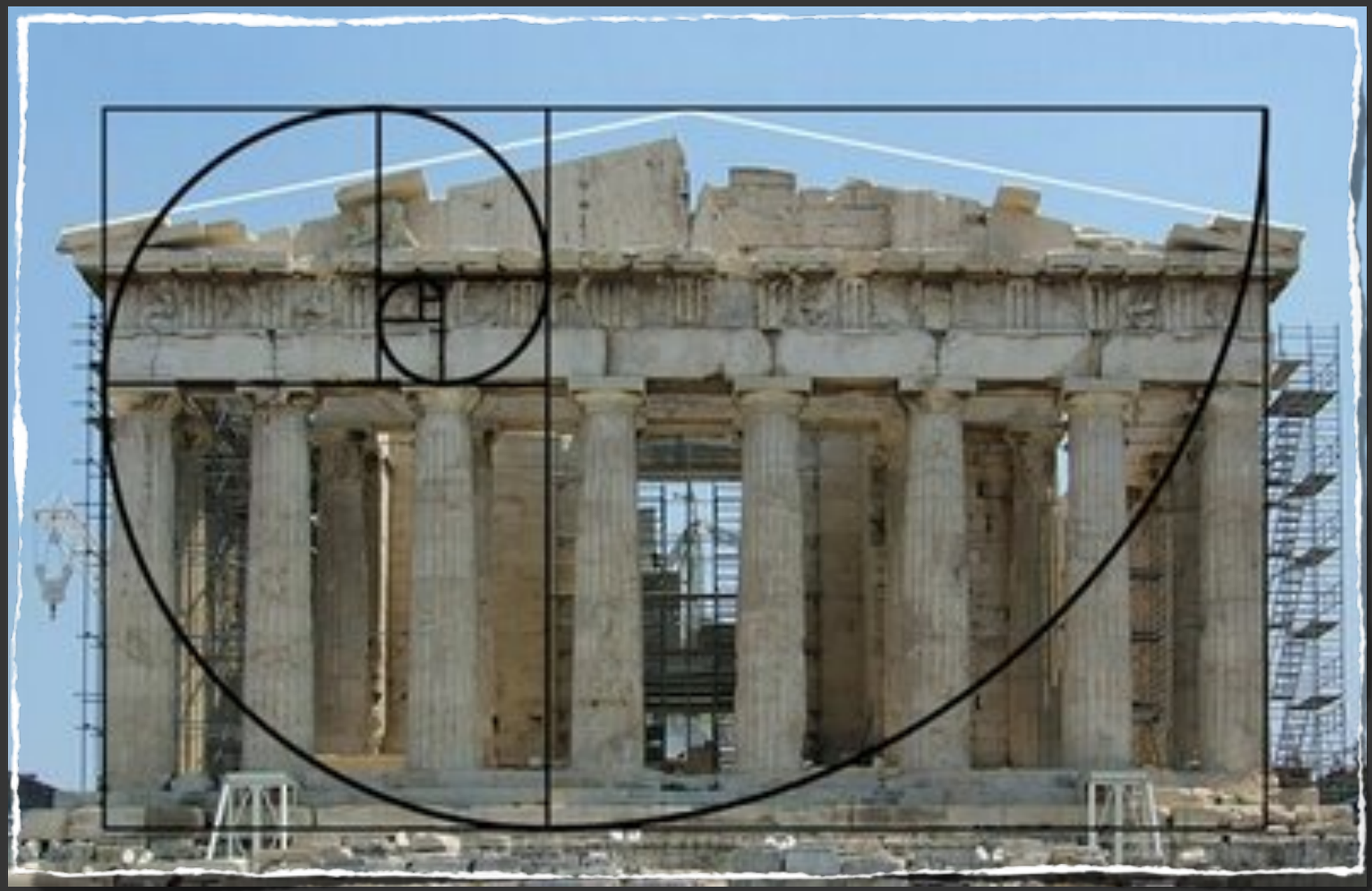

write and edit
patterns

create



github issues

use a pattern



pii.privacypatterns.org

thank you