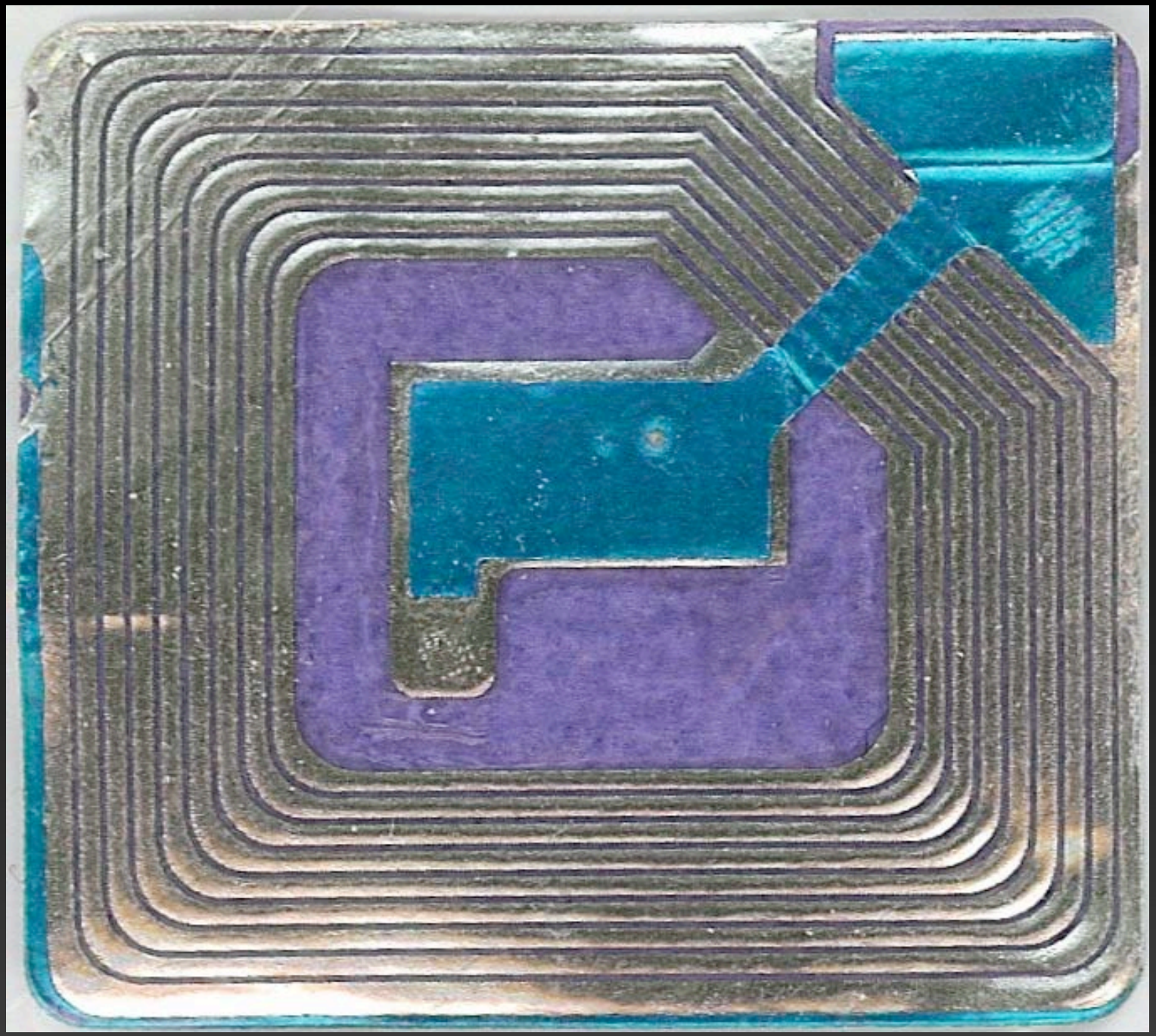
RFID

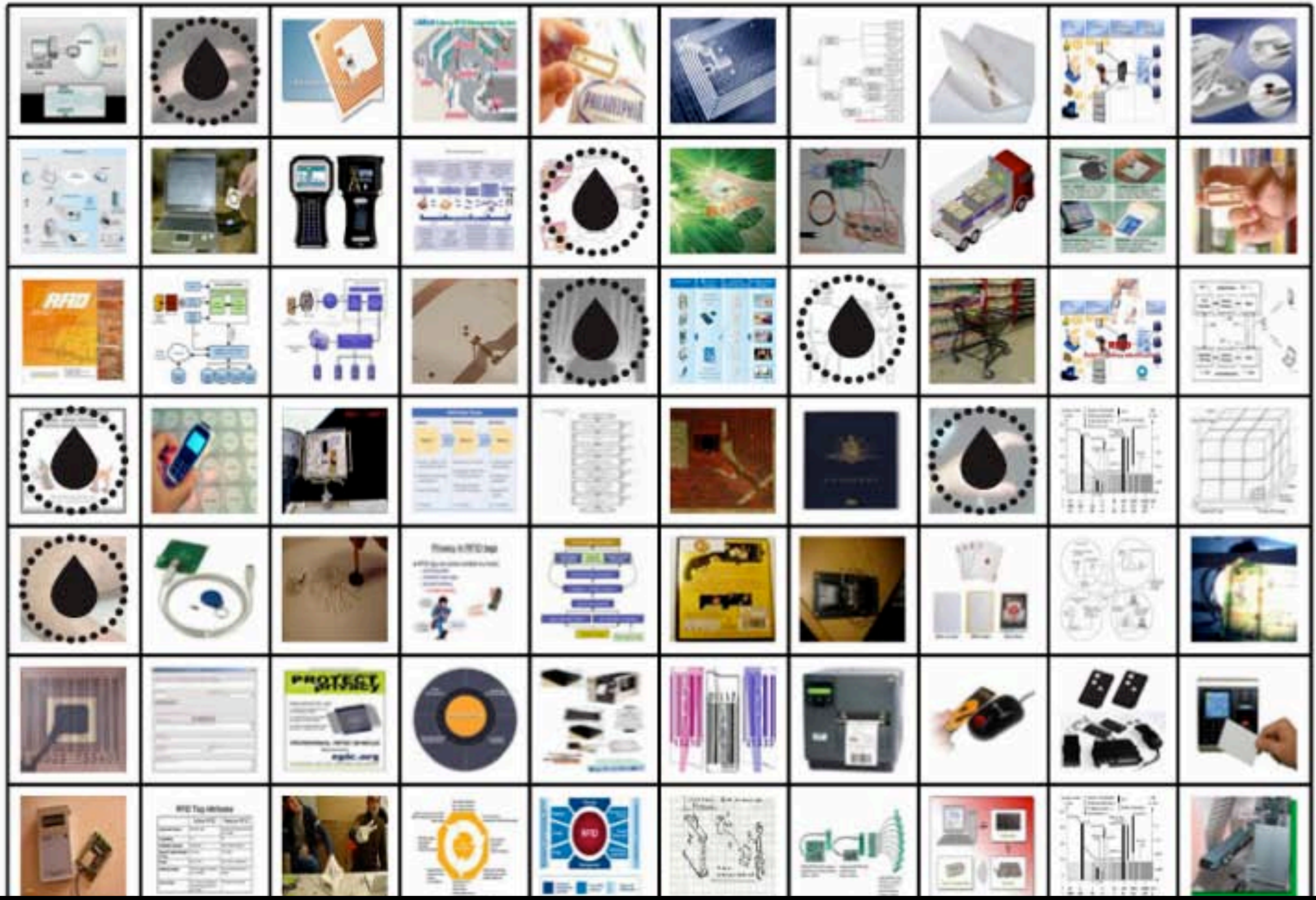
Patrick Gage Kelley

portions adapted from slides from Sarah Spiekermann



RFID | midnightcomm

RFID's 'dry' associations



Remove Before Washing or Wearing

Daveblog

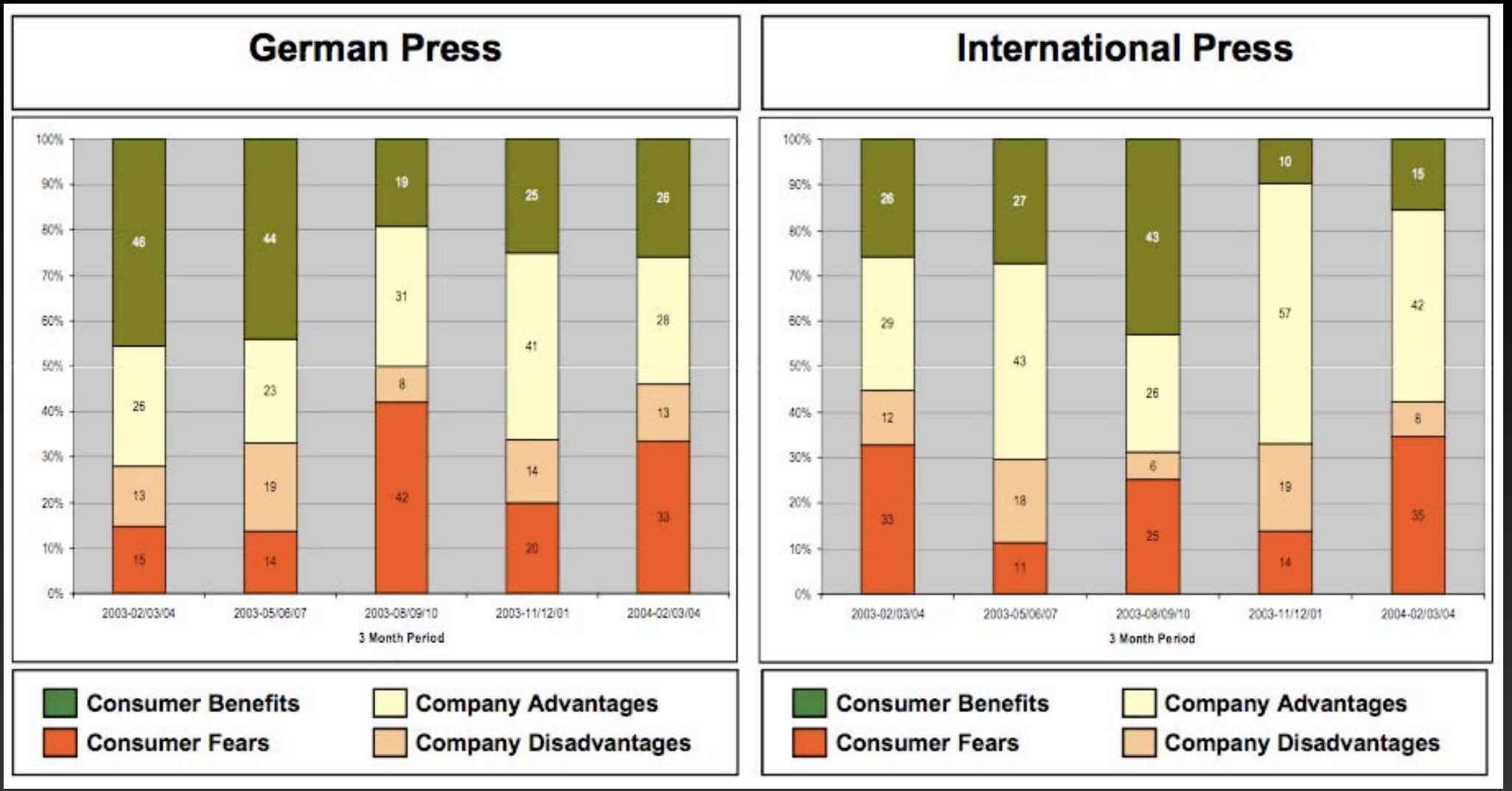
RFID also has the potential to revolutionize marketing at the POIS.

- Product Portfolio
  - More precise sales analysis through enhanced numbering system use
  - Person –product attribution
  - … through combination with video systems
  - … through enhanced numbering system in combination with loyalty cards
  - Optimization of product qualities through serial number tracking
- Price
  - Facilitationof price differentiation through intelligent shelves
- Promotion
  - More precise measurement of advertisment effectiveness: ad pricing based on consumer attention instead of eye-balls.
  - Personalized recommendations based on “attention” information
- Product placement and shop-floor design
  - Optimization of shop-floor design through enhanced movement tracking

Public Outcry in Rheinberg

Sarah Spiekermann

Boycott Benetton | http://boycottbenetton.com



The press picks up privacy

Sarah Spiekermann

	2002	2003	2004	2005	2006	2007 (until June)	Total
Number of papers published on security and privacy in RFID systems on Gildas Avoine's Site	1	11	23	59	66	17	177
Number of papers containing technical proposals to control information flow between tag and reader	1	8 (72%)	17 (74%)	32 (54%)	52 (79%)	13 (76%)	123 (69%)
…of these, those which describe their motivation as protecting *end-user* privacy	0	4 (50%)	14 (82%)	25 (78%)	22 (42%)	6 (46%)	71 (57%)
dealing with…							
RFID Kill Function							
User Scheme		1	2	2	0	0	5
Agent Scheme		1	1	3	3	0	8
On-tag Scheme		2	11	20	19	6	58

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

“If you consider that RFID tags represent the future of computing technology, this proposal [the kill function] becomes as absurd as permanently deactivating desktop PCs to reduce the incidence of computer viruses and phishing”

(p. 92 in (Rieback, Gaydadjiev et al. 2006)).

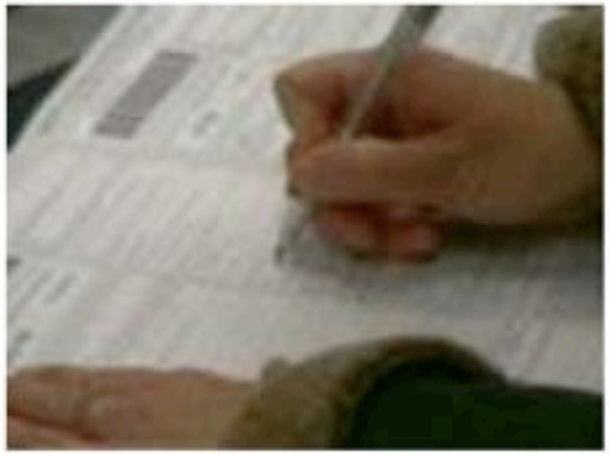
User/Password Model: Direct User Control

- RFID chips are sealed (deactivated) at the store exit with a privacy password.
- This deactivation is done seamlessly and simultaneously for all products (no transaction cost)
- The password scheme is supposed to be secure.

- If services are sought on the basis of RFID chips after purchase, the privacy password serves as authorization.
- The consumer initiates service use.

–Spiekermann, S., Berthold O., "Maintaining privacy in RFID enabled environments - Proposal for a disable-model", in: Privacy, Security and Trust within the Context of Pervasive Computing, Hrsg. P. Robinson, H. Vogt, W. Wagealla, The Kluwer International Series in Engineering and Computer Science, Springer Verlag, 2005

Network (Agent) Model: Control is delegated



- RFID chips are generally left on to respond to network requests.
- Access to chips is managed via privacy preferences stored on the network.
- A user specifies these privacy preferences in written form with a mobile operator.

- Privacy preference management is then done automatically via the mobile phone.
- The mobile phone serves as a privacy buffer.
- It is asked by readers whether tags can be read out or not.
- It has the power to deny access.

73% of participants want to see RFID chips destroyed rather than taking advantage of the benefits. The trend is reenforced the more education people have.

F48: Die vorangegangenen Fragen und der Film zeigen, dass RFID Technologie Nachteile und Vorteile für den Verbraucher mit sich bringt. Natürlich wäre statt des Passwortschutzes denkbar, alle Chips am Ladenausgang vollständig zu vernichten. Was ist Ihre Gesamteinschätzung zu dieser Frage? Bitte markieren Sie Ihre Tendenz auf einer Skala:

□ □ □ □ □ □ □ □ □ □ □

Chips vollständig vernichten — **Chips mit Passwort versehen**

	Tendency to reject PET (1-5)	Undecided (6)	Tendency to use PET for advantage (7-11)
User Model with IB	69.9% *82.9%**	8.2% *4.9%**	21.9% *12.2%**
Network Model without IB	78.2% *71.4%*	9.1% *11.4%*	12.7% *17.1%*
Gesamt with IB	73.4% *77.6%*	8.6% *7.9%*	18.0% *14.5%*

Deactivation vs. PET. The numbers in italics represent the top 60% of the panel with respect to education.
The asterisk* denotes a significant difference of technology perception due to education.

- Günther, O., Spiekermann, S. , "RFID And The Perception of Control: The Consumer's View", Communications of the ACM (CACM), Vol. 48, No. 9, September 2005

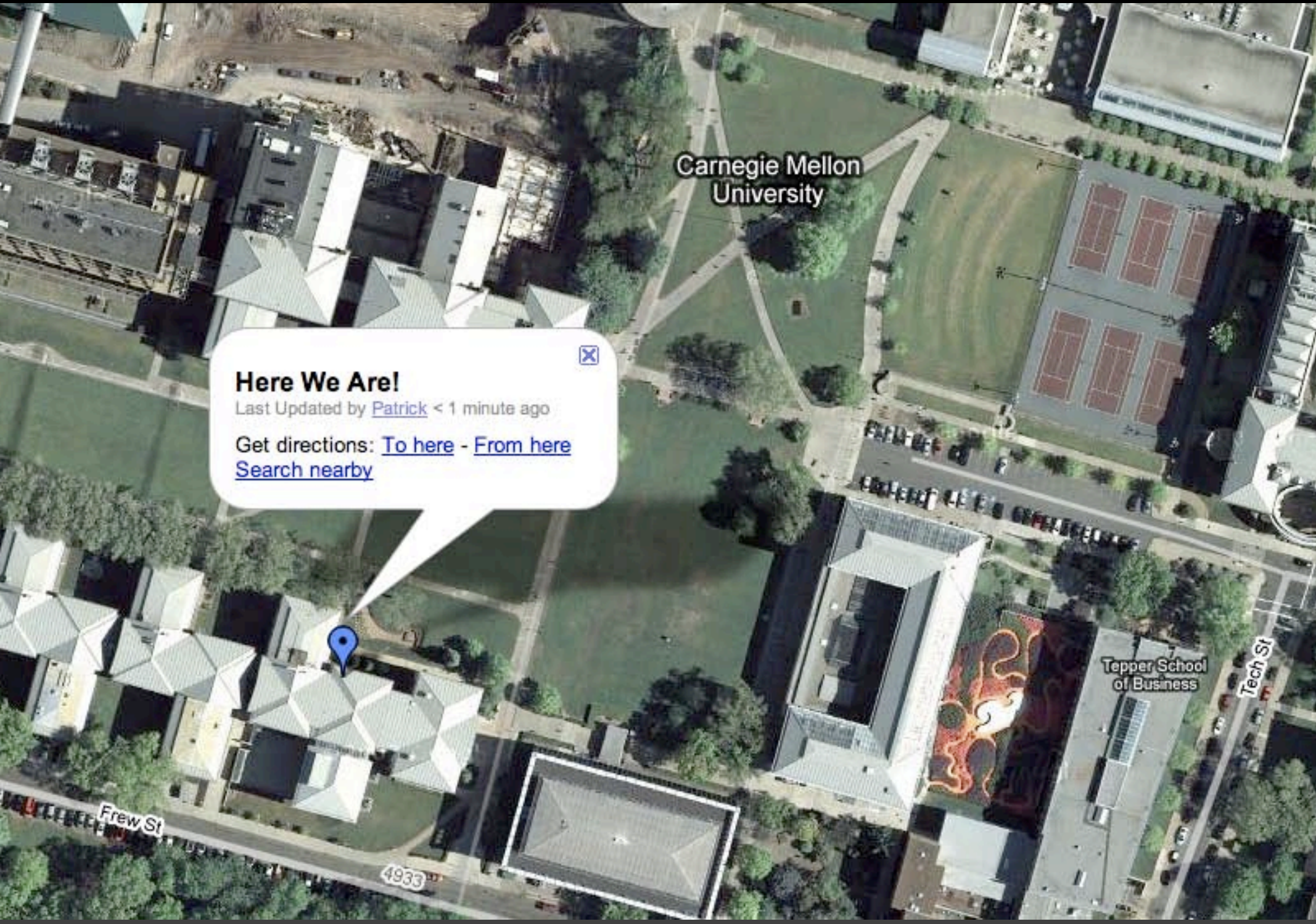
RFID

Ubiquitous Computing

Ubiquitous computing (ubicomp) is a post-desktop model of human-computer interaction in which information processing has been thoroughly integrated into everyday objects and activities. As opposed to the desktop paradigm, in which a single user consciously engages a single device for a specialized purpose, someone "using" ubiquitous computing engages many computational devices and systems simultaneously, in the course of ordinary activities, and may not necessarily even be aware that they are doing so.

This paradigm is also described as pervasive computing, ambient intelligence, or more recently, everyware. When primarily concerning the objects involved, it is also physical computing, the Internet of Things, haptic computing, and things that think.

Wikipedia!


Carnegie Mellon University
Here We Are!
Last Updated by Patrick < 1 minute ago
Get directions: To here - From here
Search nearby
Tepper School of Business
Tech St
Frew St
4933

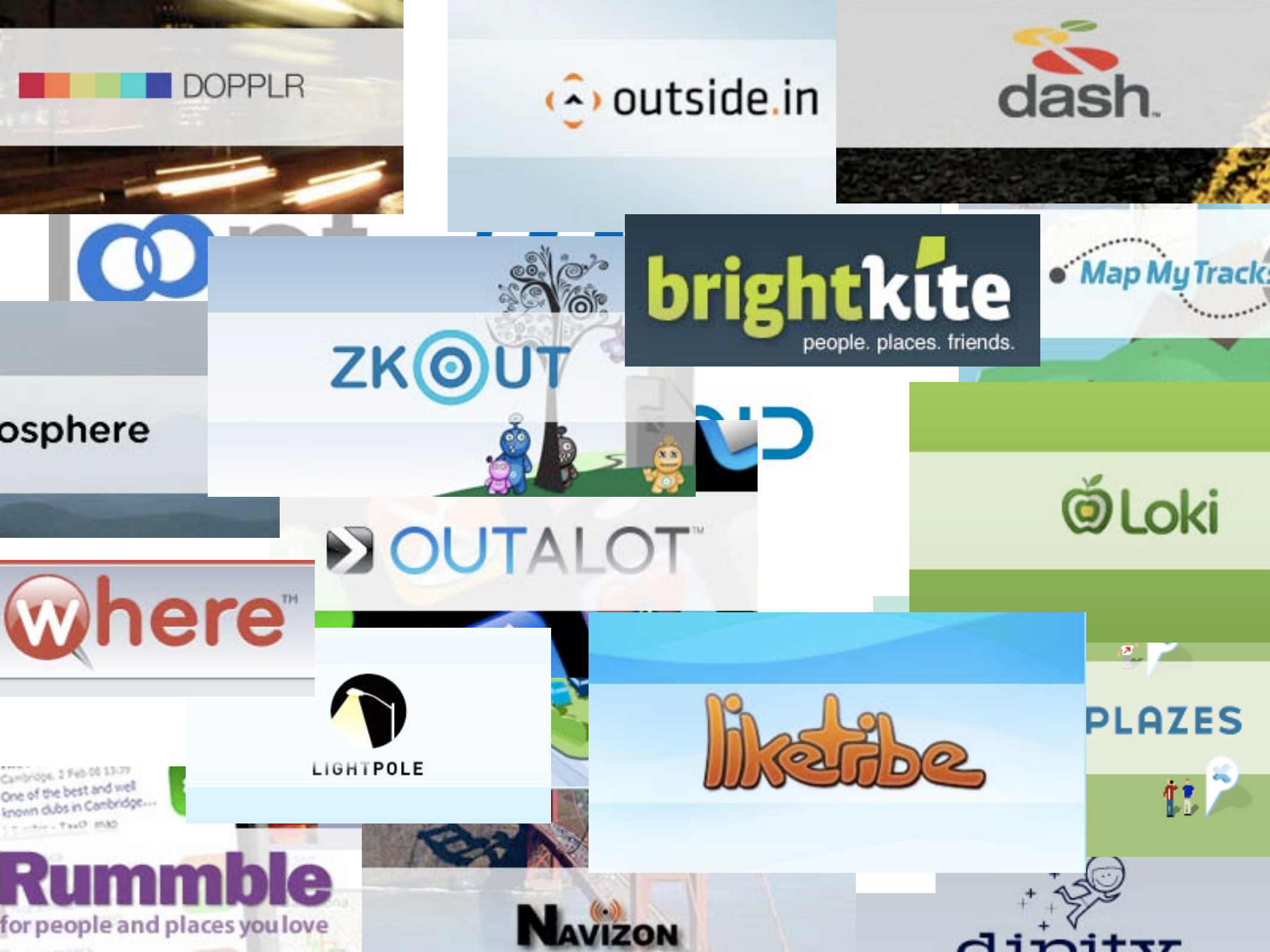
blank.

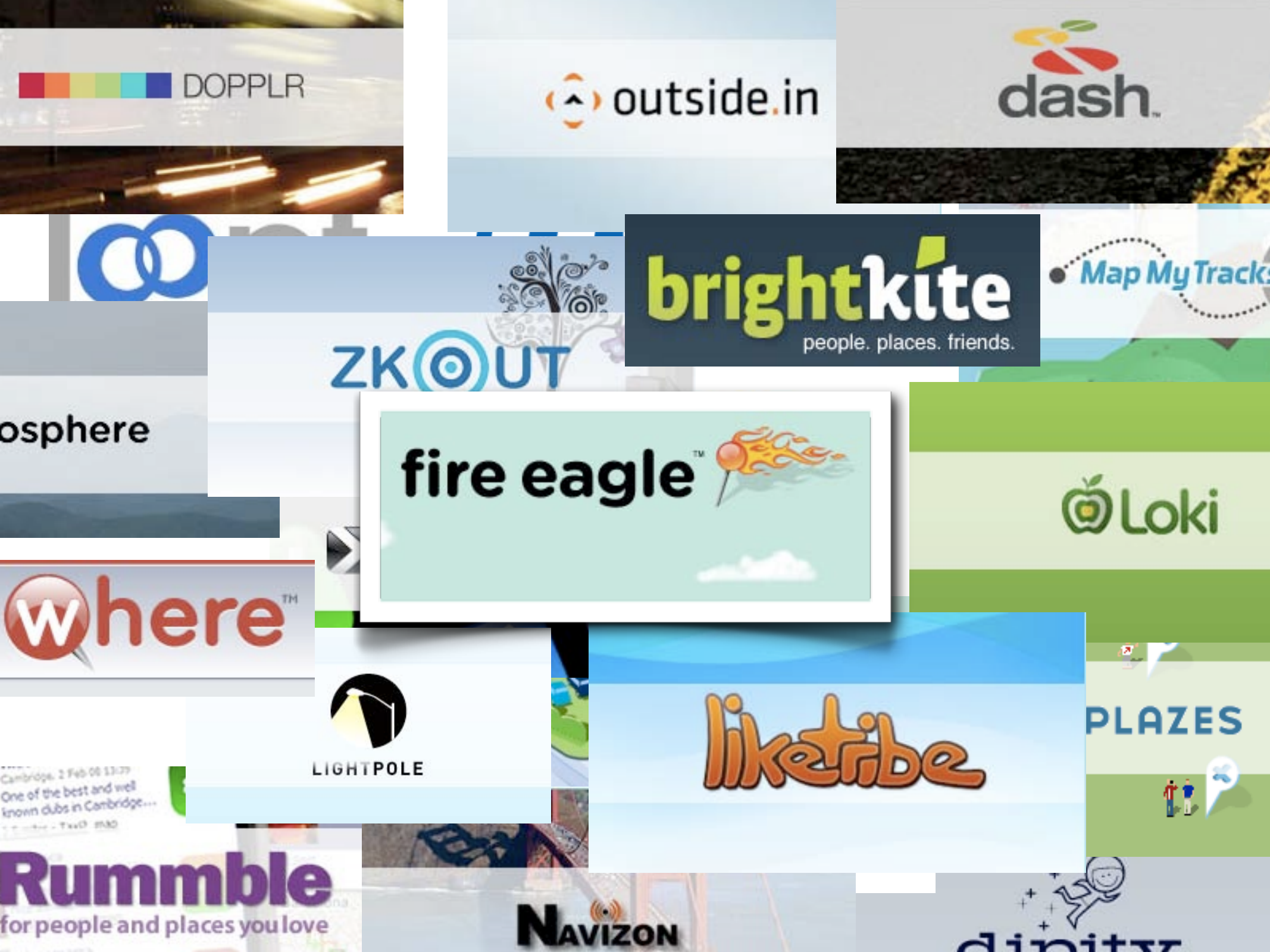
loopt

meetro

HELIO

android


DOPPLR
outside.in
dash
brightkite
people. places. friends.
Map My Tracks
ZKOUT
osphere
OUTALOT
Loki
where
LIGHTPOLE
liketribe
PLAZES
Rummble
for people and places you love
NAVIZON


DOPPLR
outside.in
dash
brightkite
people. places. friends.
Map My Tracks
ZKOUT
fire eagle
Loki
where
LIGHTPOLE
liketribe
PLAZES
Rummble
for people and places you love
NAVIZON

Your Privacy:

We believe this is
not enough...

Users have control:

Time

Location

Group

Facebook | pplFindr4fbook

http://apps.facebook.com/pplfindr/index.php?id=24400569

Google

Facebook | pplFindr4fbook

facebook

Profile edit | Friends | Networks | Inbox | home account privacy logout

Search

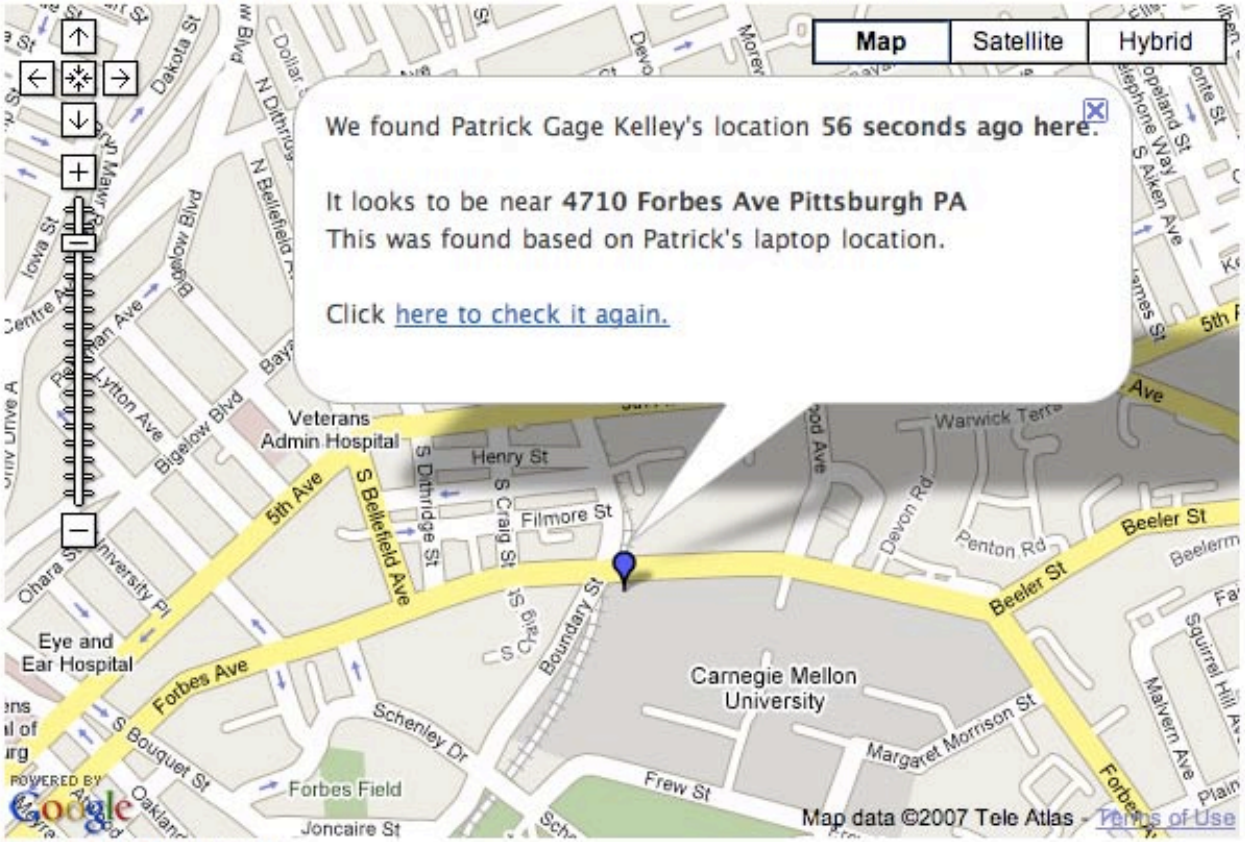
Applications edit

- pplFindr4fbook
- Photos
- Groups
- Events
- Marketplace
- Developer
- del.icio.us

more

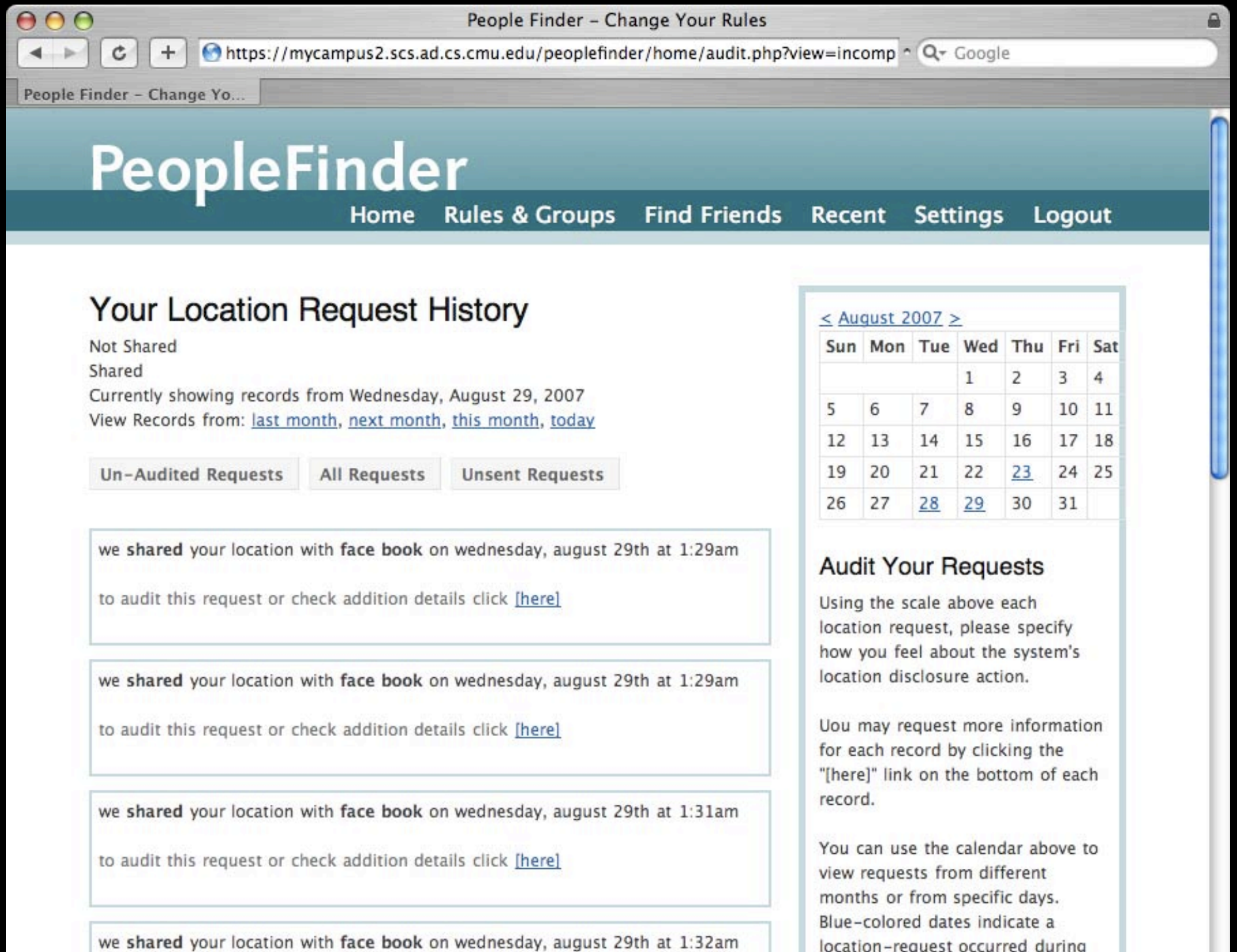
PeopleFinder

Patrick's Location



[back to find a friend]

PeopleFinder was created by the Mobile Commerce Lab at Carnegie Mellon University


People Finder – Change Your Rules
https://mycampus2.scs.ad.cs.cmu.edu/peoplefinder/home/audit.php?view=incomp
Google
People Finder – Change Yo...
PeopleFinder
Home
Rules & Groups
Find Friends
Recent
Settings
Logout
Your Location Request History
Not Shared
Shared
Currently showing records from Wednesday, August 29, 2007
View Records from: last month, next month, this month, today
Un-Audited Requests
All Requests
Unsent Requests
we shared your location with face book on wednesday, august 29th at 1:29am
to audit this request or check addition details click [here]
we shared your location with face book on wednesday, august 29th at 1:29am
to audit this request or check addition details click [here]
we shared your location with face book on wednesday, august 29th at 1:31am
to audit this request or check addition details click [here]
we shared your location with face book on wednesday, august 29th at 1:32am
< August 2007 >
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
Audit Your Requests
Using the scale above each location request, please specify how you feel about the system's location disclosure action.
Uou may request more information for each record by clicking the "[here]" link on the bottom of each record.
You can use the calendar above to view requests from different months or from specific days. Blue-colored dates indicate a location-request occurred during

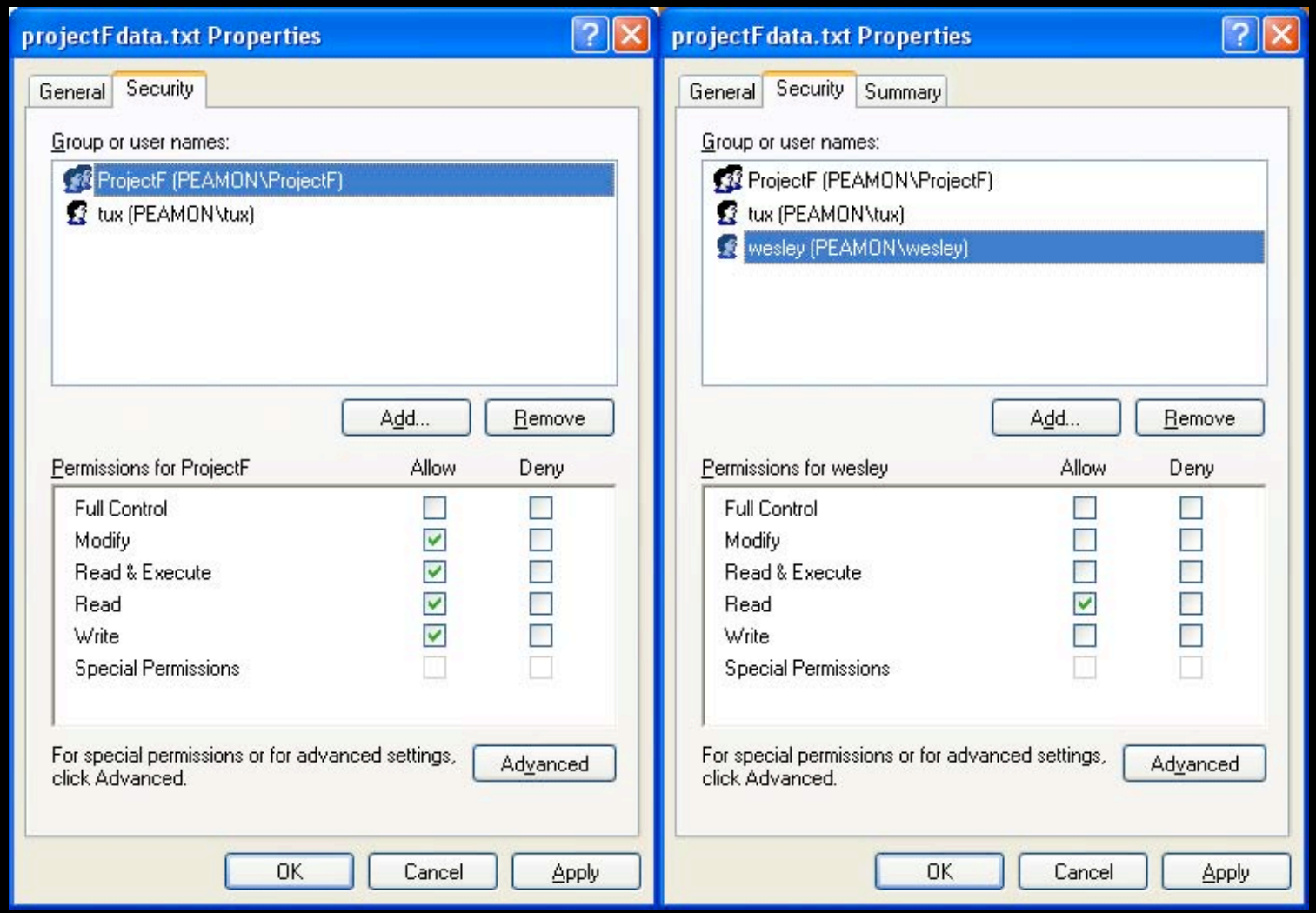
we want to show that managing complex policies on a mobile device is possible

this way we can give users more control than a simple on/off switch

Policy Authoring Basics

- Default rules (What happens when no rule applies?)
- **Composite values** (groups, folders, etc.)
  - What are the component values?
- **Rule conflicts** & tie-breaking are frequent
  - What if more than one rules applies?
- **Scale** - Large policies can get tricky

To begin with...

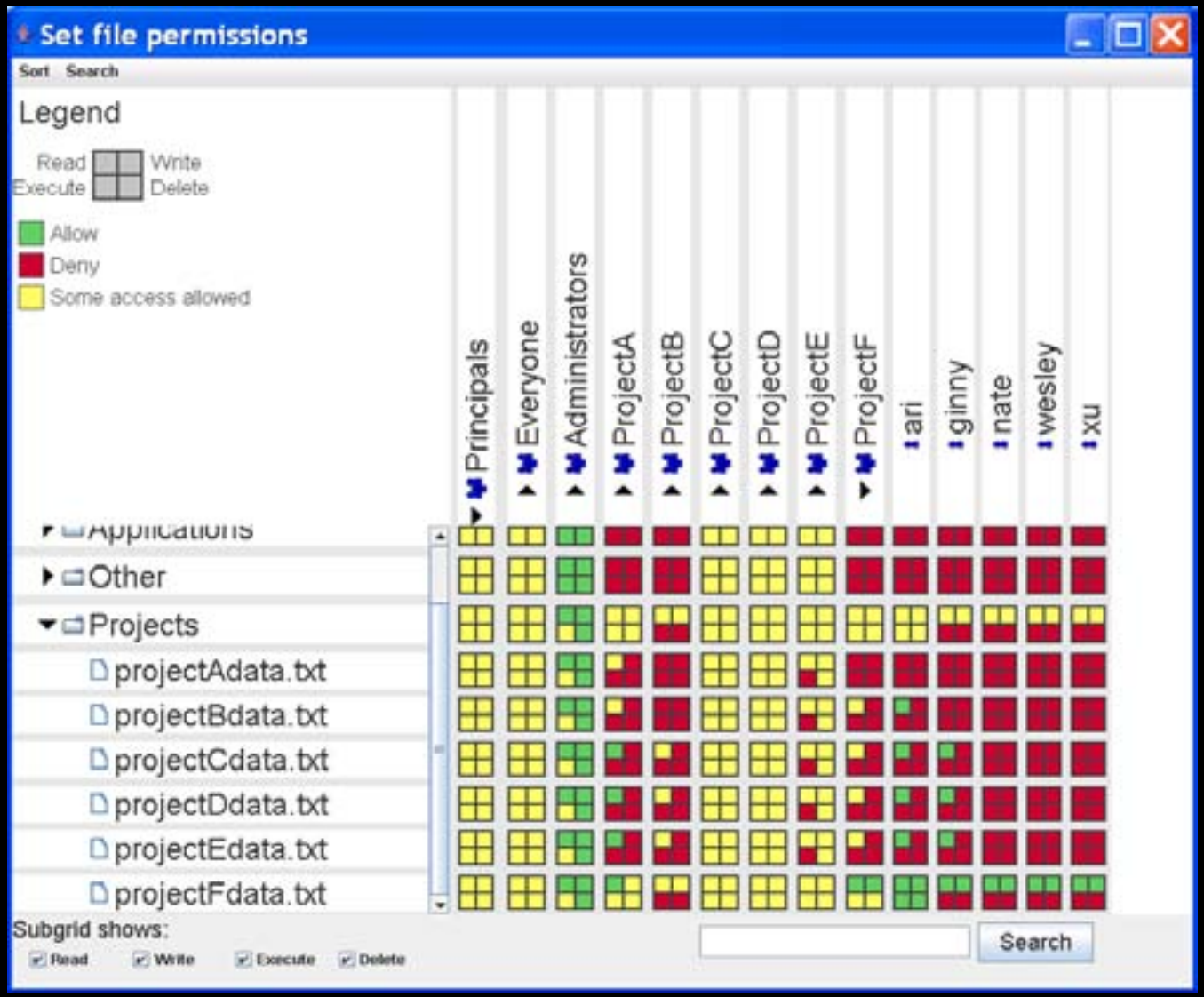


Expandable Grids

- Key insight: Policy-authoring user interfaces should display the **whole effective policy, not a list of rules**

- **Visualization** technique developed by Rob Reeder while at IBM

Expandable Grids



User Controllable Learning of Security & Privacy Policies

(patent pending)

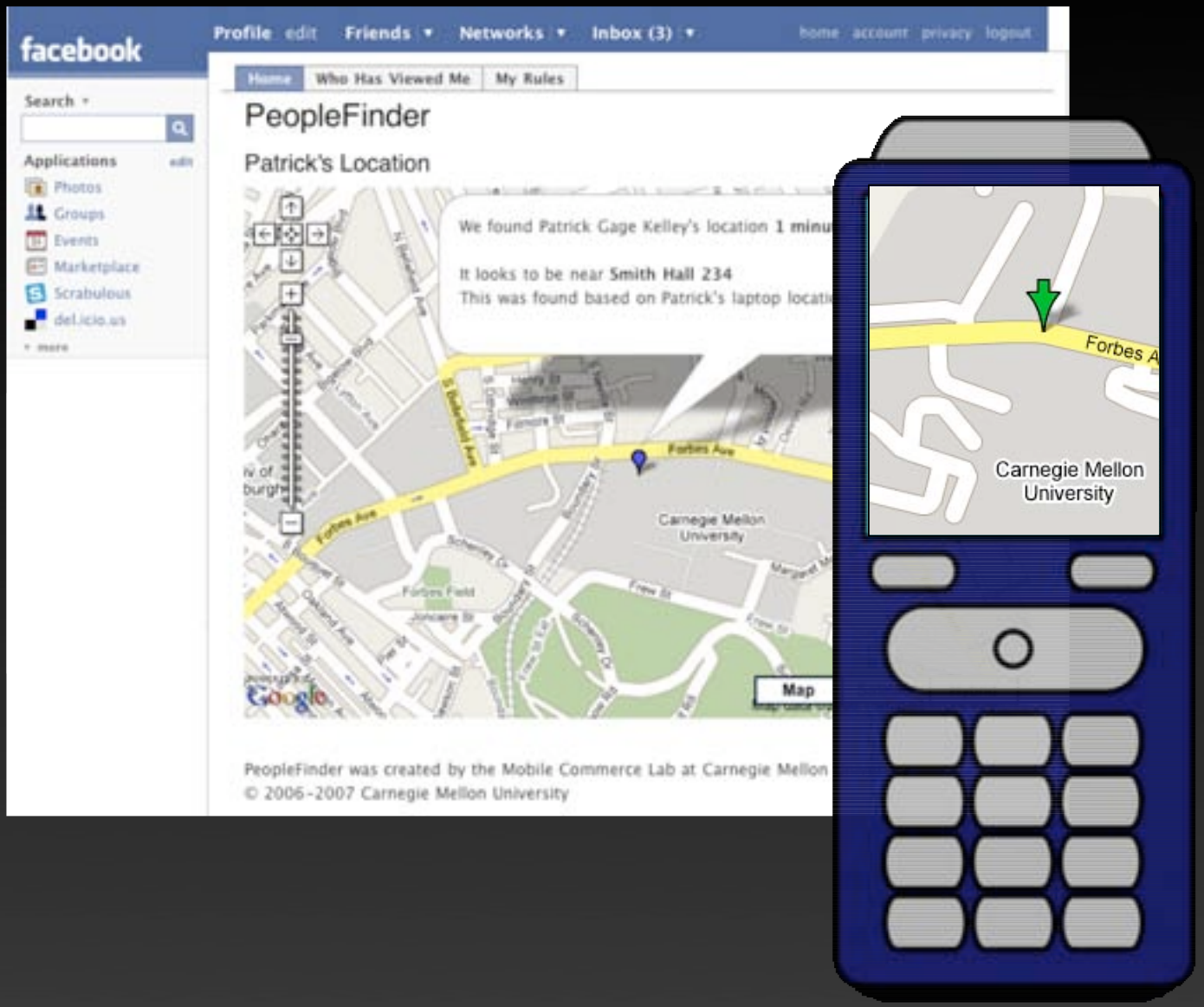
Patrick Gage Kelley

with
Paul Hankes Drielsma, Norman Sadeh, and Lorrie Faith Cranor
Carnegie Mellon University School of Computer Science

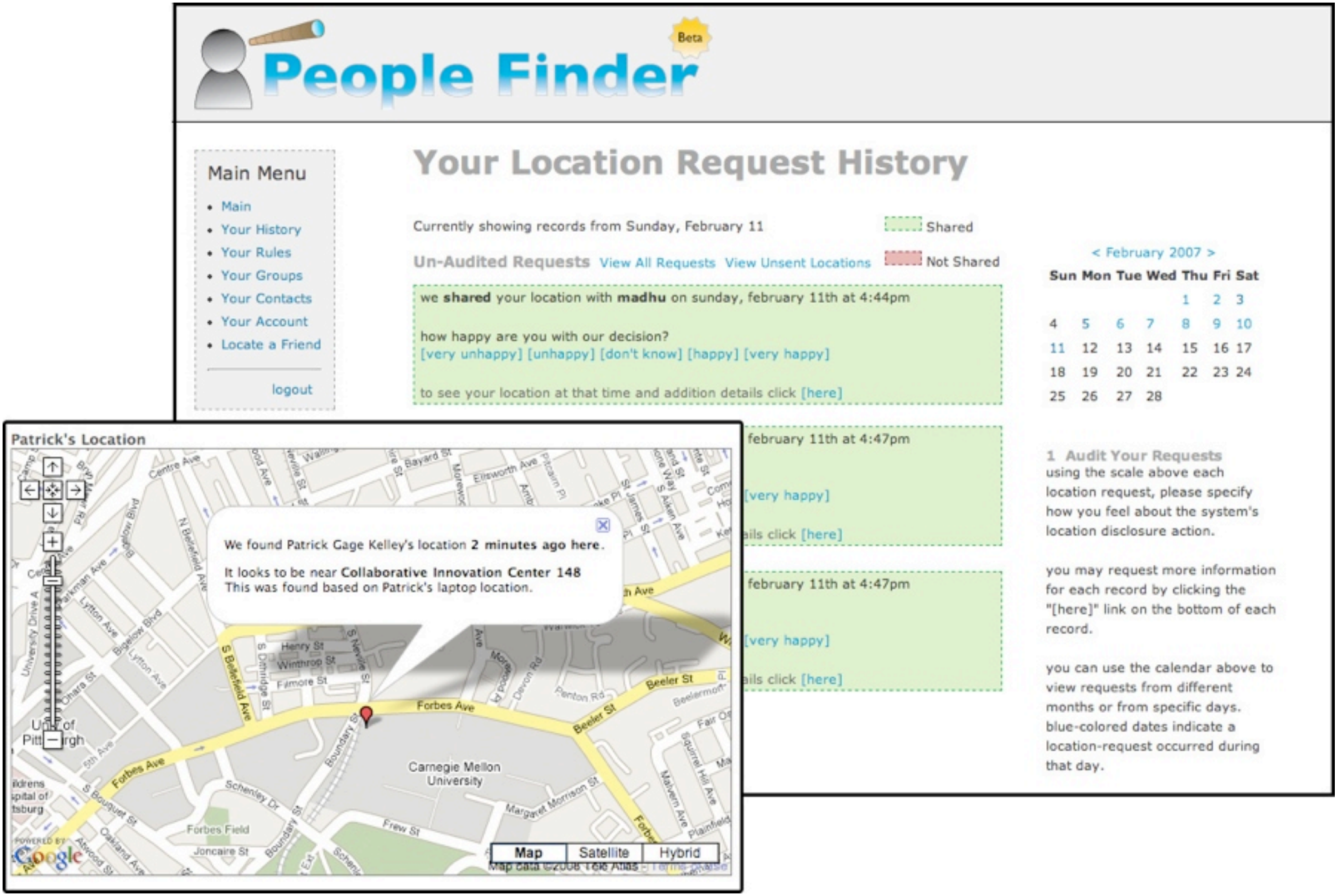
users have great difficulty specifying their security and privacy policies

User-Controllable Policy Learning

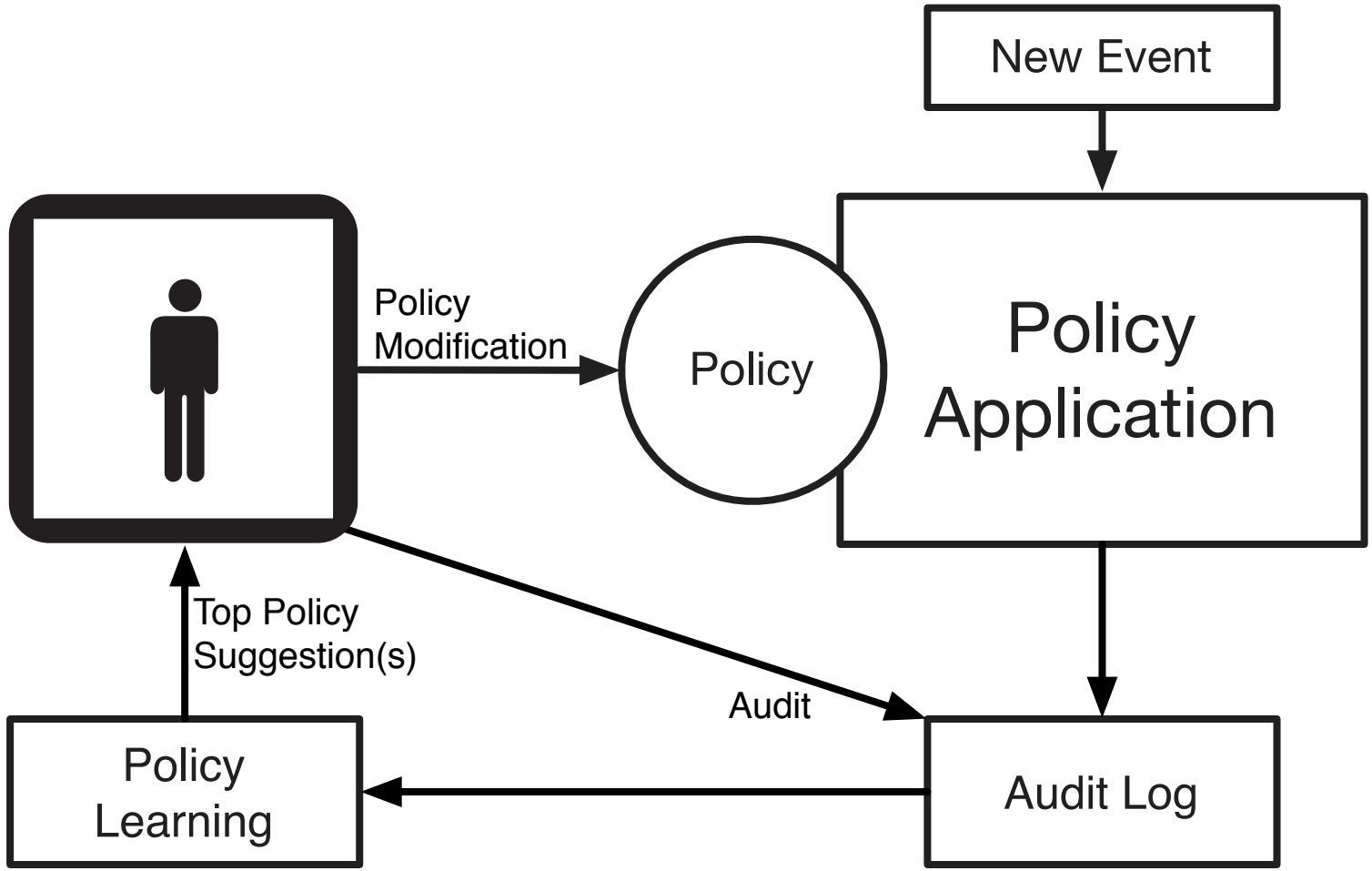
- **Incremental** manipulation of policies
- System and user refine a **common** policy model
- The user regularly provides feedback
- This feedback is used to identify *(learn)* incremental policy improvements which are presented as **suggestions** to the user
- The user reviews these suggestions and decides which to accept



PeopleFinder



PeopleFinder | An Example



System Diagram

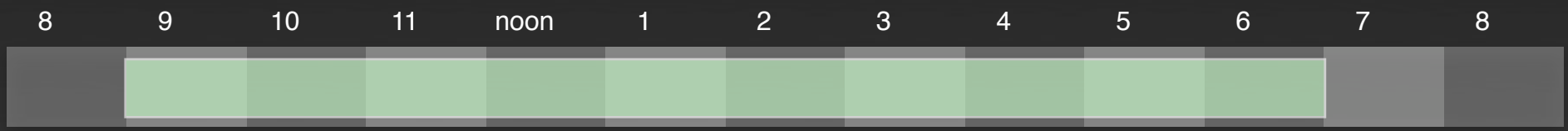
Simulated Results

- Based on real world PeopleFinder deployments
  - Used numbers of rules, groups, contacts as baseline
  - Simulated an average of five requests per day
  - Simulated policy change every other day

Let’s imagine a rule that we have created for a user, Dean.

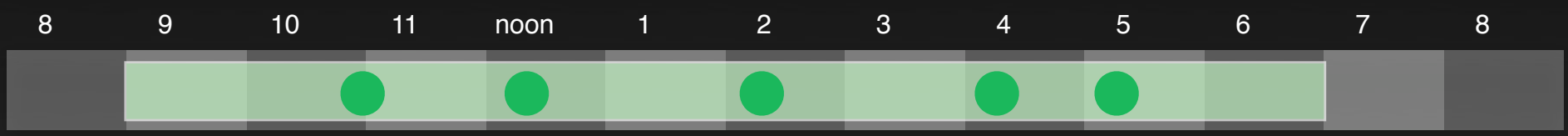
We want Dean to be able to view our location any day of the week, from 9 AM to 7 PM.

Now, let’s create a rule for his brother Hank. We want decide to give Hank a policy similar to Dean’s rule.

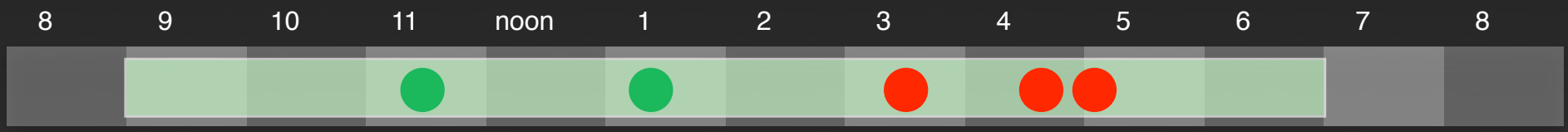


Now in continuing the last example, after a week, lets say I have checked my Query Log, and noticed that both Hank & Dean have both queried my location five times. I audit each of these with how I felt about my location being revealed.

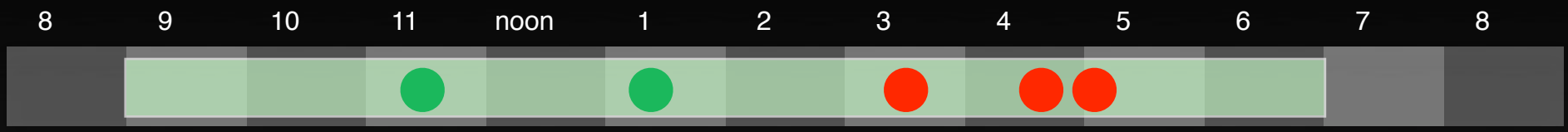
Dean



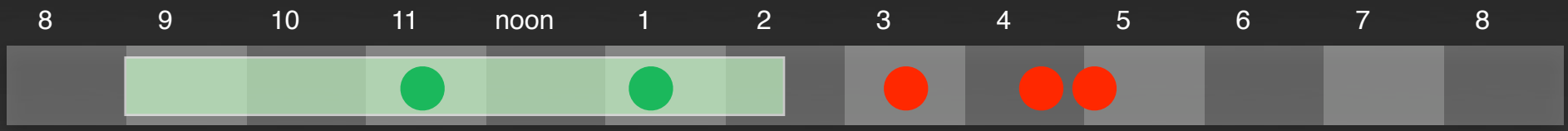
Hank



It is clear now that with these three bad audits, Hank's rule needs to be modified.

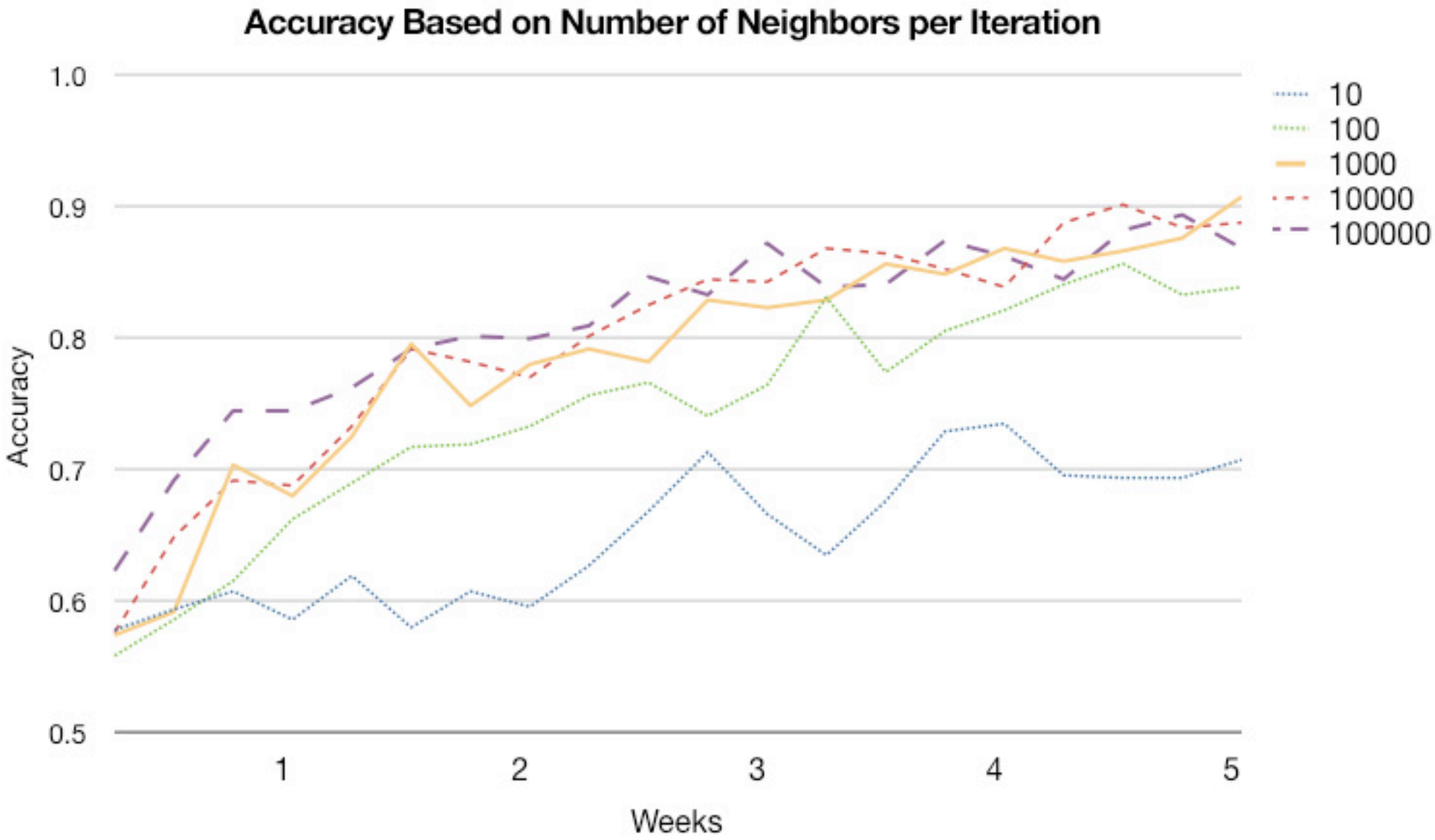


To a human we want to remove Hank's ability to see our location in the afternoon - simply shrinking the amount of hours he can view our location - in this simple case. But how can we generalize this type of change?

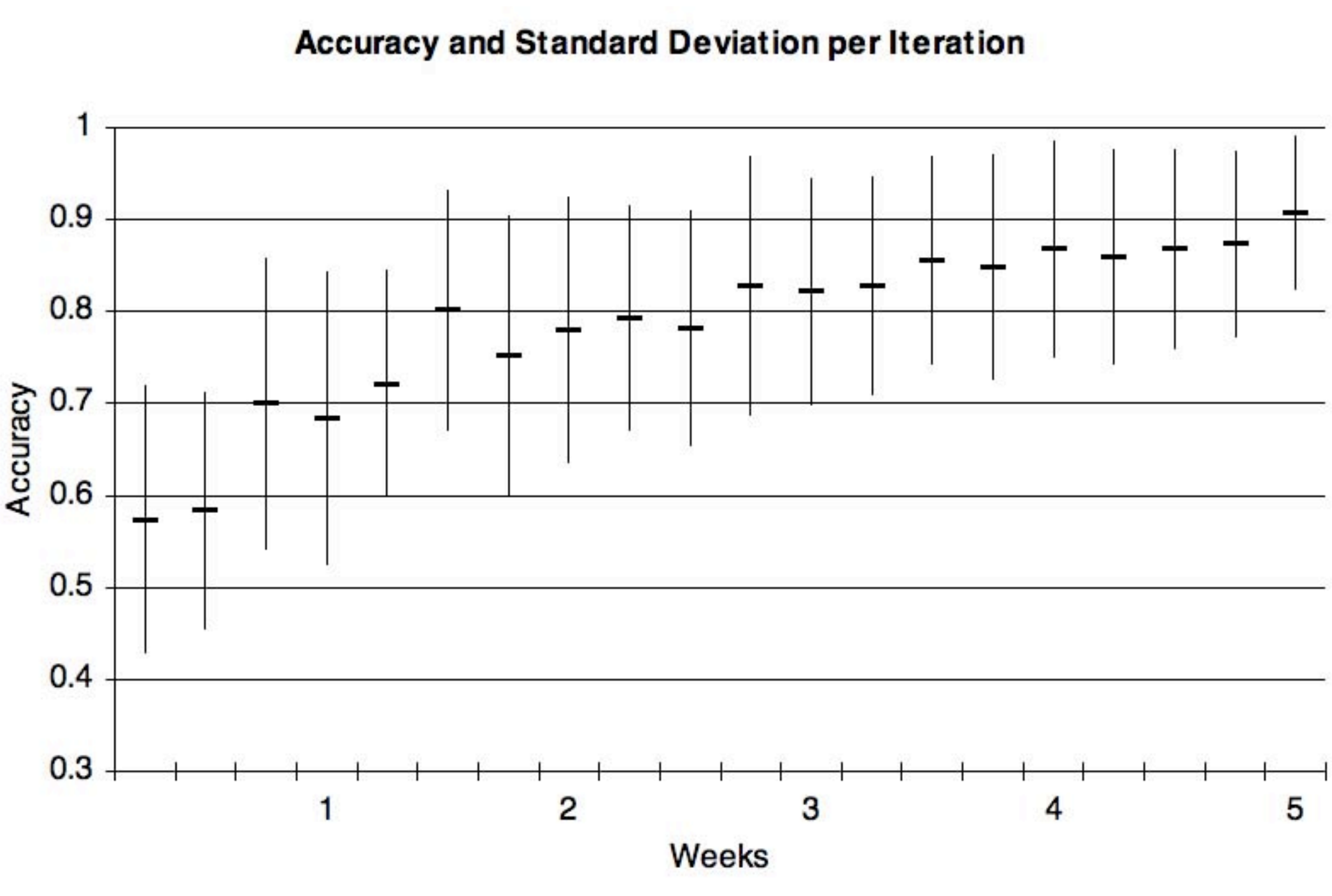


Policy Modifications

- The deletion of a rule, or the addition of a rule permitting disclosure to a user during a time span on a day.
- Change of either the start or end of a time-span
- Deletion or addition of a day to/from within a rule
- Deletion or addition of a person to/from a group



Accuracy of Increased Neighbors



Accuracy & Standard Deviation

Future Work

- We intend to further validate the model introduced here in the field
  - Testing usability and cognitive burden in our rule-specification and suggestion interfaces, followed by adoption and verification of the simulation accuracy results in our application
- We also see great potential in applying this model to policy improvement tasks in other areas: for instance, administrative tools for security applications such as firewall management, and also access control systems.

“Seems kinda stalker-ish”

“I would want to see other people but I wouldn’t want them to see me.”

“I think it is because I hate text messages. I would rather just call them.”

“I am worried about the contacts I would meet. I can’t be friends with people who have this phone, they must be more of a geek than I am ... Maybe in the future.”

“I would tag locations, but I would just meet my friends, not new people.”

“I think it is better because you can get a hold of people without necessarily calling them.”

“I don’t want them to find me too often I might feel violated. If it happens a lot.”

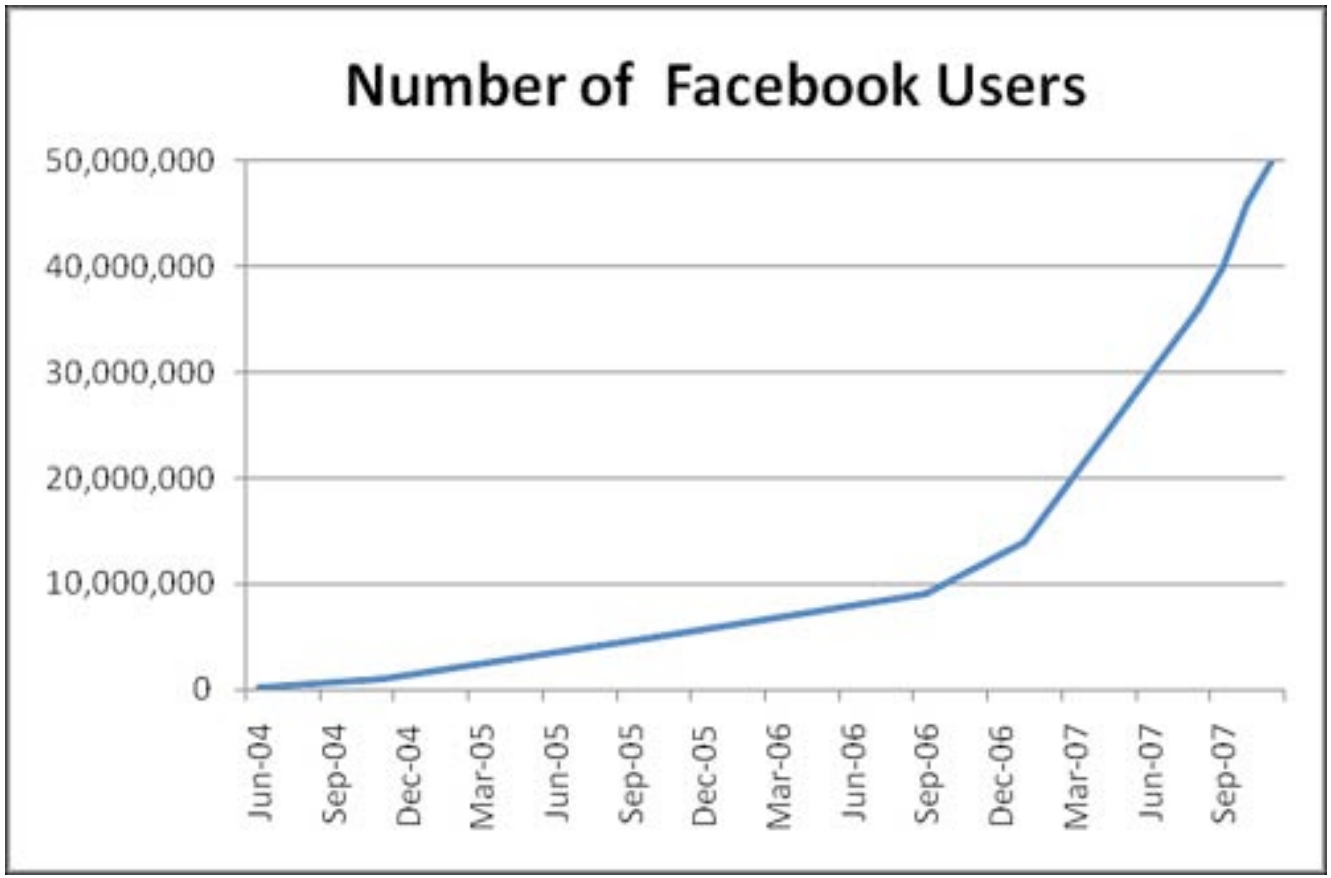
“Go around to a certain area, competing wth your friends. If I am member to a certain service, that I don't have to play or join, i will probably use it. I don't know if I would pay or do anything extra to do it. Playing is fun, but it needs to come up.”

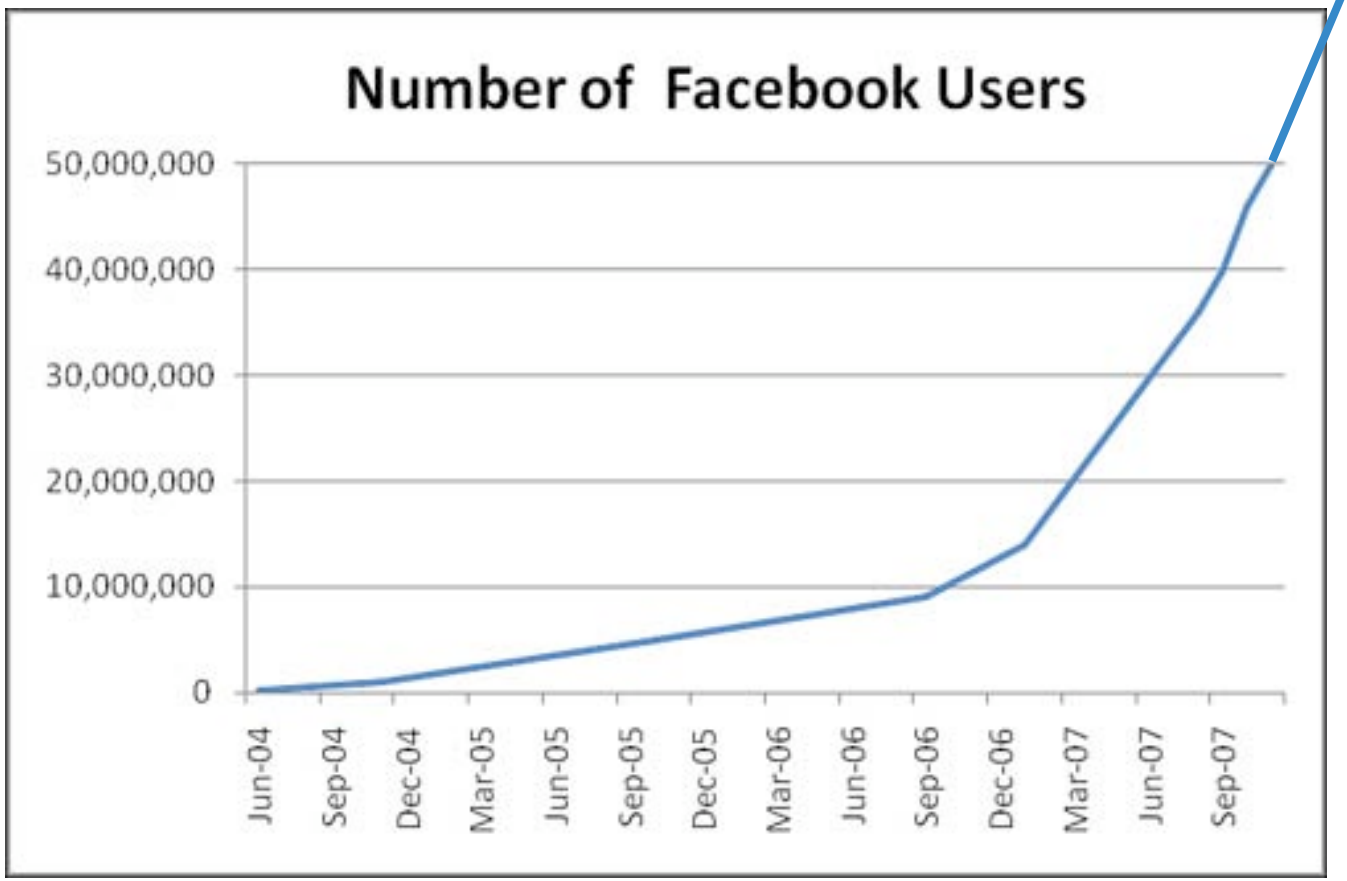
Response


facebook®

Facebook's chief operating officer,
Owen Van Natta, describes the opportunity
this way: "Take anything today on the Internet and
overlay a lens that is the people you know and
trust."

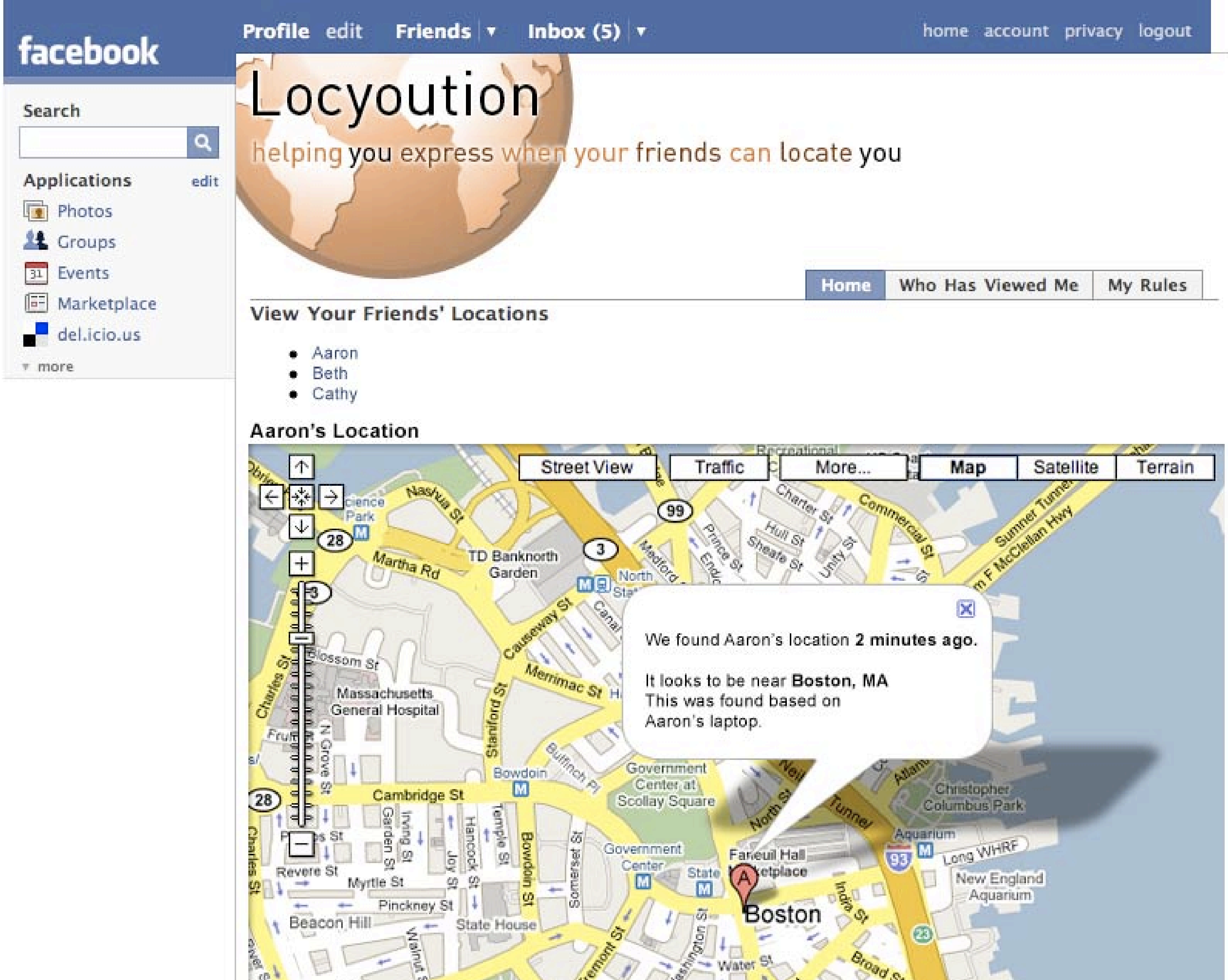
CrunchBase


Number of Facebook Users
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
Jun-04
Sep-04
Dec-04
Mar-05
Jun-05
Sep-05
Dec-05
Mar-06
Jun-06
Sep-06
Dec-06
Mar-07
Jun-07
Sep-07



September 2008
105 Million Active Users

Average Visit Time


facebook
Profile edit Friends Inbox (5)
home account privacy logout
Search
Applications edit
Photos
Groups
Events
Marketplace
del.icio.us
more
Locyoution
helping you express when your friends can locate you
Home
Who Has Viewed Me
My Rules
View Your Friends' Locations
Aaron
Beth
Cathy
Aaron's Location
Street View
Traffic
More...
Map
Satellite
Terrain
We found Aaron's location 2 minutes ago.
It looks to be near Boston, MA
This was found based on
Aaron's laptop.
TD Banknorth Garden
Massachusetts General Hospital
Government Center at Scollay Square
Christopher Columbus Park
Faneuil Hall Marketplace
New England Aquarium
Beacon Hill
State House
Boston

Locyoution

2. Platform Policy Overview: What Applications Cannot Do

We're excited about the growth of Facebook Platform and always do our best to ensure a thriving application ecosystem where user experience is paramount -- which we believe also creates the best developer experience.

In keeping our users' best interests as our primary goal, applications cannot:

1. Generate any notification, request, invitation, News Feed story, Mini-Feed story, profile box content, or message on behalf of a user that misrepresents that user's activity in any way. All representations of action taken by a user must correspond to actions a user has initiated within your application.
2. Represent themselves or any features of the application as Facebook, such as using Facebook product terms like "wall" or "message" to refer to something other than Facebook's functionality of the same name, unless there is an agreement in writing to the contrary.
3. Express or imply any affiliation or relationship with or endorsement by Facebook.
4. Contain anything designed to mislead, confuse, or defraud the user in any way.
5. Present a user with a subsequent friend invite page if the user has already clicked a Facebook-rendered **Skip**, **Cancel**, or **Skip This Step** button, unless the user explicitly selects to invite friends from a page that offers more than just the friend invite option. If the application presents the user with a friend invite page that does not include a Facebook-rendered **Skip**, **Cancel**, or **Skip This Step** button, the application must offer some navigation option to leave the friend invite process, and the application must never present the user with a subsequent friend invite page unless the user explicitly selects to invite friends from a page that offers more than that single option.
6. Require that users invite, notify, or otherwise communicate with one or more friends to gain access to any feature, information, or portion of the application, unless (a) it would be logically impossible to deliver that content without the user's friend(s) also using the application, and (b) the fact of this requirement, and the reason(s) for it, are explicitly and prominently explained inside the application before the first element of the flow path users would reasonably expect to lead to that content.
7. Include JavaScript actions pretending to be user actions.
8. Track visits to a user's profile, whether aggregated anonymously or identified individually.
9. Contain content or features unsuitable for consumption by the general Facebook user base unless a description of the nature of the content is on the application's About page. Examples of appropriate descriptions include: "strong language, fantasy violence, simulated gambling", and so forth.
10. Deliver content via Facebook "push" communication methods (including notifications, feed stories, requests, and notification email) to people who are not users of the application unless the content is suitable for consumption by the general Facebook user base. For example, application-generated and user-generated content in requests and feed stories cannot use objectionable language or evoke adult themes.
11. Contain functionality that exceeds the dimensions of the canvas page.
12. Publish stories in which the user is a passive actor. The user must be the person performing the action in order to generate a story about that user. In technical terms, this means the feed.publishTemplatizedAction API method ignores the `actor_id` parameter and uses the session key to generate the feed story.
13. Promote other applications in notifications in order to pool notifications together and work around either application's allocation limit.
14. Put links into feed stories and notifications that trick users into installing another application.
15. Tag images, nor encourage users to tag images, when the tag does not accurately label what is depicted in the image.
16. Store API data about a user unless the the application clearly gives the user the choice to submit the data, and the user agrees. It must be made clear to the user prior to submission that this data will be stored by the application/developer, and not by Facebook.
17. Use another user's session key when making a call to the Facebook Platform API. You must use the session key of a user who is actively using the application.
18. Send notifications conveying information to a user about the discrete action(s) of one or more other users more than 12 hours after completion of the oldest action referenced in the notification, unless the notification explicitly indicates the particular time when the oldest action was initiated by the user taking the action or completed by the application.

    Examples:

    1. "<Username> posted an item on <your Appname> Board." This user action, and the application completion of the action, are nearly simultaneous. The API call to send this notification must be initiated within 12 hours of the action.
    2. "<Username> sent you a birthday gift. Click here to see it." If <Username> took an action in the application on January 5th indicating he wanted to send this birthday gift to the recipient on February 9th, and the application did indeed deliver the gift inside the application on February 9th, the API call to send this notification must be made within 12 hours of the application delivering the gift.
    3. "Three of your friends posted items on <your Appname> Board." The API call to send this notification must be made within 12 hours of the first friend posting to the recipient's board.
    4. "Yesterday, <Username> posted an item on <your Appname> Board." If factually correct, this notification can be sent more than 12 hours after the event. However, because the information is not timely, this is a departure from best practices and might result in adverse feedback from users, leading to restrictions on the notifications allocation for your application. Best practices dictate you only send delayed notifications when there is particular user benefit in doing so.

All disclosures required by Facebook policy must be in a location and font size, style, and color, that makes the information readily apparent to the user.

Suitability of content for the general Facebook user base: While additional standards may apply, Facebook typically deems content unsuitable for the general user base if it does not meet MPAA **PG-13** and ESRB **Teen** standards.

The policies in this section took effect noon Pacific Daylight Time, 17 June, 2008.

1. **Principle: Users must not be surprised by the outcome of an action they take.**

   Details: When an application offers a user an option to take an action, the user interface must make clear at the point of first click/first step (rather than just in a subsequent confirmation step):

   (a) what the action is, and

   (b) who is being acted upon or falls within the scope of the action, and who will receive notice of the action.

   (c) When it is technologically reasonable to do so, the application should offer a readily discoverable way to reverse, undo, nullify, recall, or delete the consequences of any action that doesn't have the presumption of irreversibility (such as a payment or move in a game with no "take-backs").

2. **Principle: To ensure users only take actions they intend, an application must avoid one-click triggers of actions that apply to multiple people, except in special circumstances.**

   Details: When an action in an application applies to more than one person, or causes the delivery of a direct communication (other than a Feed story) to more than one person (whether that communication is entirely within the application or via a Facebook communication channel), the user's activity that triggers the action must consist of more than one click or one step, unless

   (a) the one-click action is part of an engagement in a sub-part of the application where all of the recipients would expect to receive such a communication, or be the objects of such an action, because of an activity they have chosen (such as when making a move in a synchronous multi-player game, or sending a message in a chat room).

   (b) The following are insufficient to qualify under clause (a): the recipients are (i) friends with the acting user, (ii) have authorized the application, or (iii) have visited the canvas page.

3. **Principle: To ensure users only take actions they intend, multiple recipients must be selected by the user, rather than pre-selected by the application.**

   Details: Applications cannot pre-select more than one person to receive a communication or be acted upon. The acting user must choose multiple recipients individually -- for example, by clicking boxes next to their names -- or collectively, by clicking on or selecting a clearly and completely described group.

   (a) "Select all" is a permitted way to allow users to indicate multiple recipients from a list (as long as the user interface makes it clear who is encompassed by "all").

Additional Requirements

- Contain anything designed to mislead, confuse, or defraud the user in any way.
- Include JavaScript actions pretending to be user actions
- Track visits to a user's profile, whether aggregated anonymously or identified individually.
- Store API data about a user unless the the application clearly gives the user the choice to submit the data, and the user agrees. It must be made clear to the user prior to submission that this data will be stored by the application/developer, and not by Facebook.

These Matter

Values that are storable indefinitely:

uid	User ID
nid	Primary network ID
eid	Event ID
gid	Group ID
pid	Photo ID
aid	Photo album ID
notes_count	Total number of notes written by the user
profile_update_time	Time that the user's profile was last updated

The storable IDs enable you to keep unique identifiers for Facebook elements that correspond to data gathered by your application. For instance, if you collected information about a user's musical tastes, you could associate that data with a user's Facebook uid.

However, note that you cannot store any relations between these IDs, such as whether a user is attending an event. The only exception is the user-to-network relation.

Storable Information Policy

facebook

Profile edit | Friends | Inbox (5) | home account privacy logout

Search

Applications edit

- Photos
- Groups
- Events
- Marketplace
- del.icio.us

more

Locyoution

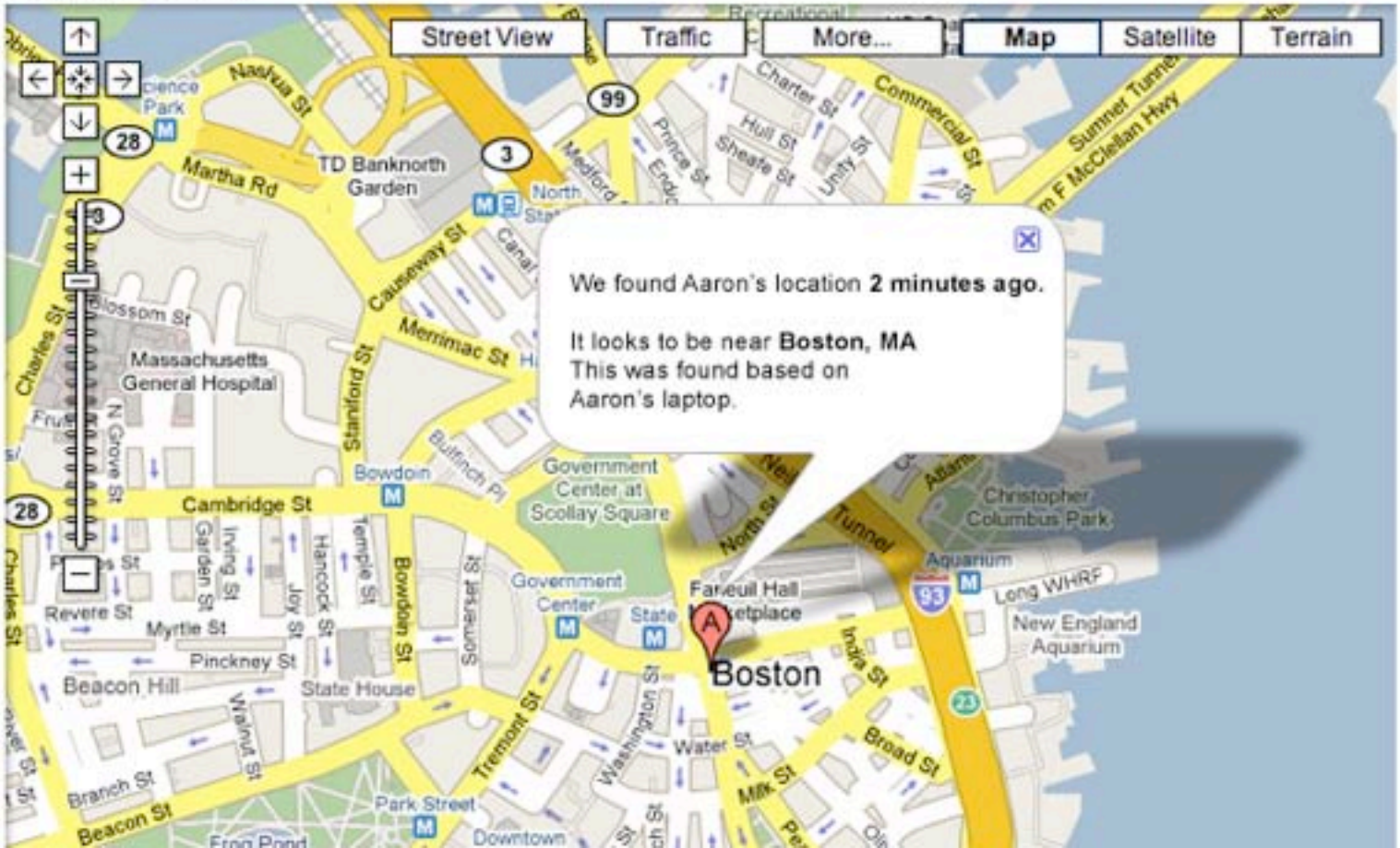
helping you express when your friends can locate you

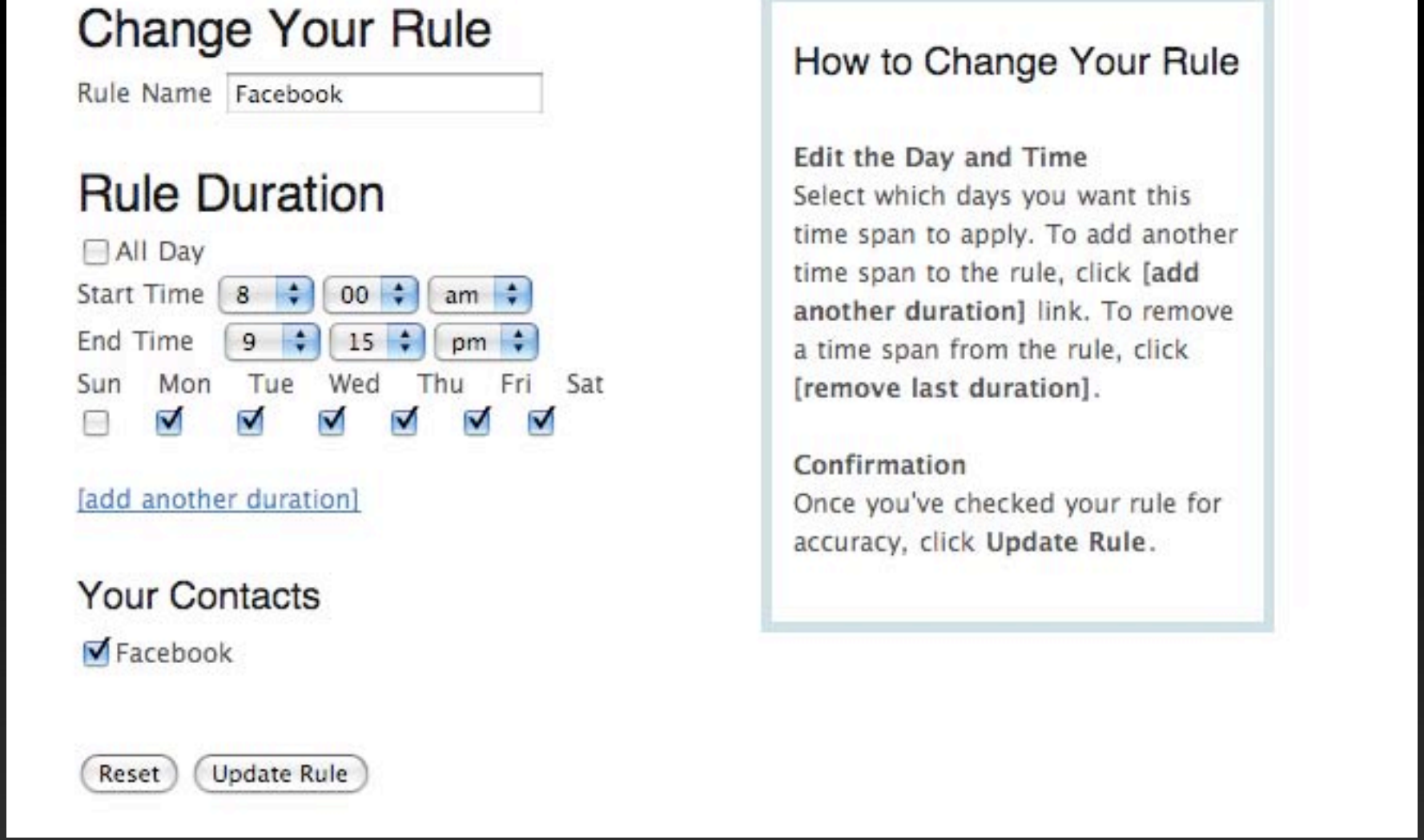
Home | Who Has Viewed Me | My Rules

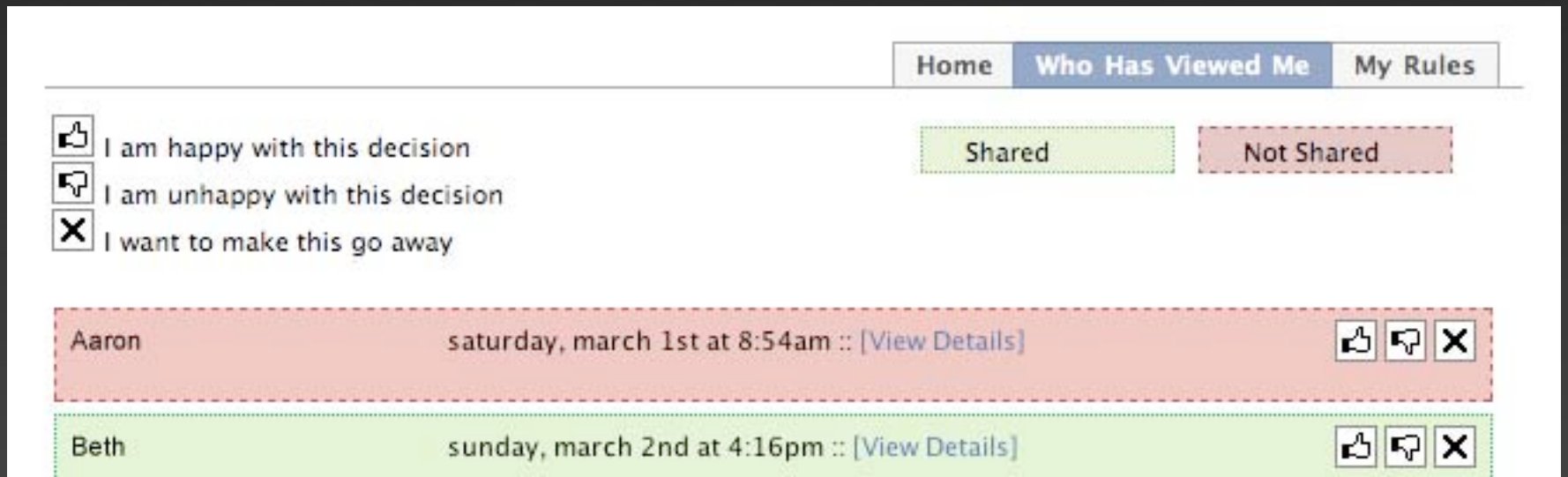
View Your Friends' Locations

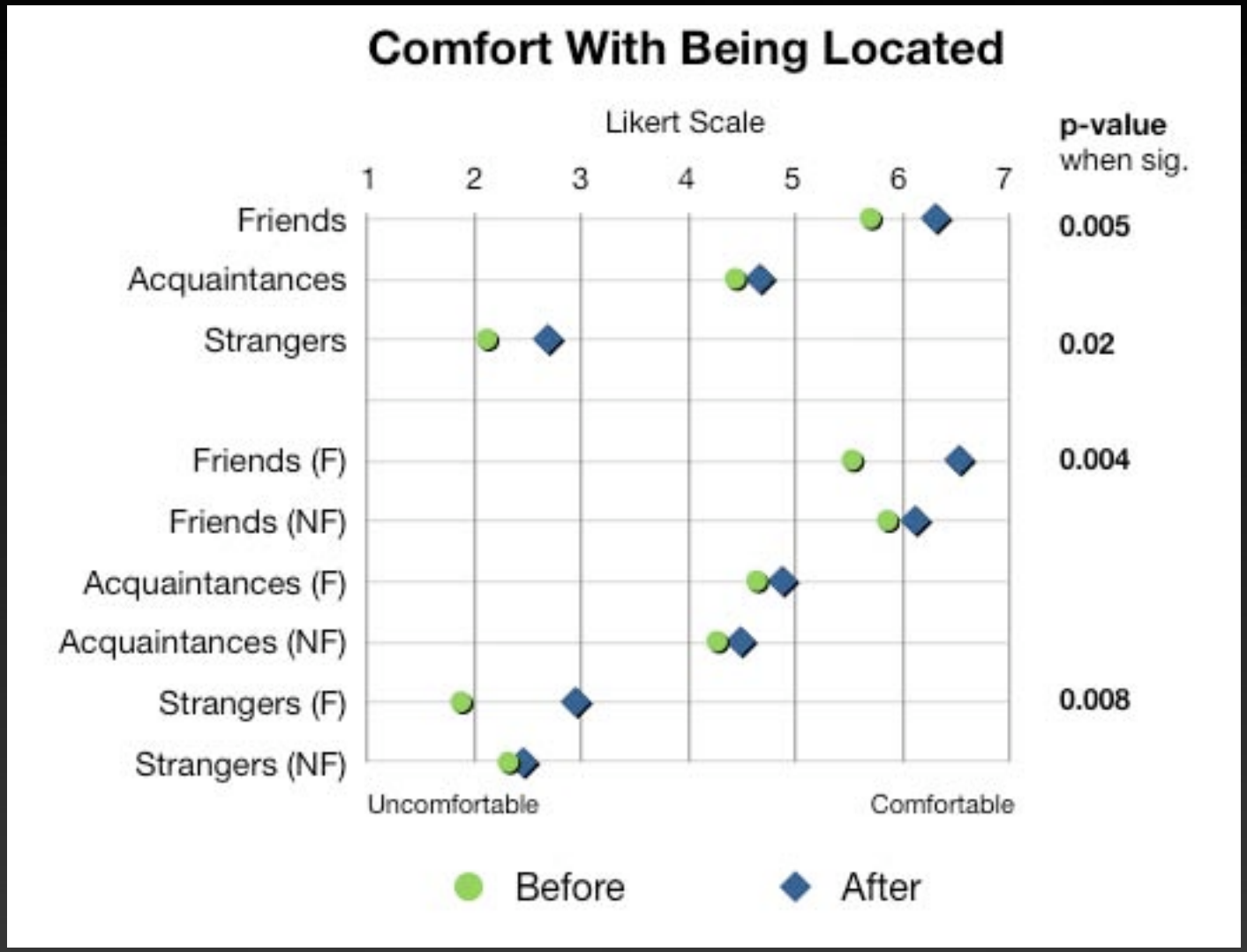
- Aaron
- Beth
- Cathy

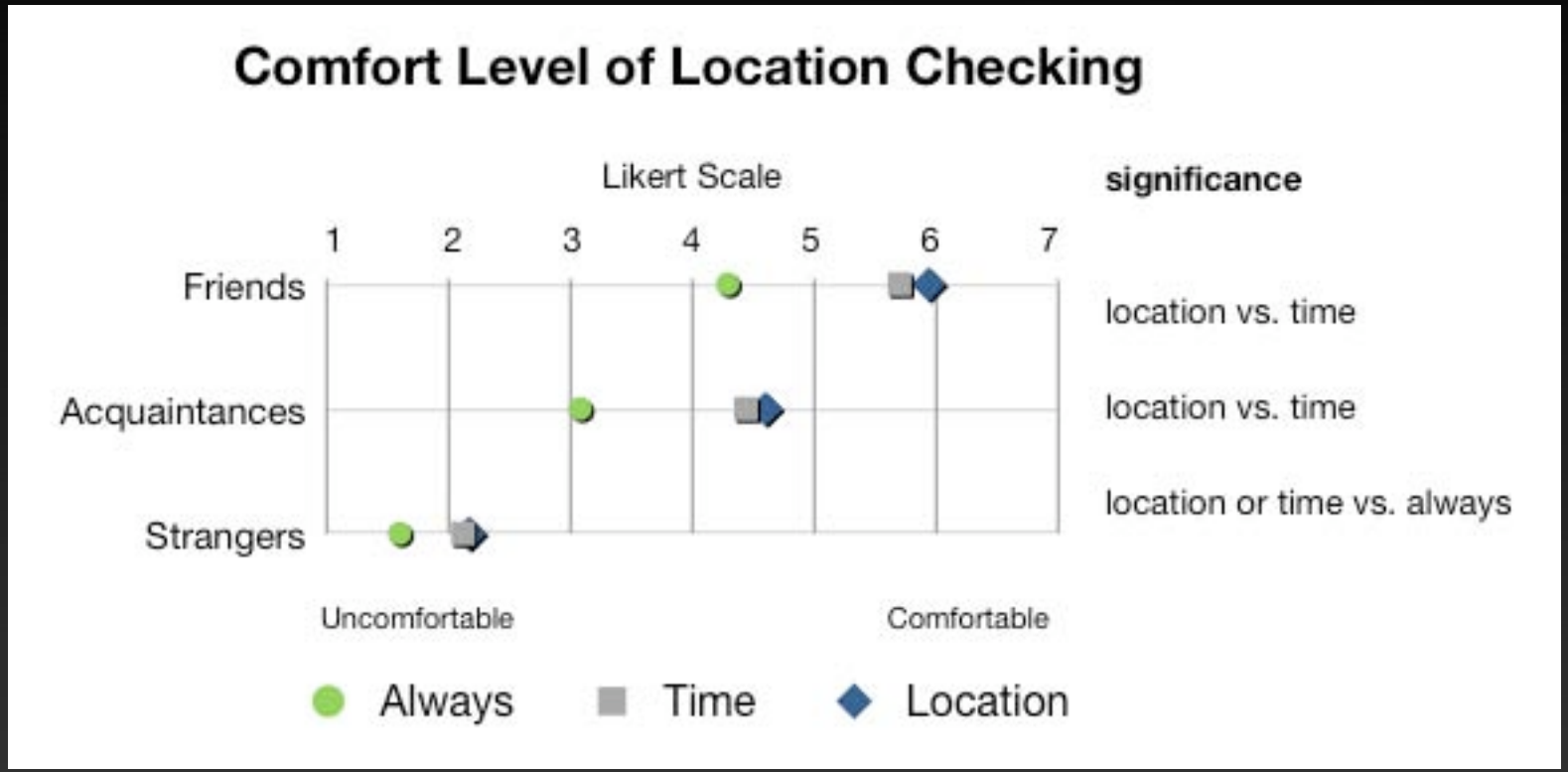
Aaron's Location



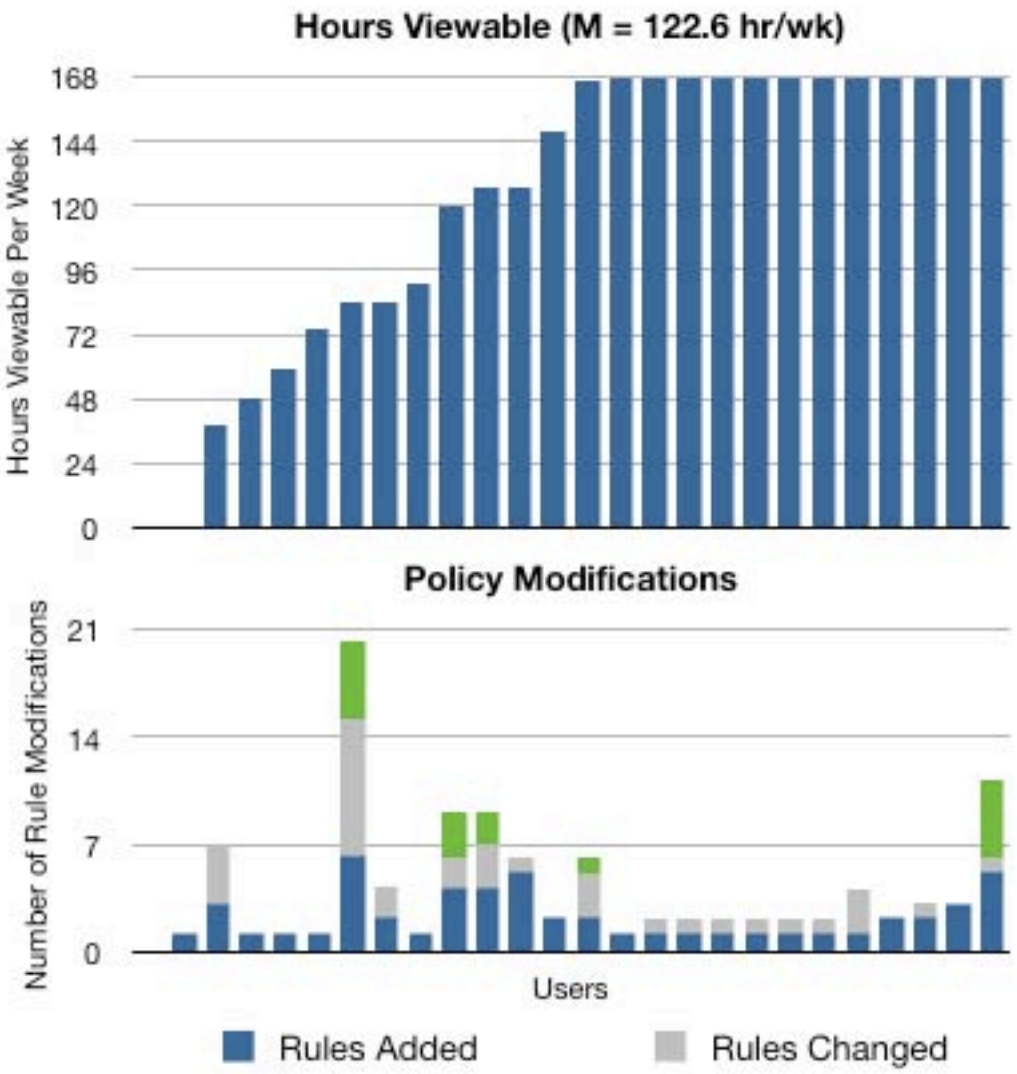

Change Your Rule
Rule Name Facebook
Rule Duration
All Day
Start Time 8 00 am
End Time 9 15 pm
Sun Mon Tue Wed Thu Fri Sat
[add another duration]
Your Contacts
Facebook
Reset
Update Rule
How to Change Your Rule
Edit the Day and Time
Select which days you want this time span to apply. To add another time span to the rule, click [add another duration] link. To remove a time span from the rule, click [remove last duration].
Confirmation
Once you've checked your rule for accuracy, click Update Rule.


Home
Who Has Viewed Me
My Rules
I am happy with this decision
I am unhappy with this decision
I want to make this go away
Shared
Not Shared
Aaron
saturday, march 1st at 8:54am :: [View Details]
Beth
sunday, march 2nd at 4:16pm :: [View Details]

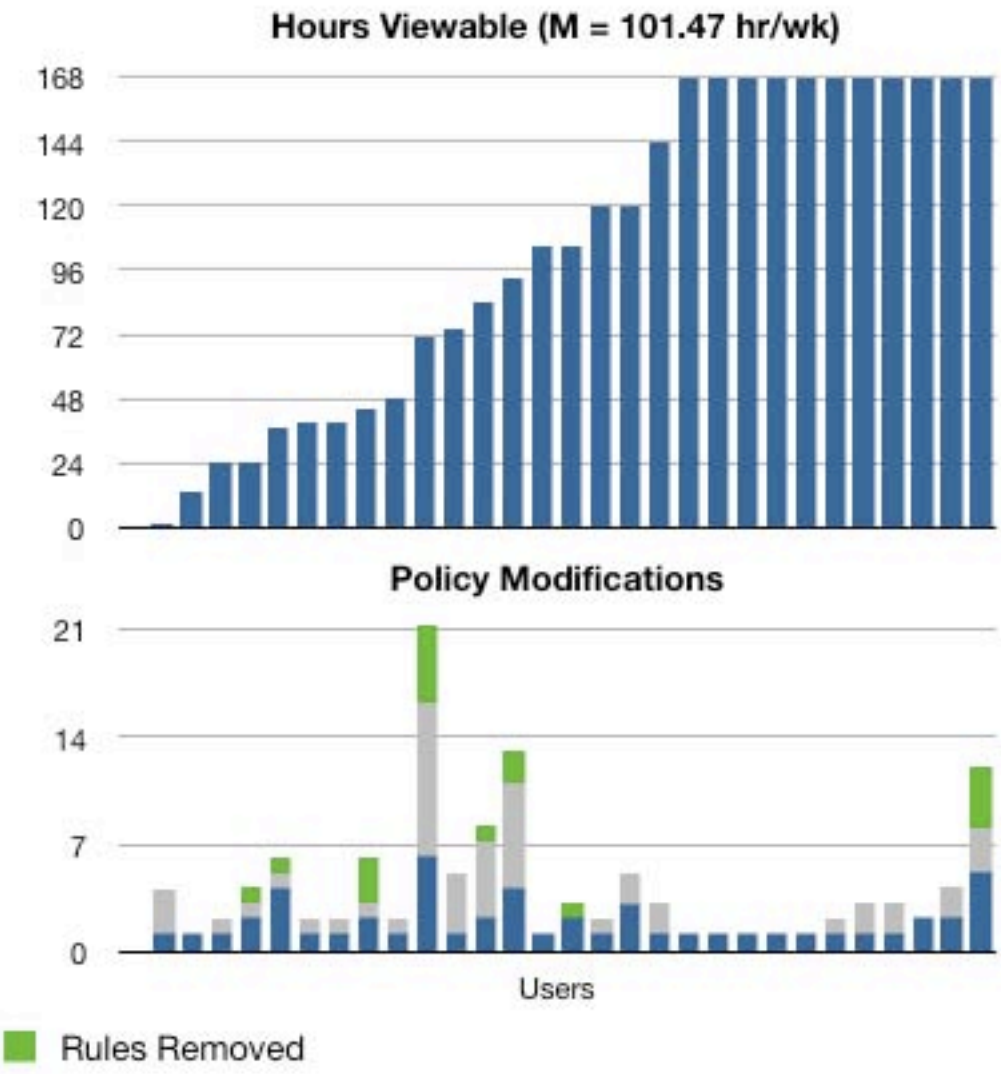

Comfort With Being Located
Likert Scale
1
2
3
4
5
6
7
p-value when sig.
Friends
Acquaintances
Strangers
Friends (F)
Friends (NF)
Acquaintances (F)
Acquaintances (NF)
Strangers (F)
Strangers (NF)
0.005
0.02
0.004
0.008
Uncomfortable
Comfortable
Before
After


Comfort Level of Location Checking
Likert Scale
1
2
3
4
5
6
7
Friends
Acquaintances
Strangers
Uncomfortable
Comfortable
Always
Time
Location
significance
location vs. time
location vs. time
location or time vs. always

Feedback



No Feedback



Lots more to do.

seriously.

PeopleFinder has been developed by the Mobile Commerce Lab at
Carnegie Mellon University

Norman Sadeh, Jason Hong, Lorrie Cranor, Paul Hankes-Drielsma, Ian Fette, Madhu Prabaker, Jinghai Rao, Janice Tsai, Jialiu Lin, Eran Toch, Jay Springfield, Harry Son, Tony Poor, Michael Benisch, Kami Vaniea, Robert Reeder

Patrick Gage Kelley
patrickgage.com
pgage@cmu.edu

http://cups.cs.cmu.edu
CMU Usable Privacy & Security Lab