

# Security as Risk Communication

Usability Is Not Enough

L Jean Camp

[ljean.com](http://ljean.com)

# Why Usable Security is Not Usability

- People rarely want to perform security tasks
- People often want to subvert, minimize, or ignore security
- People need to trust their machines, achieving suspicion is not a goal

# Usable Transparent Design

- Make the connection between action and consequence clear
- Risk is inherently probabilistic
  - There may be no consequence
  - Consequence is very likely to be delayed
  - Consequence may prove catastrophic
  - Action-risk-consequence information may be overwhelming

# Opaque Stops Actions

▼ [Help me understand](#)

When you connect to a secure website, the server hosting that site presents your browser with something called a "certificate" to verify its identity. This certificate contains identity information, such as the address of the website, which is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network).

In this case, the certificate has not been verified by a third party that your computer trusts. Anyone can create a certificate claiming to be whatever website they choose, which is why it must be verified by a trusted third party. Without that verification, the identity information in the certificate is meaningless. It is therefore not possible to verify that you are communicating with **mail.google.com** instead of an attacker who generated his own certificate claiming to be **mail.google.com**. You should not proceed past this point.

If, however, you work in an organization that generates its own certificates, and you are trying to connect to an internal website of that organization using such a certificate, you may be able to solve this problem securely. You can import your organization's root certificate as a "root certificate", and then certificates issued or verified by your organization will be trusted and you will not see this error next time you try to connect to an internal website. Contact your organization's help staff for assistance in adding a new root certificate to your computer.



# Opaque Stops Actions



## The site's security certificate is not trusted!

You attempted to reach **mail.google.com**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

Back

---

▶ [Help me understand](#)

# Opaque

Security as a default

Require explicit confirmation

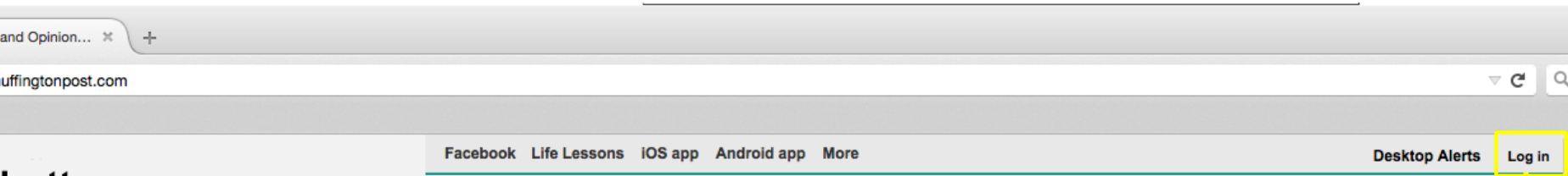
May be disabling

- So individuals disable it

# Beyond Usability

- Computing will not be scary so mitigation has to be very easy
- Risk information may be unpleasant
  - So show risk avoidance
- Visible user-action-system-consequence may be overwhelming or context dependent
- Be timely, careful, targeted, & personalized

# Security Behavior is Risk Behavior




button

December 13, 2014

THE HUFFINGTON POST **Log In**


My Account

 Sign In

A modal window for logging in. It has a title 'Log in or sign up' and a close button in the top right corner. Below the title, it says 'Use your CNN account to log in:'. There are two input fields: 'E-mail' and 'Password'. Below the 'E-mail' field is a 'Log In' text label with an arrow pointing to the 'LOG IN' button. Below the 'Password' field is a checkbox labeled 'Remember me for two weeks'. At the bottom left is a red button with the text 'LOG IN'.

# Decades of Consistent Security Training




 **Secure Connection Failed**

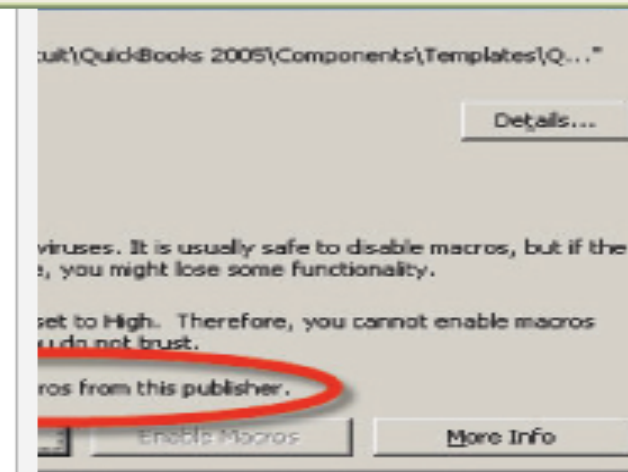
i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org uses an invalid security certificate.

The certificate is not trusted because the issuer certificate has expired. The certificate expired on 9/1/2004 6:00 PM.

(Error code: sec\_error\_expired\_issuer\_certificate)

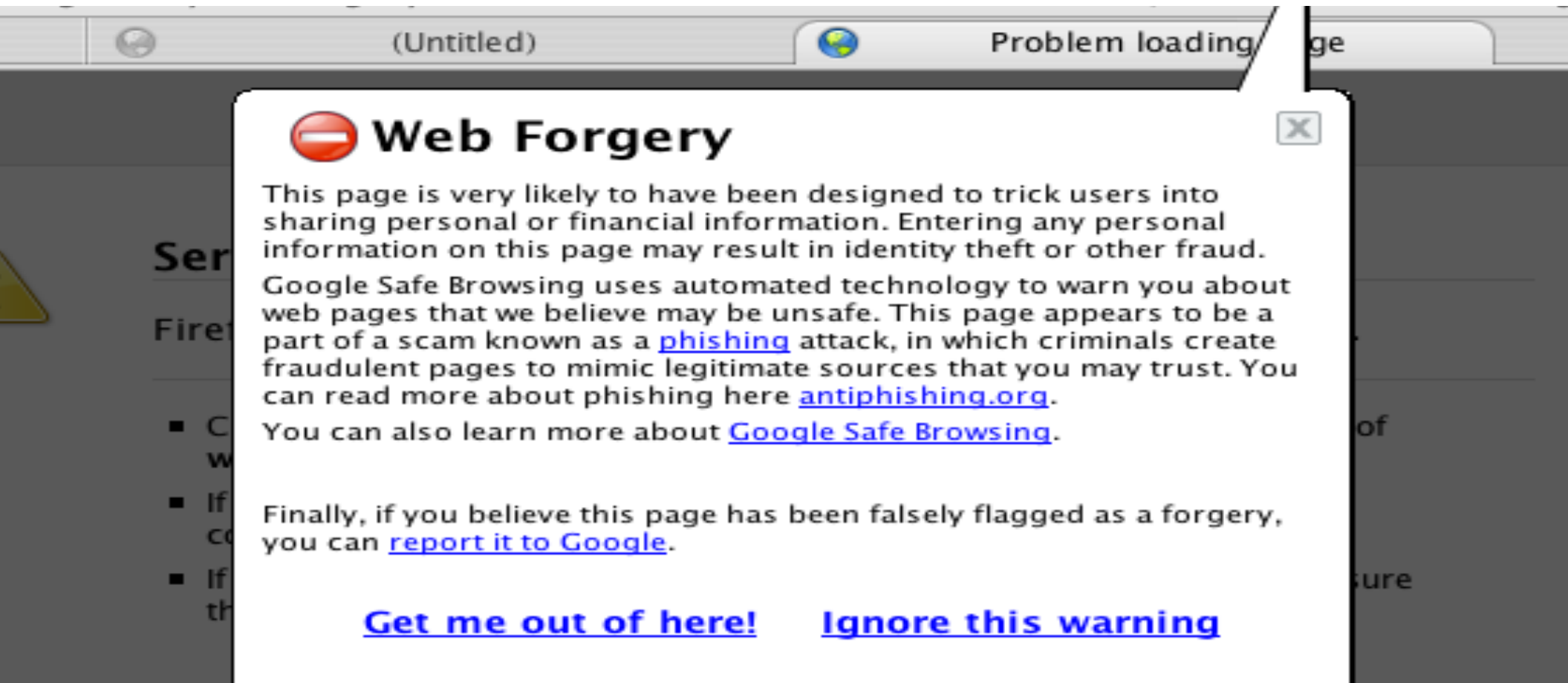
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#) 



Somehow there is still a problem

# Let Me Explain This To the User



The image shows a screenshot of a web browser window with a warning dialog box. The browser's address bar shows '(Untitled)' and 'Problem loading'. The dialog box has a red stop sign icon and the title 'Web Forgery'. The text inside the dialog box explains that the page is likely a phishing attack and provides links for more information and reporting.

**Web Forgery**

This page is very likely to have been designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Google Safe Browsing uses automated technology to warn you about web pages that we believe may be unsafe. This page appears to be a part of a scam known as a [phishing](#) attack, in which criminals create fraudulent pages to mimic legitimate sources that you may trust. You can read more about phishing here [antiphishing.org](#). You can also learn more about [Google Safe Browsing](#).

Finally, if you believe this page has been falsely flagged as a forgery, you can [report it to Google](#).

[Get me out of here!](#)      [Ignore this warning](#)

# Design for Humans Requires Designing for Humans

Smoking is a factor which contributes to lung cancer. Most cancers that start in lung, known as primary lung cancers, are carcinomas that derive from epithelial cells. Depending on the type of tumor, so-called paraneoplastic phenomena may initially attract attention to the disease. In lung cancer, these phenomena may include Lambert-Eaton myasthenic syndrome (muscle weakness due to auto-antibodies), hypercalcemia, or syndrome of inappropriate antidiuretic hormone (SIADH). Tumors in the top (apex) of the lung, known as Pancoast tumors, may invade the local part of the sympathetic nervous system, leading to changed sweating patterns and eye muscle problems (a combination known as Horner's syndrome) as well as muscle weakness in the hands due to invasion of the brachial plexus.



# Design for Humans Requires Designing for Humans





# Security is Risk

**Risk Perception and Communication Unplugged: Twenty Years of Process  
1995**

**Baruch Fischhoff**

# Goal of Risk Communication

## To change behavior

- All we have to do is show them that they've accepted/ rejected similar risks in the past
- All we have to do is show them that it's a good deal for them

## Create a partnership

- The right hat for the right context

# Individual Risk Decision

- A specific person making a potentially irrational risk decision
  - Using local client records of that individual
  - Using risk perspectives from other domains
  - Depending on their mental models for decision guidance
- Solve the problem of the homophilus individual as well as the problem of the heterogeneous network

# Learn From Other Domains

- Seat belts must be worn
- Communication must be **timely**



# Available

Free condoms vs. education

Solutions must be **available and usable.**



# Ambient acceptable Levels of Risk

Anti lock breaks increase risk-taking behavior,

**Respect their risk thermostat**



# Goals

How do you privacy risks in a way that communicates the risks and options?

- Risk Communication
- Ambient Risk Communication
- Action-based Risk Communication

# Specific User

Look for archetypes and categories

Appropriate mental models for appropriate risk communication

- Individual characteristics

- Expertise
- Demographics

- Risk perception

- Privacy perception
  - Internet users Privacy Information Concerns (IUPIC)
- Pratt-Arrow
- Balloon



# What Is This Phishing Thing?

Most popular: I don't know

Second most popular: related

- Spam, hacking

Third most popular

- Fraud, fake website, vishing

Fourth

- Privacy violations, tracking

# Certified What?

Most popular: I don't know

Second most popular: Significant over-confidence

- Jurisdiction, privacy policy, security competence of site

Third most popular

- Encryption-related

Fourth most popular

- Limited identification of site

- Not mentioned

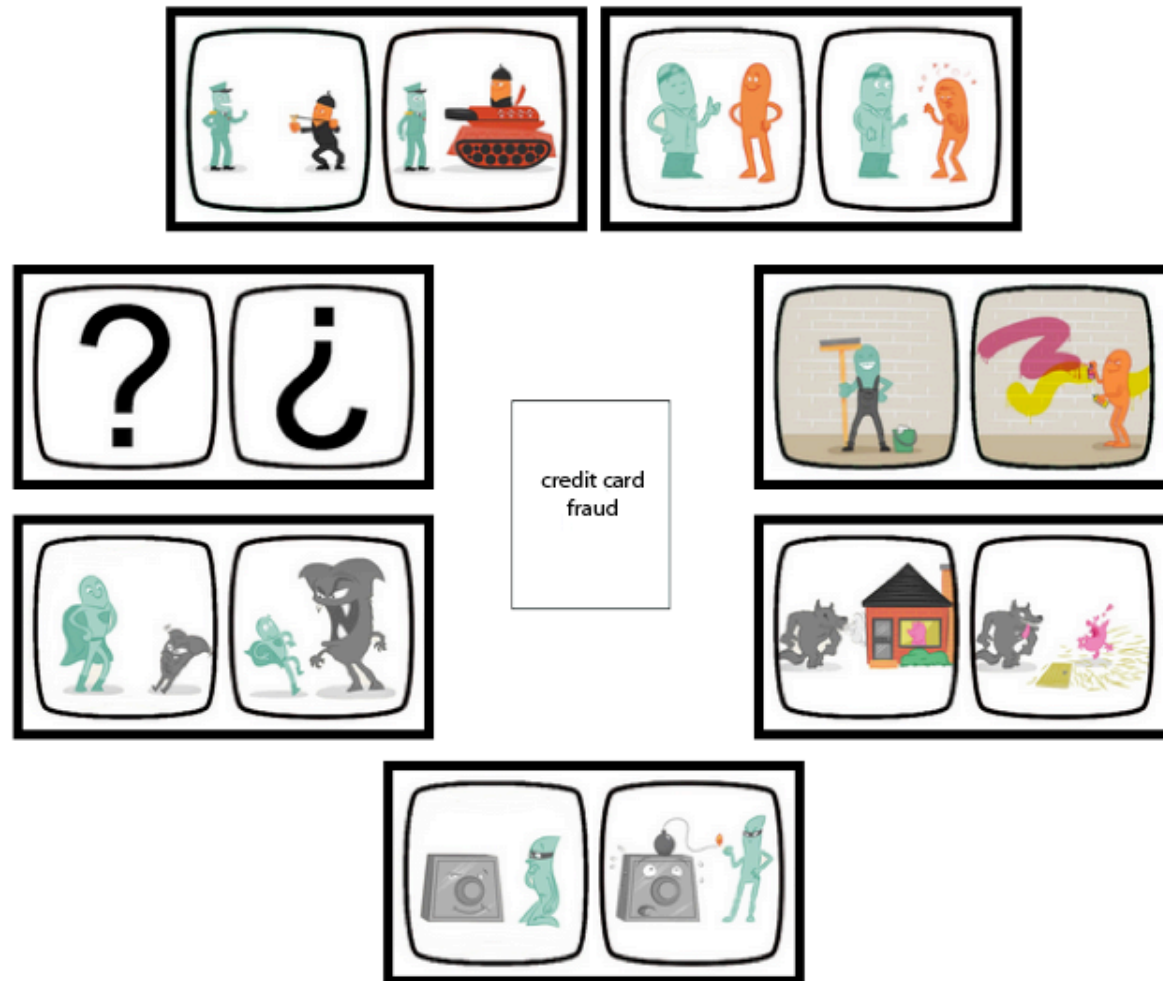
- Domain name or identity theft

We Need Better People



Not.

# Better Mental Models

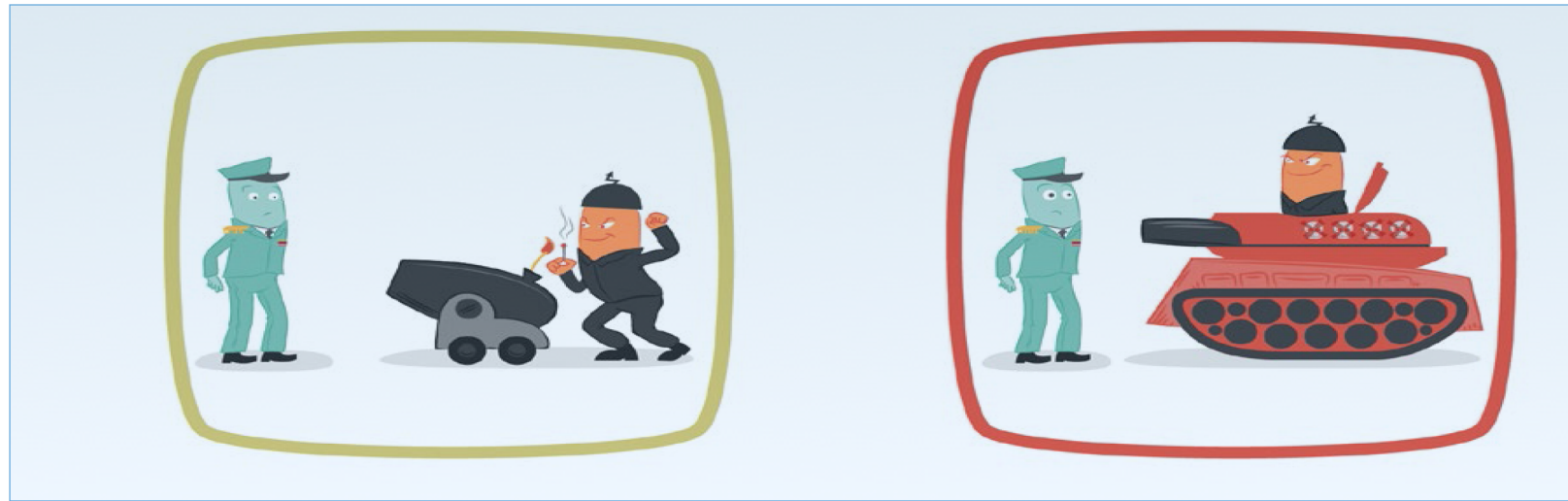


# Visual Risk Communication



Based on the concept of a risk thermostat

# Visual Risk Communication



- Disable unknown scripts
- Ad blocking (ads with scripting or from unknown sources)
- No tracking
- Cull trusted roots
- Browse privately
- Cookies only for a session
- Receive action-based warnings

# Visual Risk Communication



No ads  
No tracking  
Some sites will not work

Why is my widget not working? Why can't I read comments?  
This becomes a matter of transparency so the cost is visible

# Security as Spatial Boundaries

Theft, exfiltration,  
Web defacement

Locks, Key

Web addresses



Don't invite anyone in (download)



# Spatial Boundary Violation as a Risk

- Voluntary (exposure can be managed)
- Immediate (harm delay)
- Understood by experts
- Controllable (mitigation Not new)
- Not dreadful
- Individuals
- May be severe
- after exposure)



# Personal Safety in Security Literature

Zombie  
Slave  
Attacks



Avoid bad sites, stay safe places

# Security As Personal Safety

Not voluntary

Not immediate (harm delay)

Not understood by experts

Not controllable

Not awareness

Not dreadful (ubiquitous)

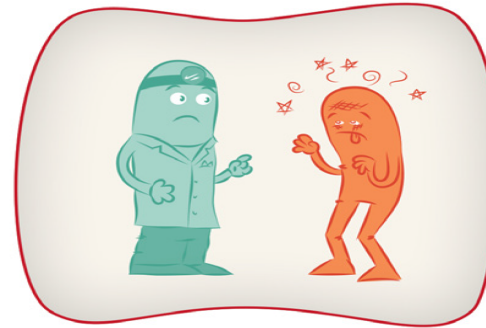
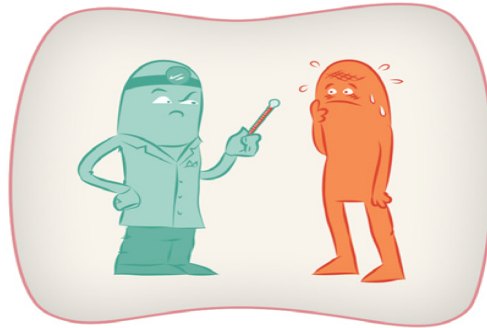
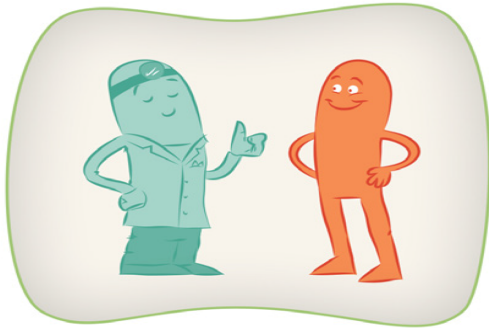
Not individual

May be severe



# Medical or Health in Security Literature

Viruses, bugs, worms  
Infectious code  
Computer hygiene



Computer hygiene

# Medical or Health Risks

Voluntary (exposure can be managed)

Not Immediate (harm delay)

Understood by experts

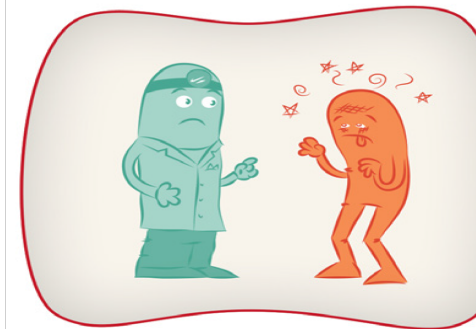
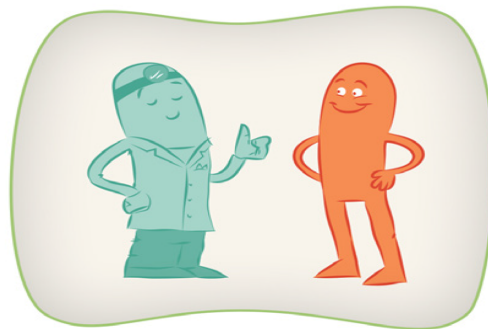
Understood by exposed

Not Controllable (mitigation Not new)

Not dreadful, not new

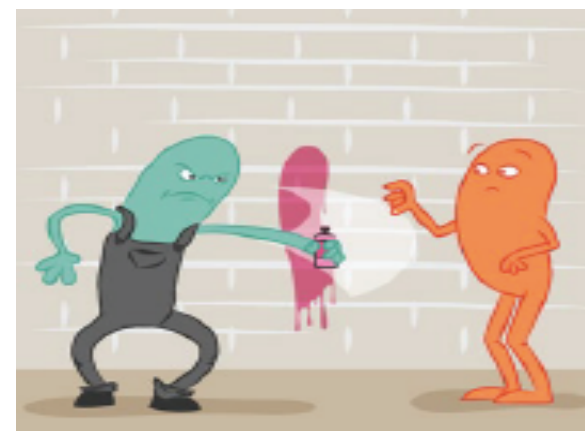
Individuals

May be severe



# Discreants in Security Literature

Vandals  
Hackers  
Defacement



Annoyance, clean up when something happens

# Discreants as a Risk

Not voluntary

Immediate (harm delay)

Understood by experts

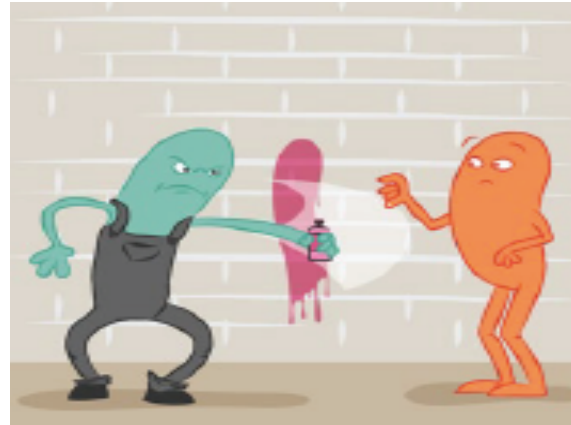
Understood by exposed

Not controllable

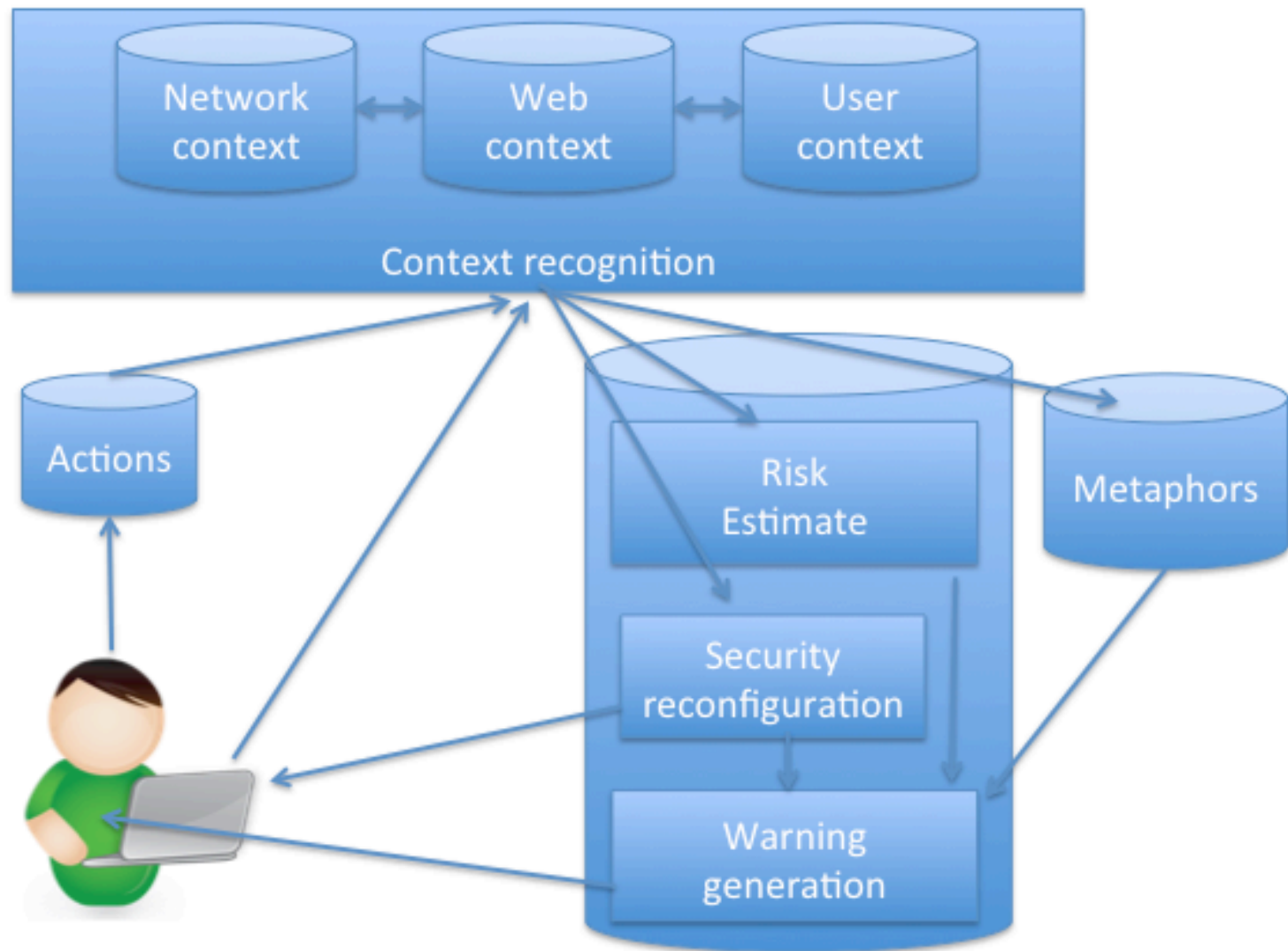
Not dreadful (ubiquitous)

Individual

Not severe

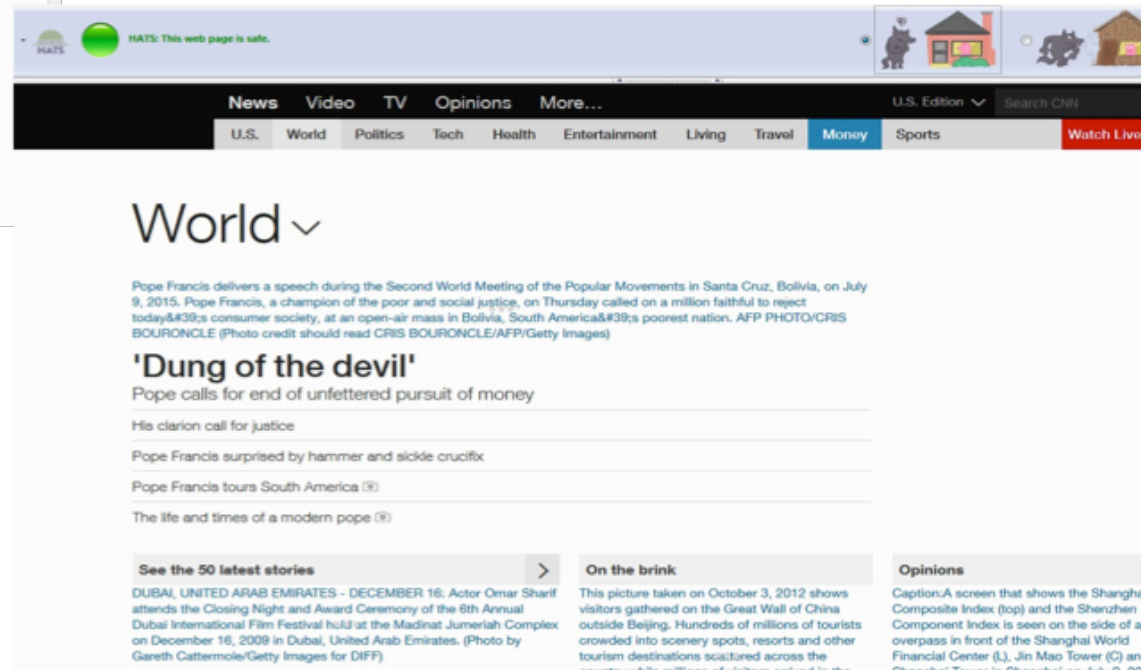
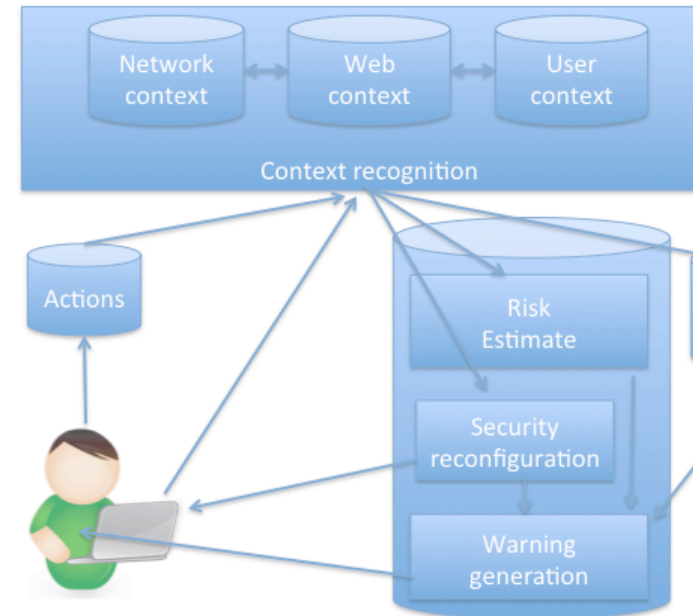
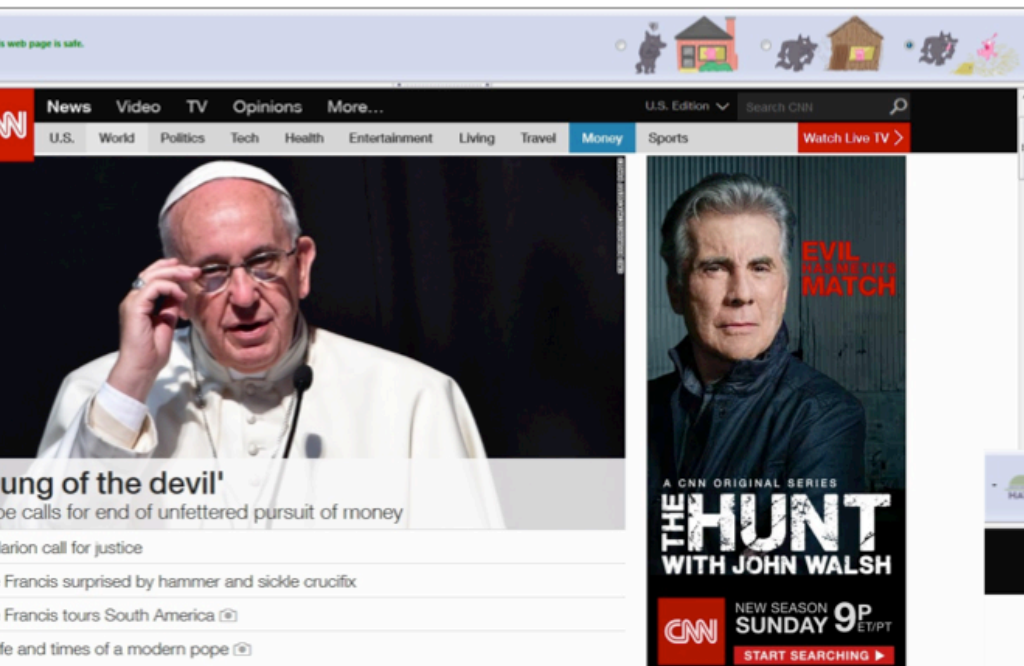


# Instrumented as an Extension

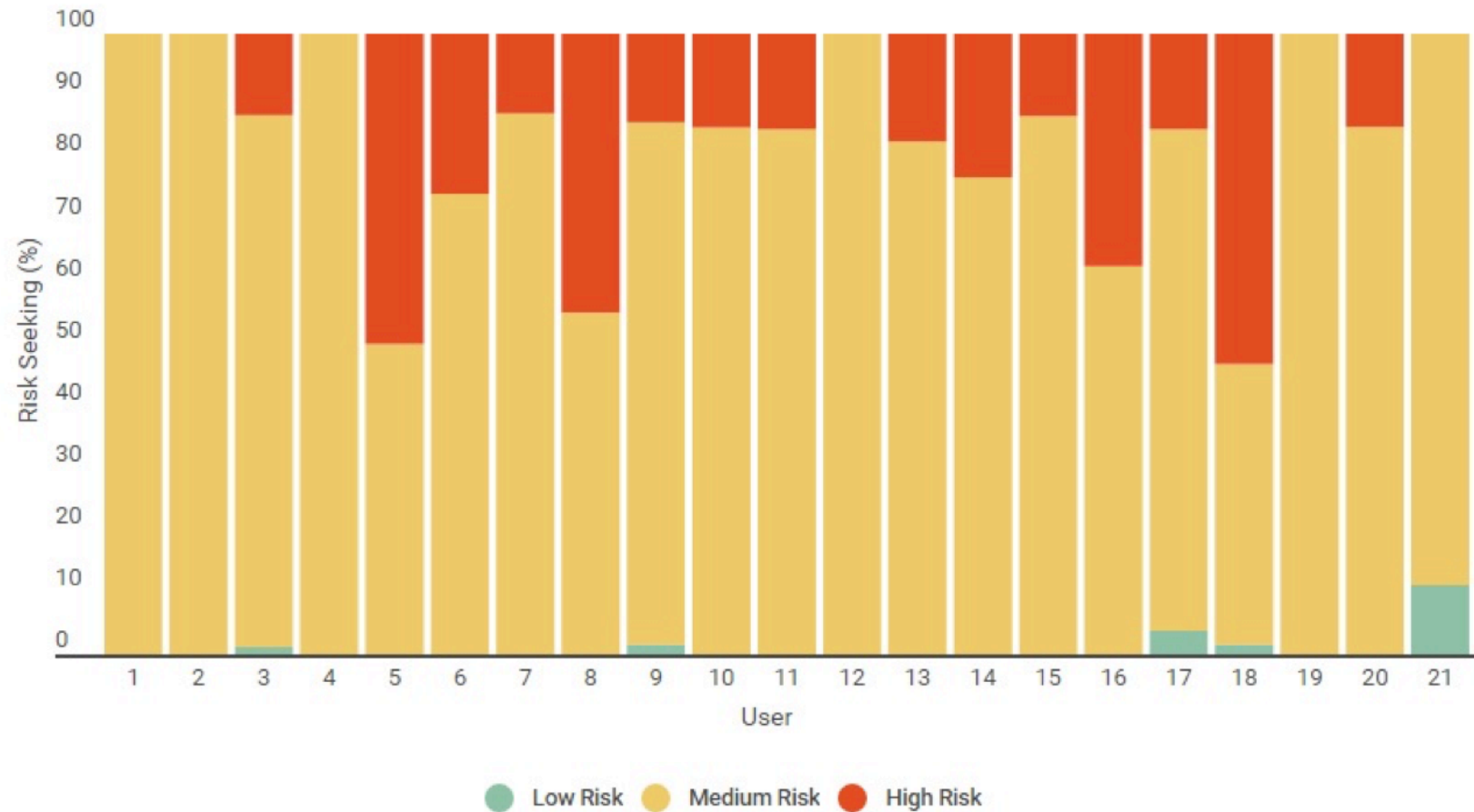




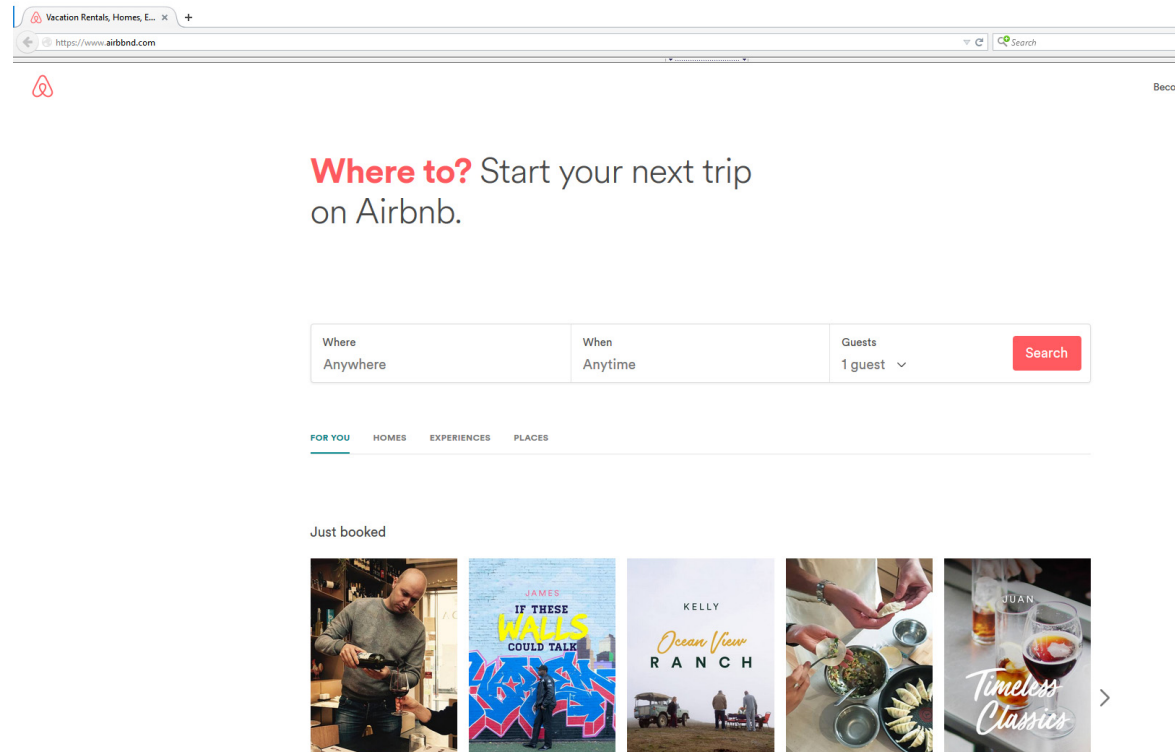
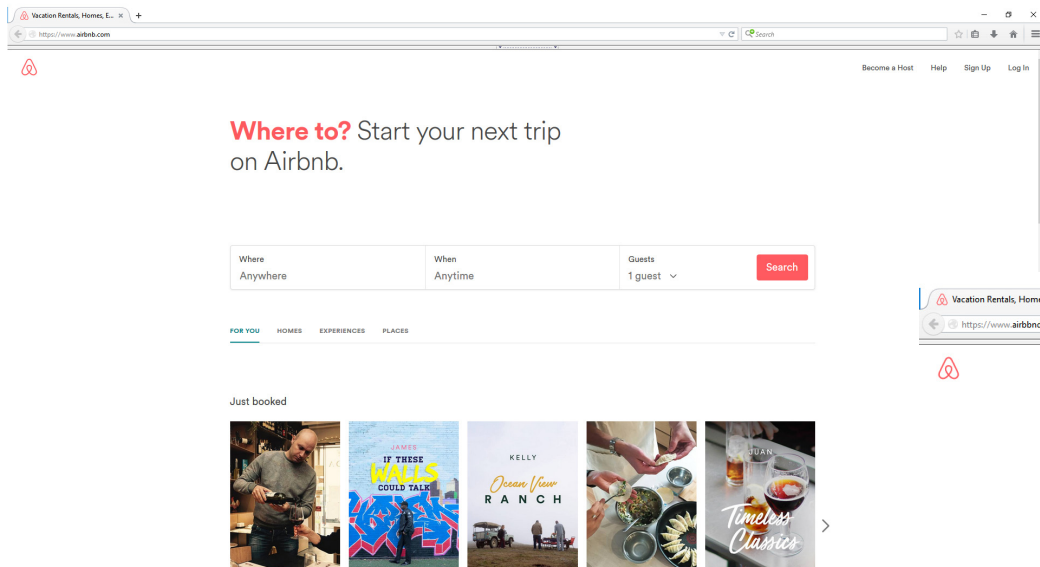
# iewed as a Toolbar



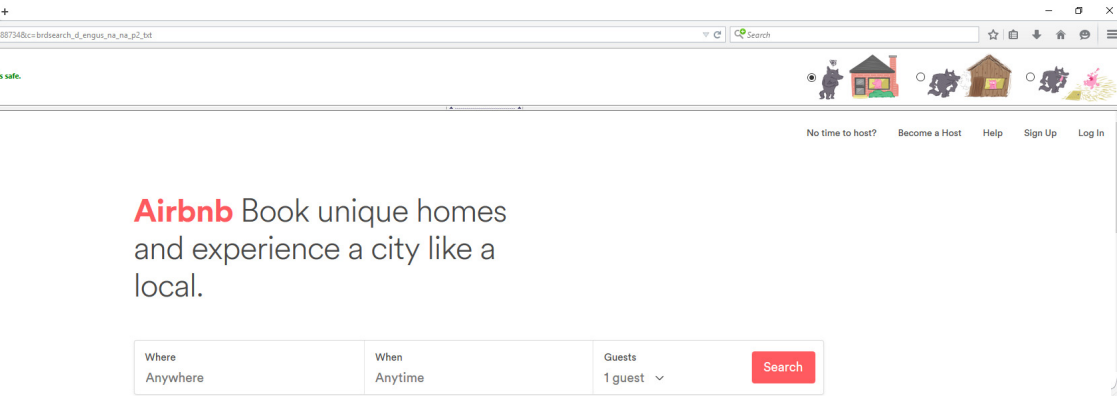
# Changed Behaviour



# Control Legitimate & Not Spoofed



# Low Risk: Legitimate and Phished



## Experiences

See all >



Where to? Start your next trip on Airbnb.

Where Anywhere	When Anytime	Guests 1 guest	Search
-------------------	-----------------	-------------------	--------

FOR YOU HOMES EXPERIENCES PLACES

# Goals

How do you describe privacy risks in a way that communicates the risks and options?

- Risk Communication
- Ambient Risk Communication
- Action-based Risk Communication
  - Creating a password
  - Downloading an app

# Information Asymmetry

Developers

Consumers

# Security as a Gain: Prospect Theory

Certain gains are preferred over probability of loss

People make decision based on gains and losses of the choice and not based on the final outcome

Right now, all people see is gain

# To Understand

Security as gain

Permissions as gain

Permissions as losses





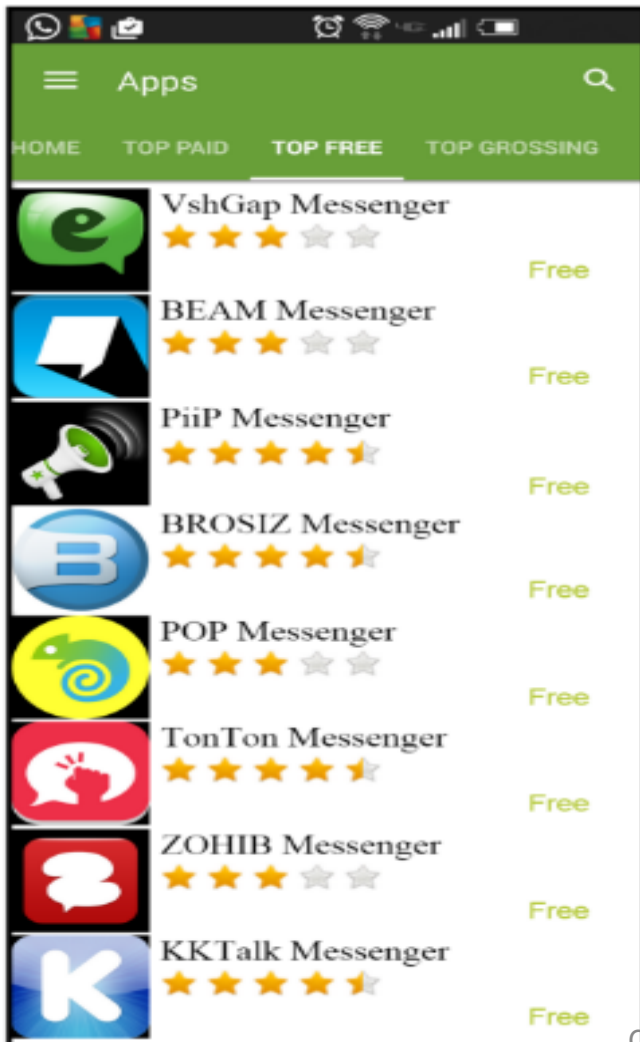
# Human Decision-Making

Developers of apps

Marketplaces

Buyers of apps

# Android Risks & Benefits



Android 5.0 Control

# What is a Over Privileged?

Only costs  
No benefits  
No data use



# Permission Types

## Normal

- Defined as being harmless

## Dangerous

- Spending money

## Signature/Systems

- Only to apps signed with device manufacturers permission

# Permissions Demystified

Android permissions inadequate to map to functionality for developers

Over privileging

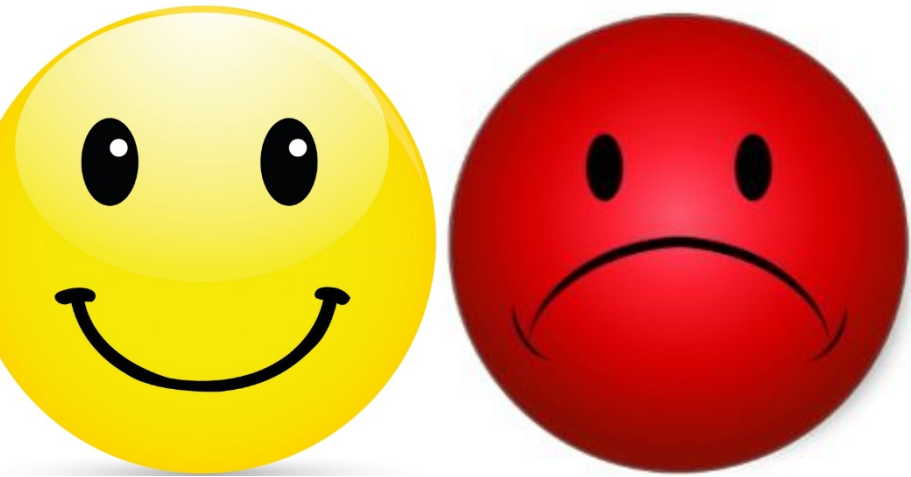
- Over one third are over-privileged

# Visual Cues: Risks and Benefits

At actual decision point

- Not after download decision

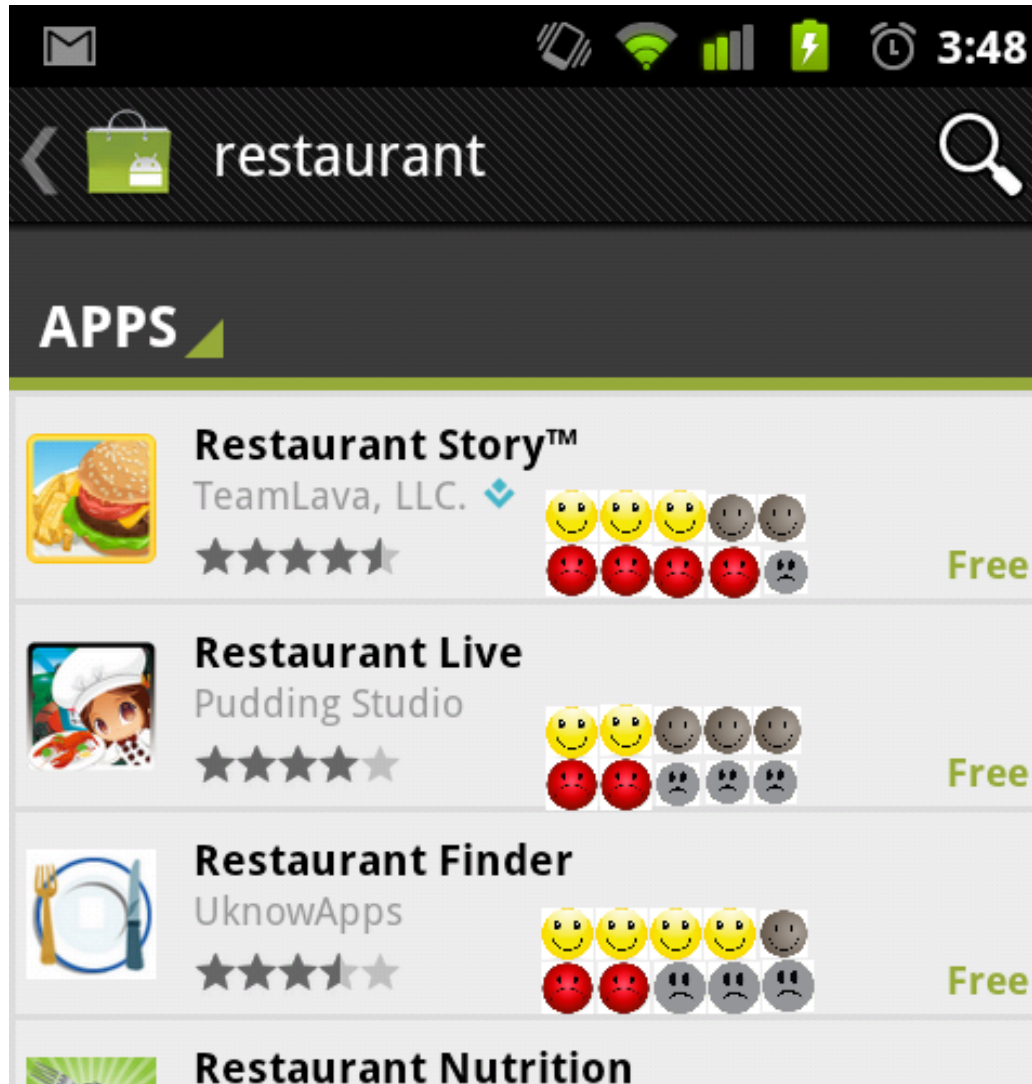
**Smiley Vs Frown**



**Healthy Vs Unhealthy**

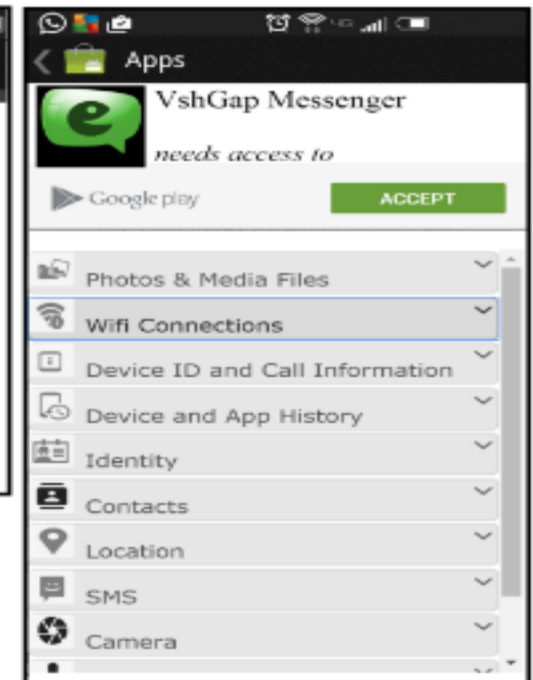
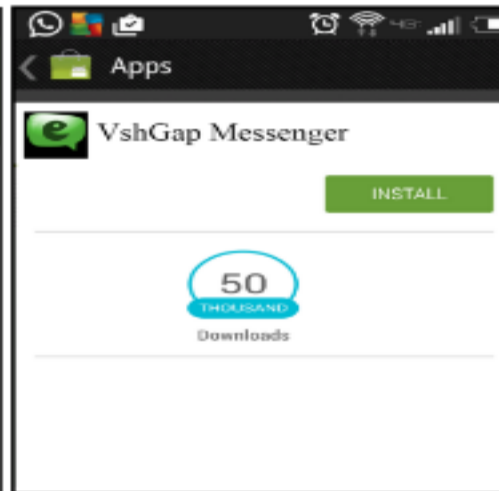
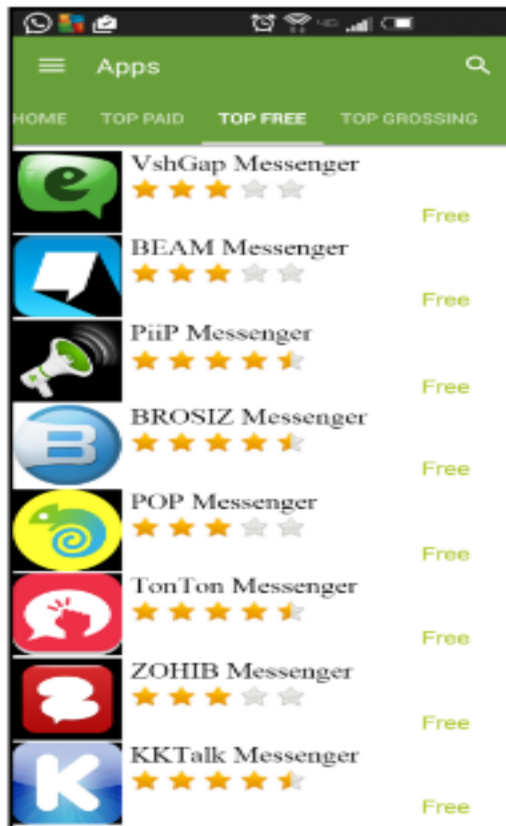


# Android Risks & Benefits



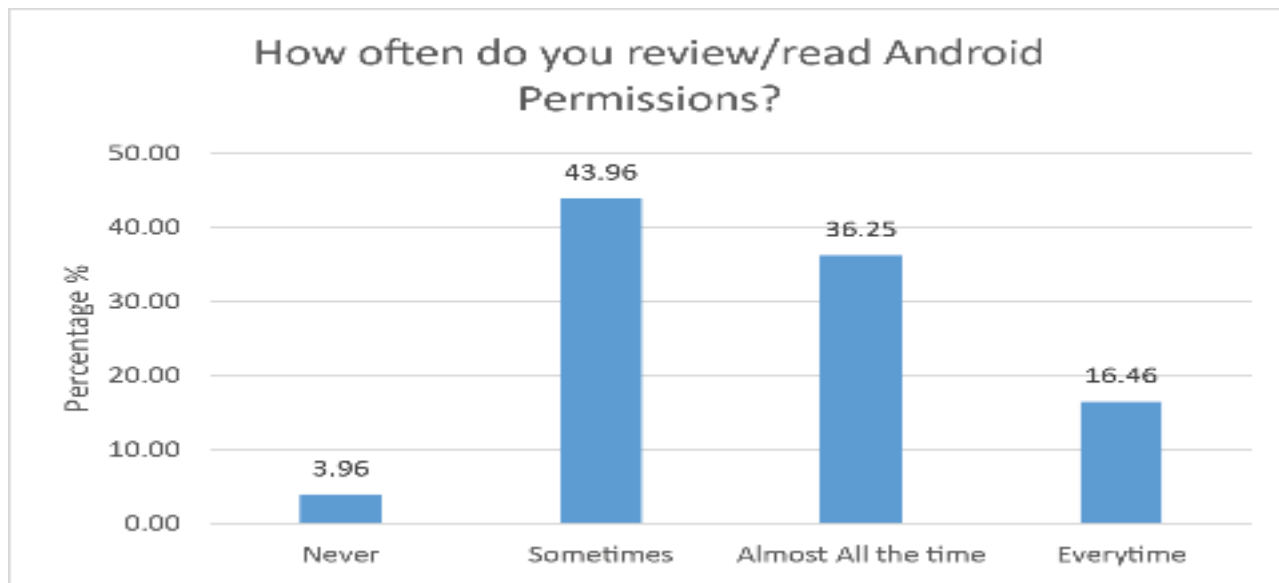
Also locks, stars, a eyeballs

MTurk

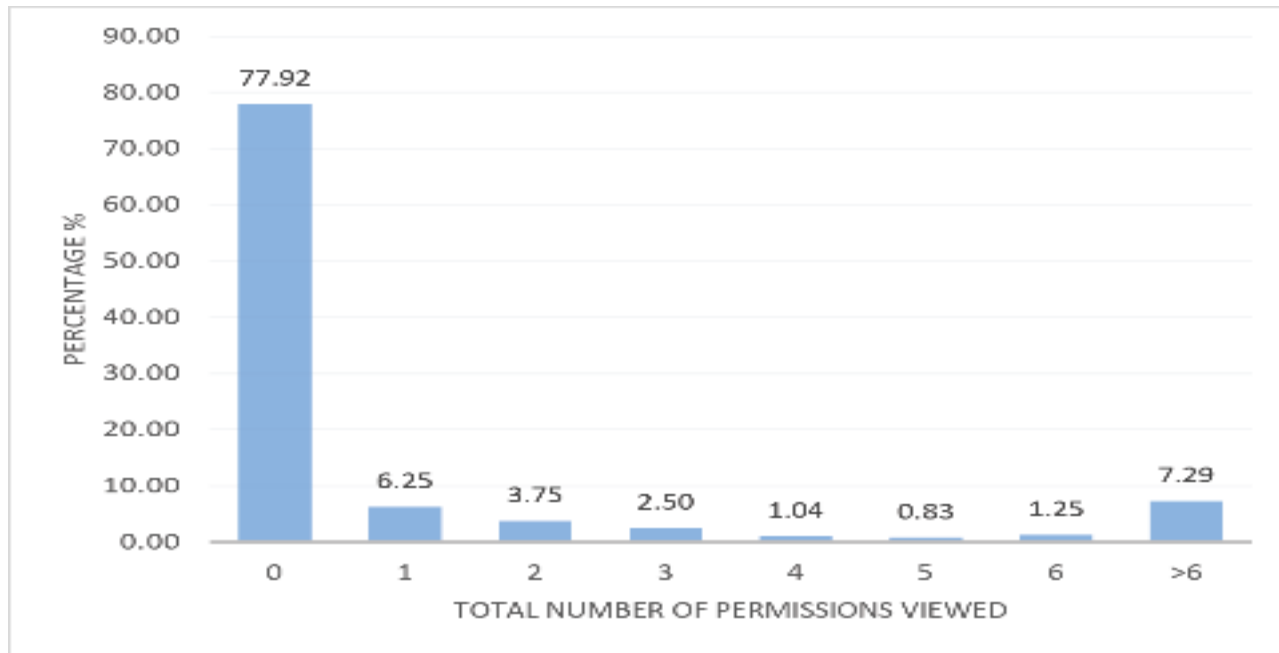




# Expressed Preferences

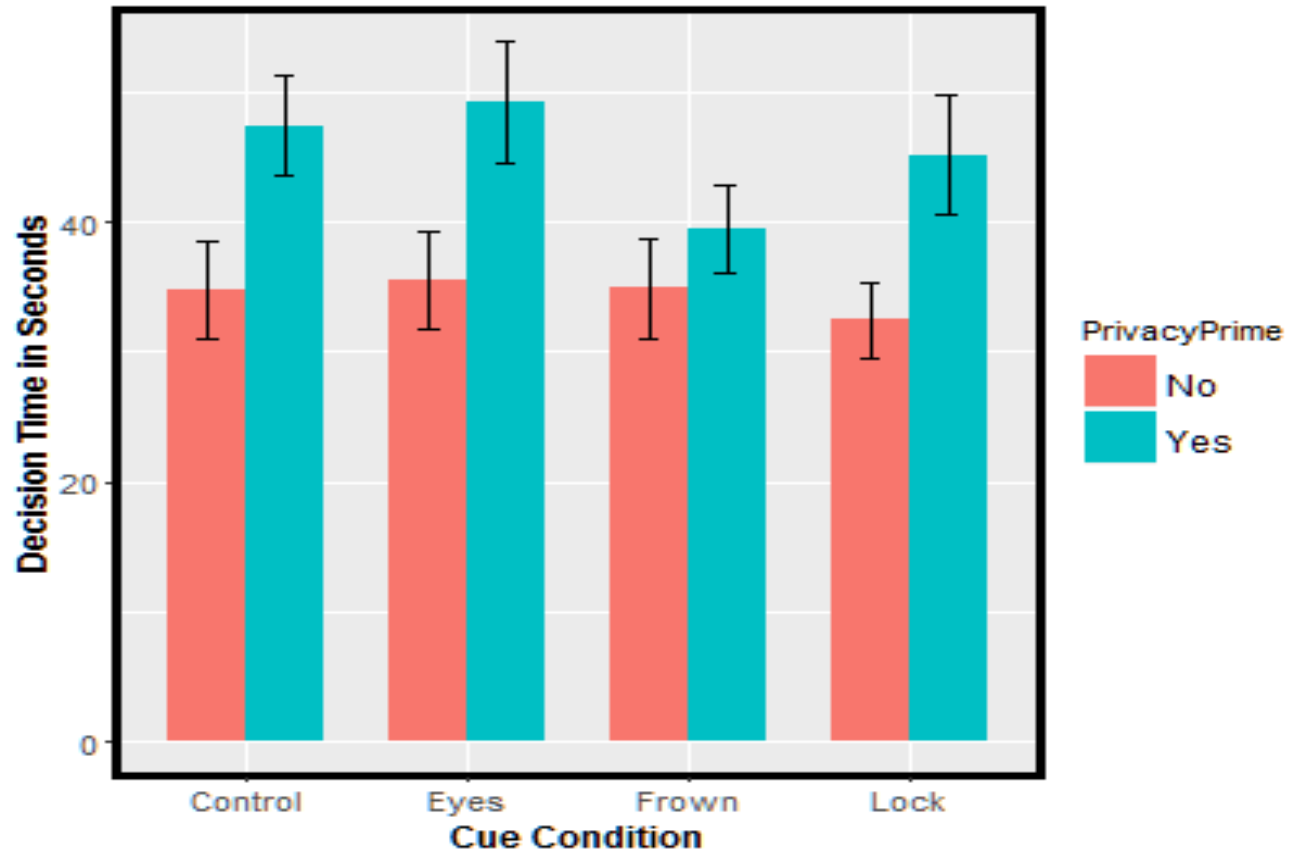


# Revealed Preferences

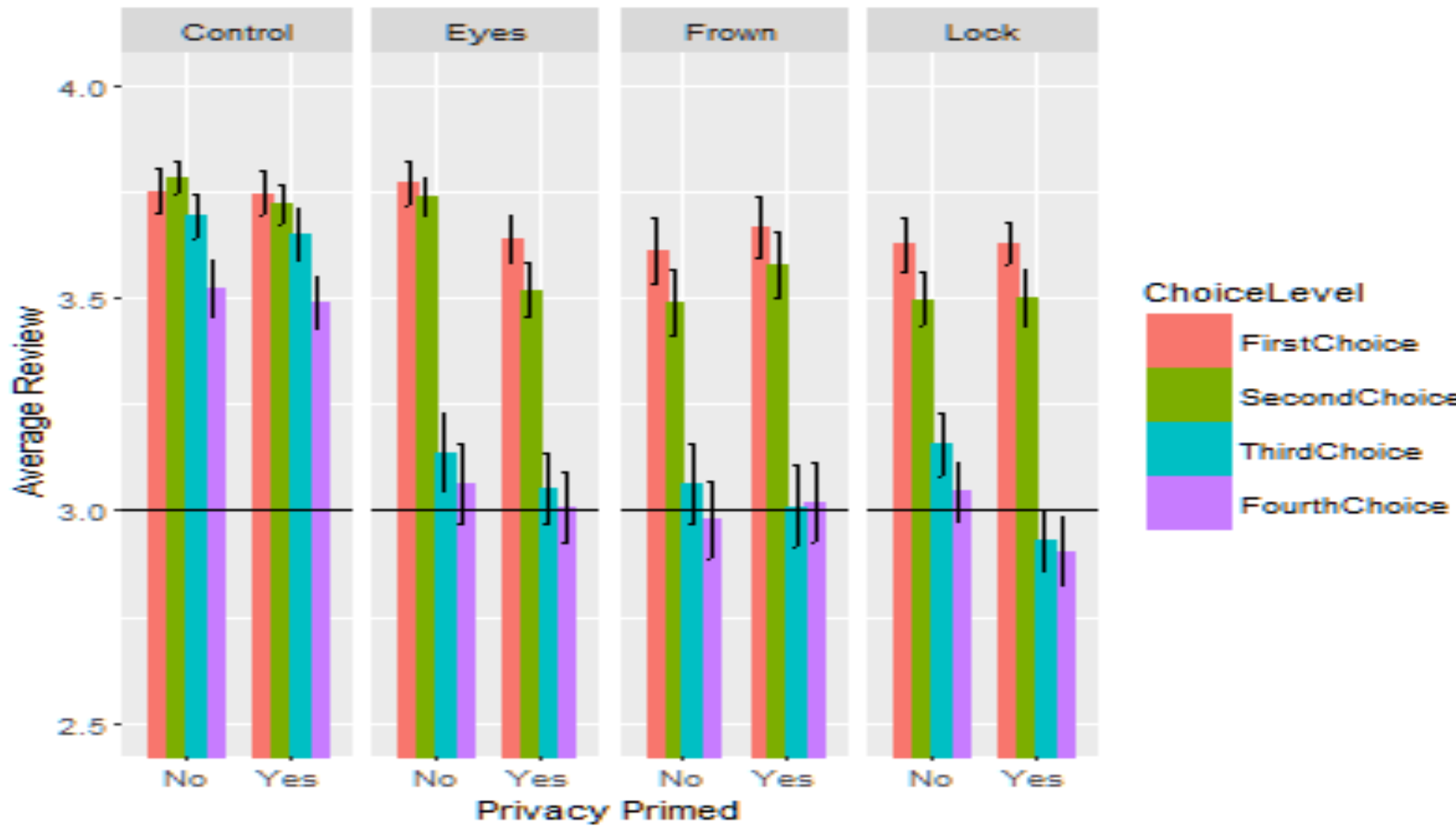


# Decision Time

Regulatory Friction

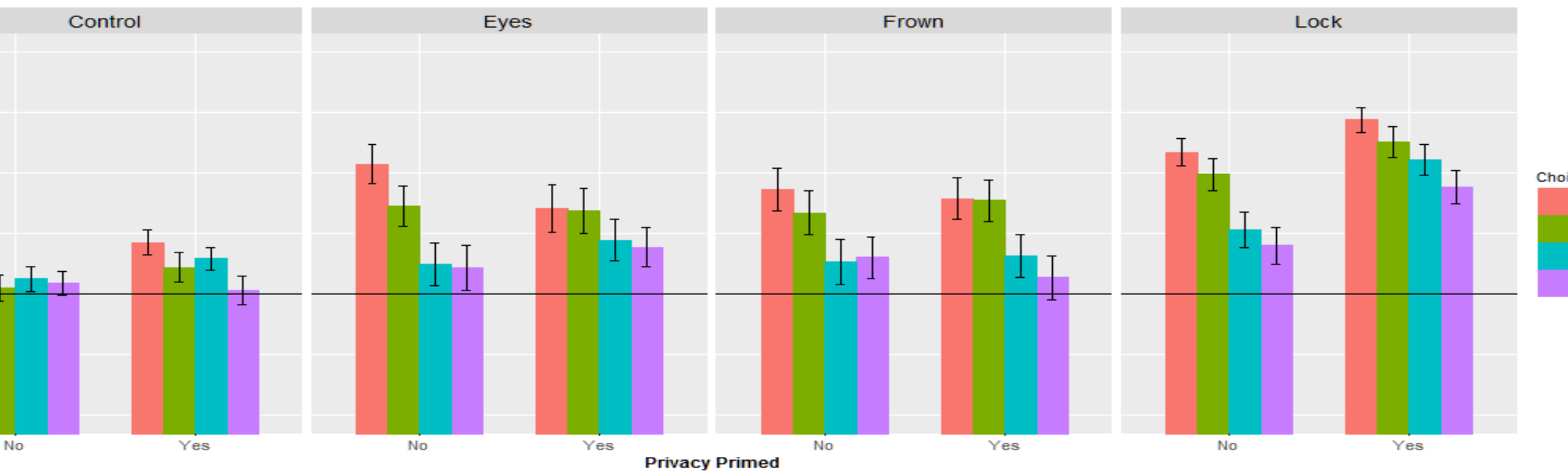


# Results: Primed and Not Primed



# Mean Privacy Rating

Higher is More Privacy



# The Cue Matters

## Eyes & Emoticons

- First and second choices there is evidence
  - More eyes was worse
    - Not intuitive
  - More frowns is worse

## Locks

- More consistent effect
- Stronger effect of priming on first and second
- In the same order as benefits
  - More locks is better

# mplications

Communicate all costs of applications to users in intuitive manner

In a way that respects cognitive misers

Improve comprehension of permissions

Towards a functioning market

The kind of cue matters



# Simple Locks

The screenshot shows the Google Play Store page for the app 'System app remover (ROOT)' by JUMOBILE. The app is available for free and has an 'INSTALL' button. Below the main app card are three smaller screenshots showing the app's interface: a menu with options like 'System app', 'User app', and 'Recycle bin'; a list of system apps with checkboxes for removal; and a 'Recycle bin' view. The app has a rating of 4.5 stars from 61,712 reviews and over 1,000,000 downloads. It was last updated on September 10, 2014, and is 1.76MB in size. A 'Description' section at the bottom explains the app's features, including system app removal, user app uninstallation, moving apps to the SD card, and rooting help.

**System app remover (ROOT)**  
JUMOBILE

★★★★★ 61,712  
1,000,000+ downloads  
Sep 10, 2014  
1.76MB

5.9K people +1'd this.

*Description*

We provide not only system app remover, but also user app uninstaller, move app to sdcard, move app to phone, apk on sdcard scan/install/delete, rooting guide help.

The screenshot shows the Google Play Store page for the app 'Brightest Flashlight Free' by GOLDENSHORES TECHNOLOGIES, LLC. The app is available for free and has a 'PERMISSIONS' button. Below the main app card are five smaller screenshots showing the flashlight app in various states: a hand holding the phone, the flashlight turned on, the screen at maximum brightness, the keyboard backlight on, and the notification LED on. The app has a rating of 4.5 stars from 132,407 reviews and over 250,000 downloads. A 'DESCRIPTION' section at the bottom lists the app's features and configurations.

**Brightest Flashlight Free**®  
GOLDENSHORES TECHNOLOGIES, LLC

★★★★★ 1324073  
>250,000 Downloads

PERMISSIONS

**DESCRIPTION**

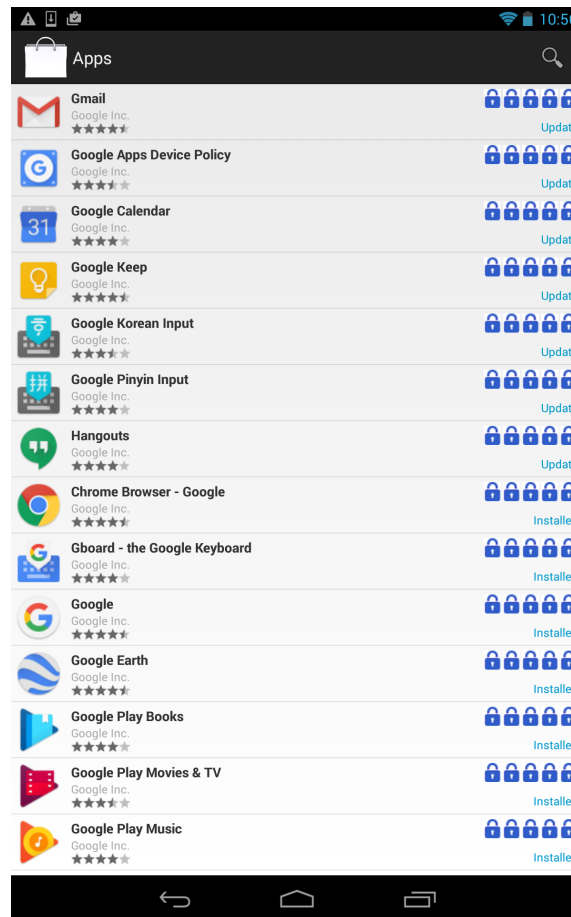
Brightest Flashlight App – Free of Charge

- \* Turns on all available lights on the device
- \* Camera Flash LED at Maximum
- \* Screen at Bright Maximum
- \* Keyboard Backlight at Maximum
- \* Soft Keys Backlight at Maximum
- \* Notification LED at Maximum
- \* Automatic Timer Exits Application after 2 Minutes
- \* Audio Effects on Start and Stop
- \* Unobtrusive Ads
- \* Please contact the support email for reporting bugs or problems so we can fix quickly as possible
- \* Best Flashlight App for dark conditions, natural LED color provides great contrast

Recently Tested Flashlight Configurations:  
Motorola DroidX Flashlight  
Samsung Galaxy S Flashlight  
Motorola Droid2 Flashlight  
Samsung Fascinate Flashlight  
Samsung Epic 4G Flashlight  
Motorola Droid Flashlight  
Motorola Defy Flashlight  
T-Mobile G2 Flashlight  
LG Optimus Flashlight  
LG Ally Flashlight  
Samsung Galaxy Note Flashlight



# Tested in Fake Store on Phones, Real Apps

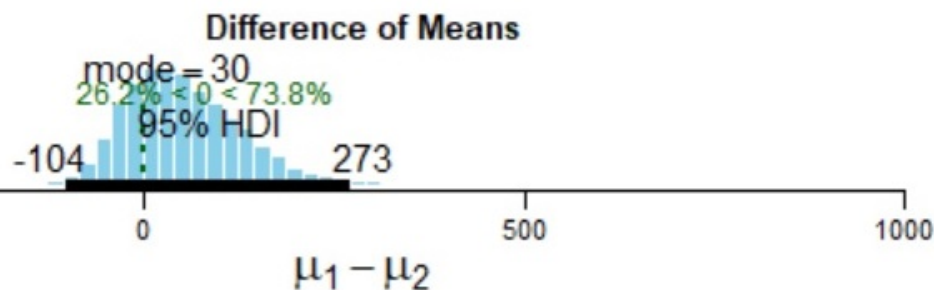


# Same Privacy, Same Function, Same Behavior

Same privacy

Equivalent distribution

Same behavior

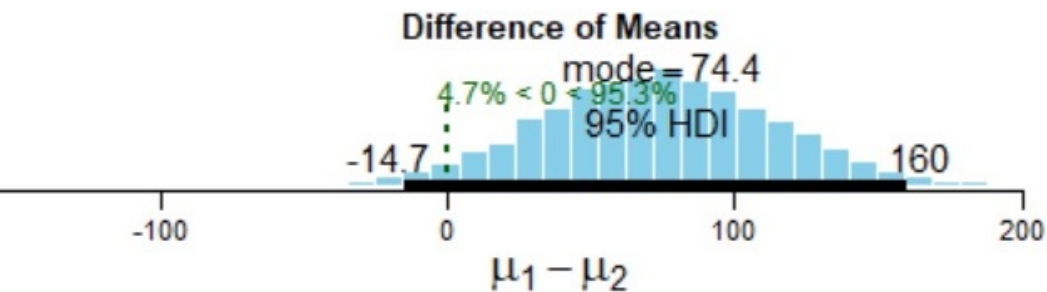


Play Store Rank and App Name	Downloads
1. Super-Bright LED Flashlight	38
3. Color Flashlight	34
2. Tiny Flashlight + LED	26
4. Brightest Flashlight Free	20
10. Flashlight Galaxy S7	16
9. Flashlight Galaxy	16
5. Brightest LED Flashlight	15
11. Flashlight	12
6. High-powered Flashlight	11
12. Flashlight Widget	7
7. FlashLight	6
13. Flashlight for HTC	5
8. Flashlight	3

# Same Functionality, Different Privacy

different behavior

different distribution

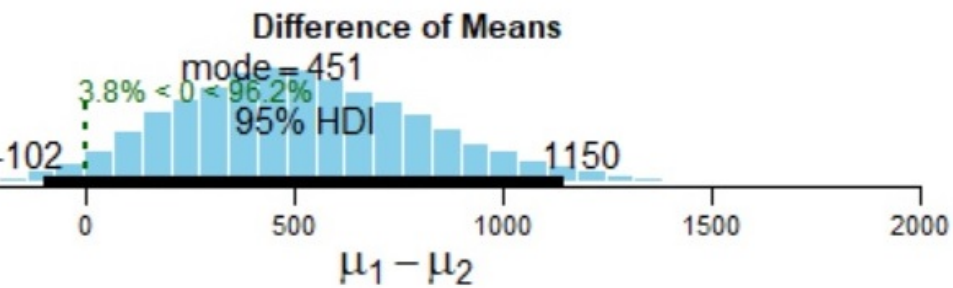


Play Store Rank and App Name	Downloads	Locks
1. Weather - The Weather Channel	40	4
2. AccuWeather	31	5
5. Yahoo Weather	27	5
10. MyRadar Weather Radar	27	5
11. Weather Underground	19	5
6. Weather by WeatherBug	16	3
4. Weather & Clock Widget Android	14	4
6. Transparent clock & weather	11	3
12. NOAA Weather Unofficial	7	4
15. Weather Project	5	1
8. Weather, Widget Forecast Radar	3	4
14. Weather Project	2	1
13. iWeather-The Weather Today HD	2	1
3. Go Weather Forecast & Widgets	5	4
9. Weather	1	4

# Different Functional, Different Privacy

Different privacy

Different distribution



Play Store Rank and App Name	Downloads	Lo
1. Google Photos	39	5
8. PhotoDirector Photo Editor App	25	5
5. Photo Lab Picture Editor FX	24	5
9. Gallery	23	5
4. Photo Editor Pro	20	5
11. A+ Gallery Photos & Videos	19	5
5. Photo Collage Editor	17	5
3. PhotoGrid & Photo Collage	15	5
10. Toolwiz Photos - Pro Editor	13	5
6. Photo Editor Collage Maker Pro	9	5
2. PicsArt Photo Studio & Collage	3	3
7. Phonto - Text on Photos	1	5

# Very Different Functional, Privacy

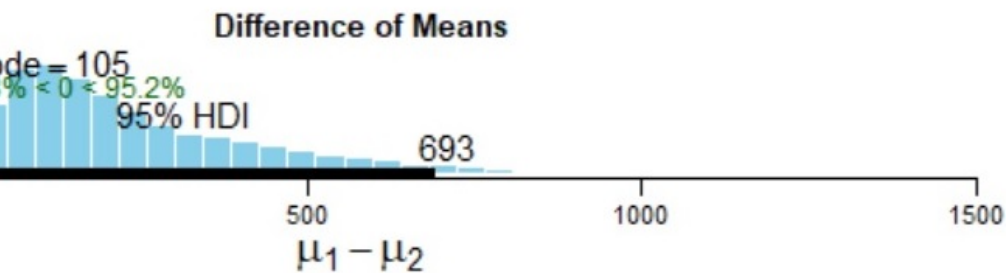
different privacy

different distribution

less difference than with

• Weather

• Photos



Play Store Rank and App Name	Downloads	Loc
2. Fruit Ninja Free	39	5
1. Subway Surfers	23	5
8. Super Smash Jungle World	22	5
5. PAC-MAN	20	5
13. Wheel of Fortune Free Play	16	5
7. Color Switch	15	5
4. Piano Tiles 2™	15	5
3. slither.io	12	5
6. Rolling Sky	11	5
9. Block! Hexa Puzzle	4	5
10. Flip Diving	3	1
16. Battleships - Fleet Battle	2	5
11. Snakes & Ladders King	2	5
13. Board Games	1	5
14. Best Board Games	1	5
12. Checkers	1	5
15. Mancala	1	3

# Closing

Use appropriate mental models

- Systems designed for the people using them
- Not only the people building them

Risk communication

Changes risk behavior

Changes network security

Questions?

