Towards Usable Web Privacy and Security

Lorrie Faith Cranor

November 2005

http://lorrie.cranor.org/

CMU Usable Privacy and Security Laboratory

Carnegie Mellon

Unusable security & privacy

- Unpatched Windows machines compromised in minutes
- Phishing web sites increasing by 28% each month
- Most PCs infected with spyware (avg. = 25)
- Users have more passwords than they can remember and practice poor password security
- Enterprises store confidential information on laptops and mobile devices that are frequently lost or stolen

Grand Challenge

"Give end-users
security controls they can understand
and privacy they can control for
the dynamic, pervasive computing
environments of the future."

- Computing Research Association 2003

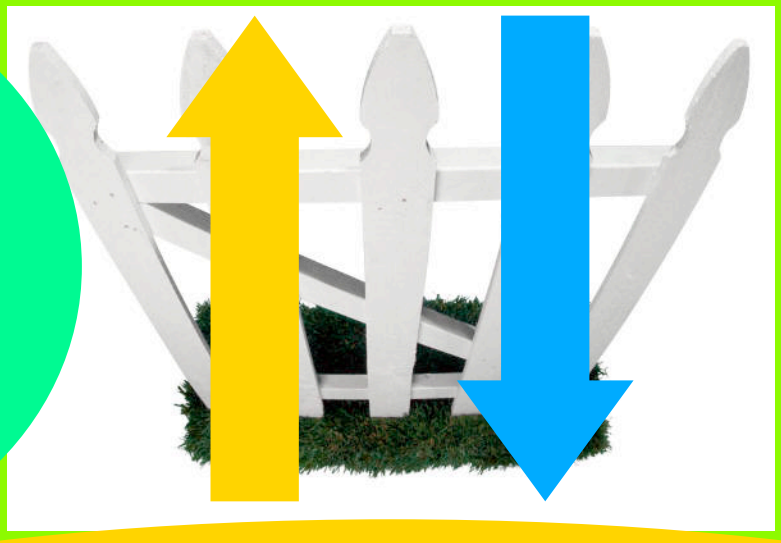
security controls they can understand

privacy they can control

Just work

security/privacy researchers and system developers

Web standards authors and user agent developers

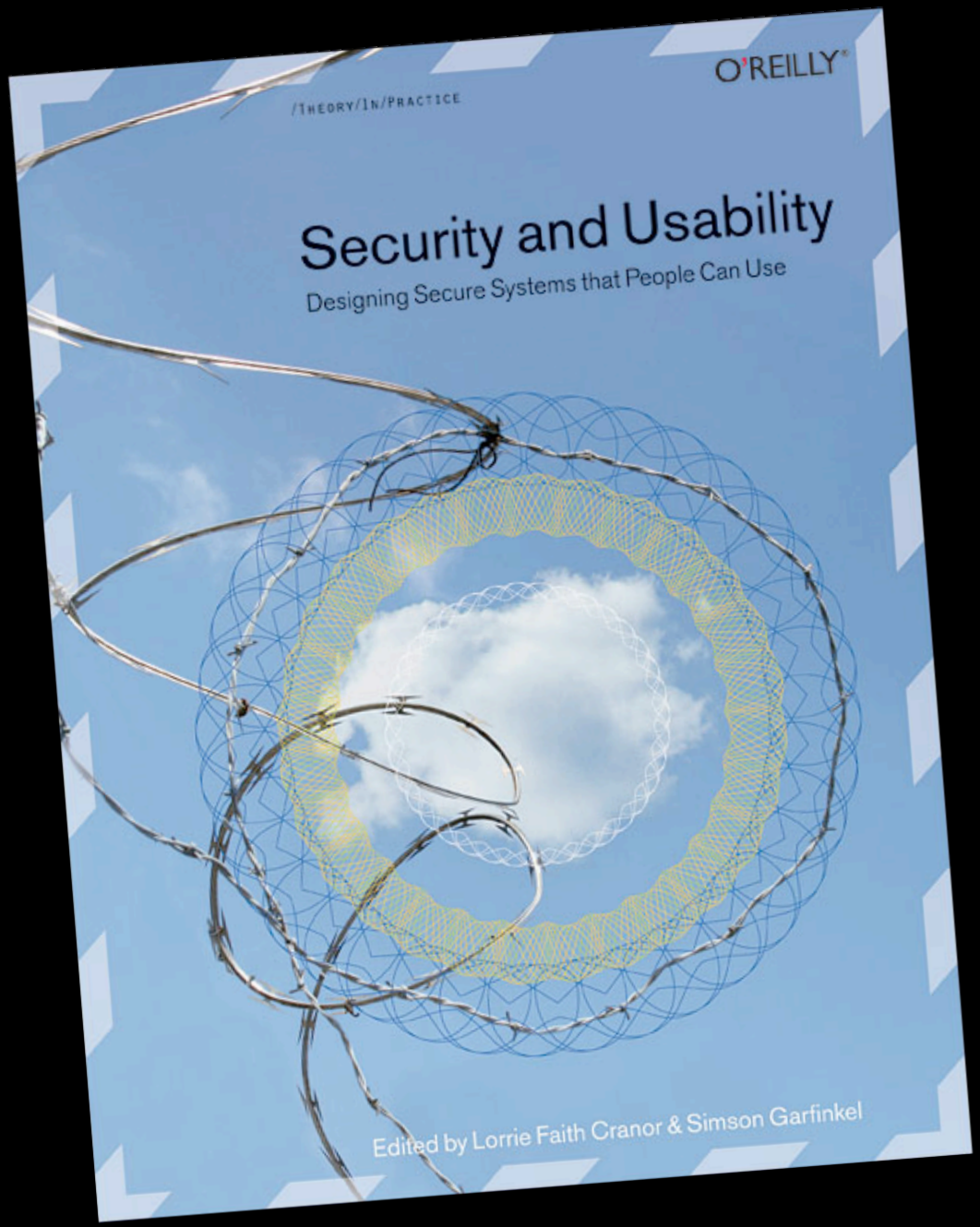


human computer interaction researchers and usability professionals

Mark your calendar for SOUPS 2006 - July 14-16 at CMU

Symposium On Usable Privacy and Security (SOUPS)

July 6-8, 2005
Pittsburgh, PA USA
http://cups.cs.cmu.edu/soups/


O'REILLY
/Theory/In/Practice
Security and Usability
Designing Secure Systems that People Can Use
Edited by Lorrie Faith Cranor & Simson Garfinkel

Agenda

1. Problems and approaches
2. Passwords
3. Symbols & metaphors
4. Rethinking cookies
5. Making Web privacy visible

Problems and approaches

1.

How do you stay safe online?

Advice


TOP TEN CYBER SECURITY TIPS
FOR TEENS, THEIR TEACHERS AND FAMILIES
Be a responsible cyber citizen.
Use anti-virus software.
Do not open email from unknown sources.
Use hard-to-guess passwords and keep them private.
Protect computers with firewalls.
Do not share access to your computers with strangers. Learn about file sharing risks.
Disconnect from the Internet when not in use.
Back-up your computer regularly.
Regularly download security protection update "patches".
Help your family to check computer security on a regular basis.
US-CERT Cyber Security Tip ST04-003 -- Good Security Habits
http://www.us-cert.gov/cas/tips/ST04-003.html
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
Search US-CERT
> Advanced Search
National Cyber Alert System
Archive
GetNetWise
You're One Click Away...
Spotlight on Spyware
Kids' Safety
Spam
Security
Keeping Children Safe Online
Stopping Unwanted E-mail and Spam
Protecting Your Computer From Hackers and Viruses
Keeping Your Personal Info Private
10 Tips:
Online Dating Safety
OnlineDatingService.net

Experts recommend...


PAL Spyware
Spy Sweeper
2004
Spyware Eliminator
Anonymous Surfing
Privacy Protection That Defends Your Confidential Information
COOKIES
POP!
SPAM
Hormel
Norton AntiVirus 2004
symantec.
OEM VERSION
Net Nanny 5.0
Net Nanny
Encryption for Everyone
PGP
Pretty Good Privacy
HARDENED
PGP
Simson Garfinkel
O'Reilly & Associates, Inc.

After installing all that security and privacy software

Do you have any time left to get any work done?

Secondary tasks

Approaches to usable security

- Make it "just work"
  - Invisible security
- Make security/privacy understandable
  - Make it visible
  - Make it intuitive
  - Use metaphors that users can relate to
- Train the user


DO NOT
PICK
UP
VIRUSES

Firefox security assumptions

1. Users want to believe that their products are keeping them secure.
2. Users do not want to be responsible for, nor concern themselves with, their own security.
3. We know more about security than our users do.

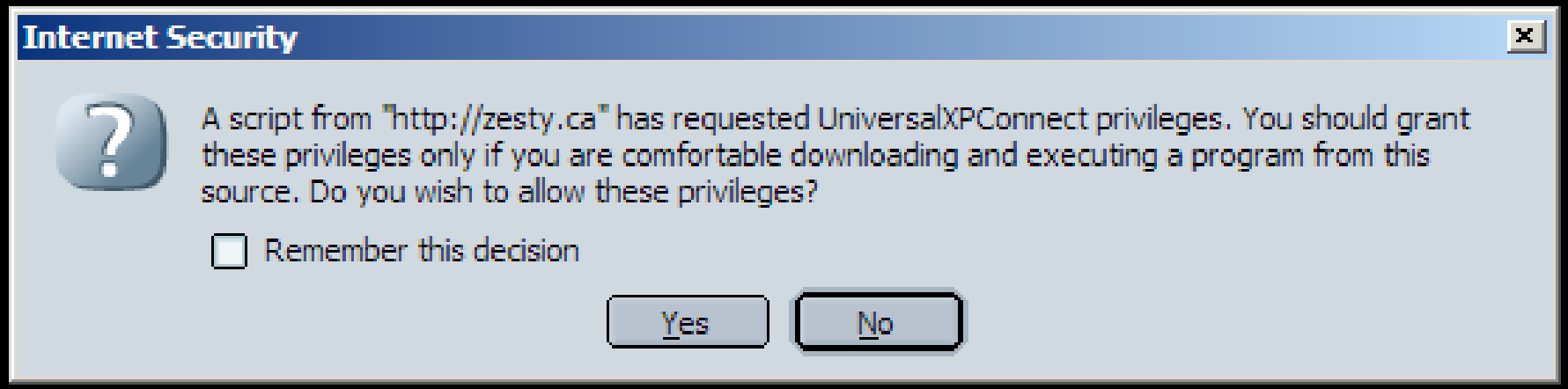
~ Blake Ross

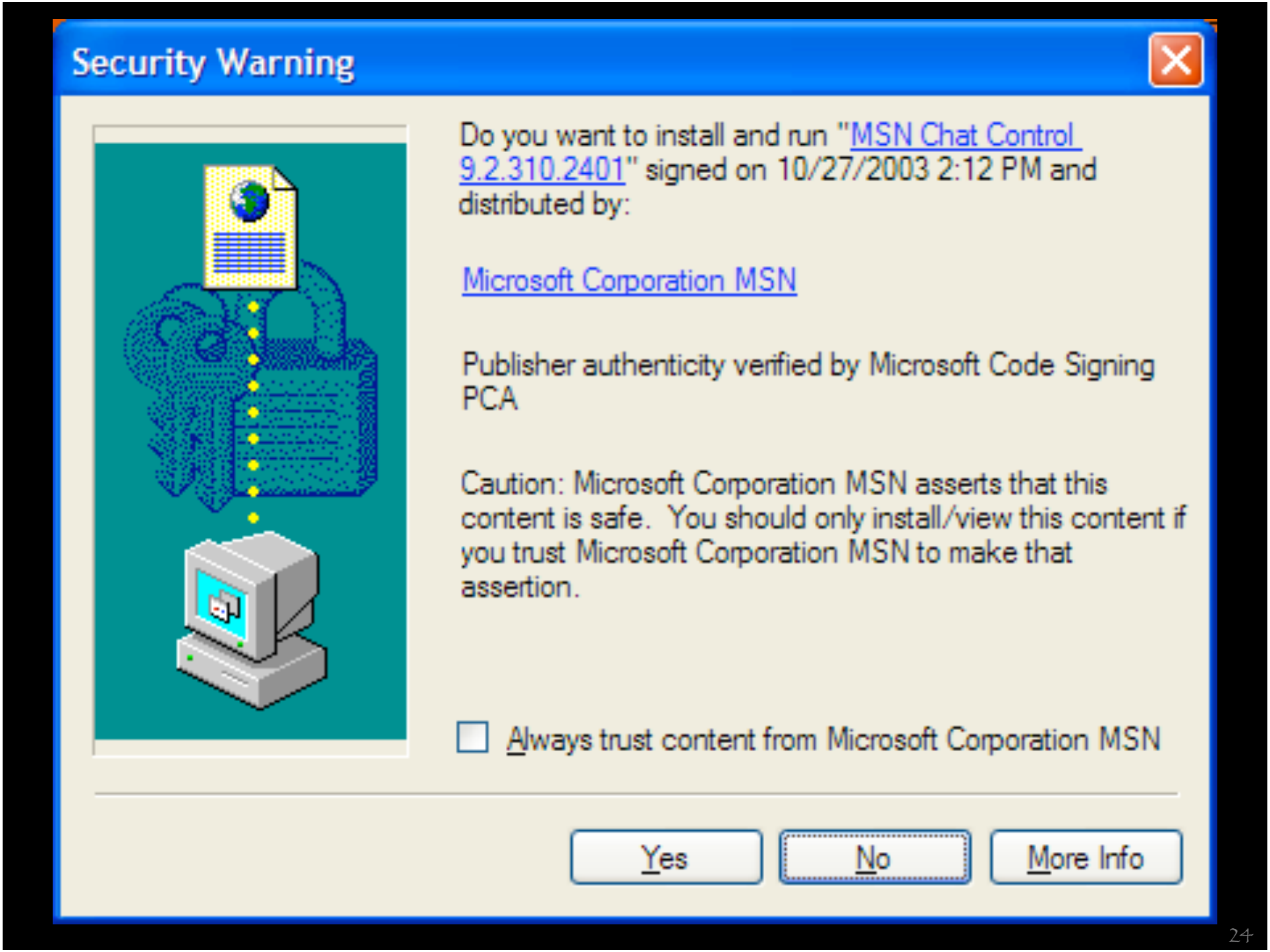
Make decisions

- Developers should not expect users to make decisions they themselves can't make

Present choices, not dilemmas

- Chris Nodder
(in charge of user experience for XP SP2)


Internet Security
A script from "http://zesty.ca" has requested UniversalXPConnect privileges. You should grant these privileges only if you are comfortable downloading and executing a program from this source. Do you wish to allow these privileges?
Remember this decision
Yes
No


Security Warning
Do you want to install and run "MSN Chat Control 9.2.310.2401" signed on 10/27/2003 2:12 PM and distributed by:
Microsoft Corporation MSN
Publisher authenticity verified by Microsoft Code Signing PCA
Caution: Microsoft Corporation MSN asserts that this content is safe. You should only install/view this content if you trust Microsoft Corporation MSN to make that assertion.
Always trust content from Microsoft Corporation MSN
Yes
No
More Info


Internet Explorer - Security Warning
Do you want to install this software?
Name: MSN Chat Control 9.2.310.2401
Publisher: Microsoft Corporation MSN
Always install software from "Microsoft Corporation MSN"
Never install software from "Microsoft Corporation MSN"
Ask me every time
Fewer options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

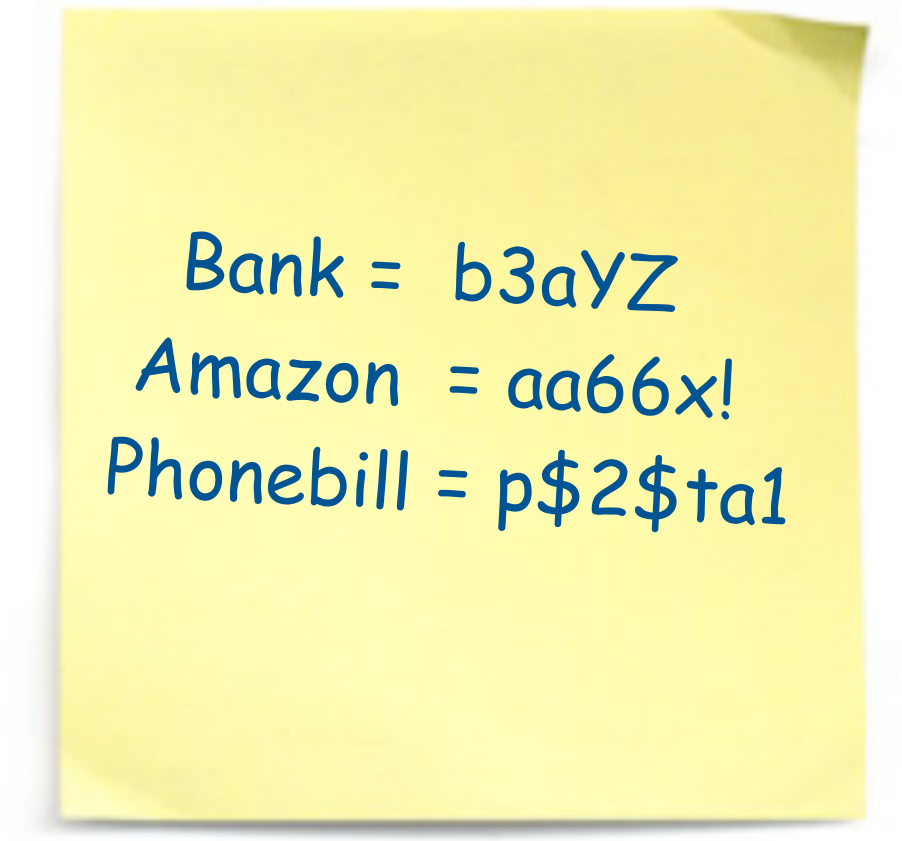
Passwords

2.

Typical advice

- Pick a hard to guess password
- Don't use it anywhere else
- Change it often
- Don't write it down

What do users do when every web site wants a password?


Bank = b3aYZ
Amazon = aa66x!
Phonebill = p2ta1

Password keeper software

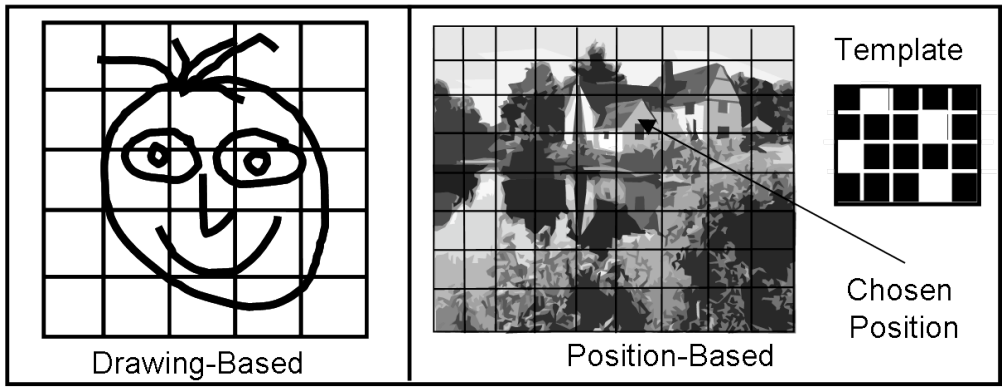
- Run on PC or handheld
- Only remember one password

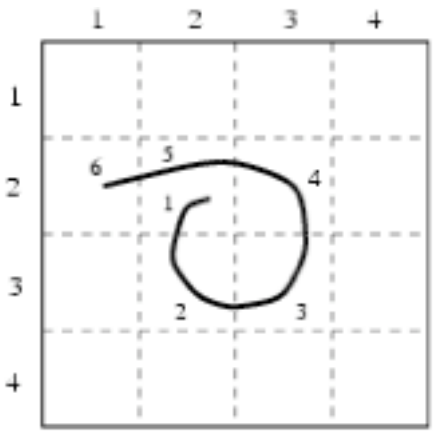
Single sign-on

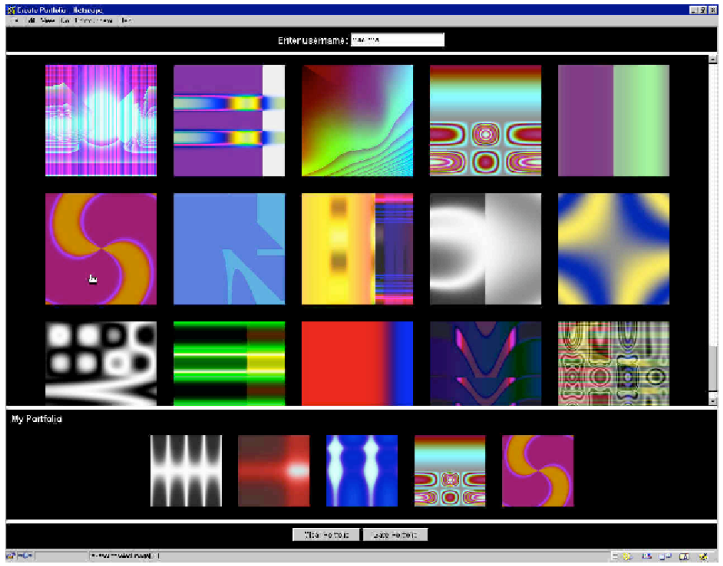
- Login once to get access to all your passwords

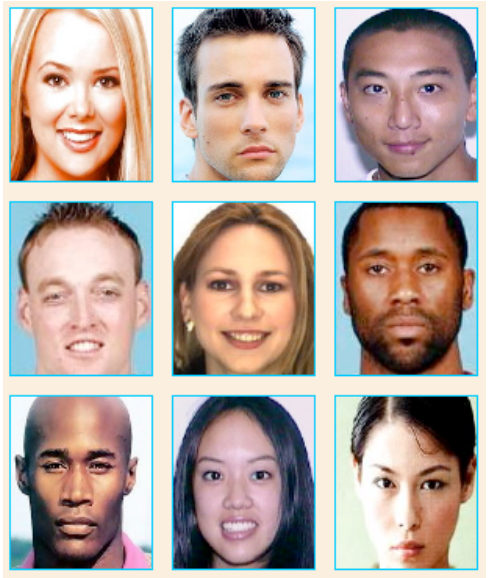
Biometrics

Graphical passwords



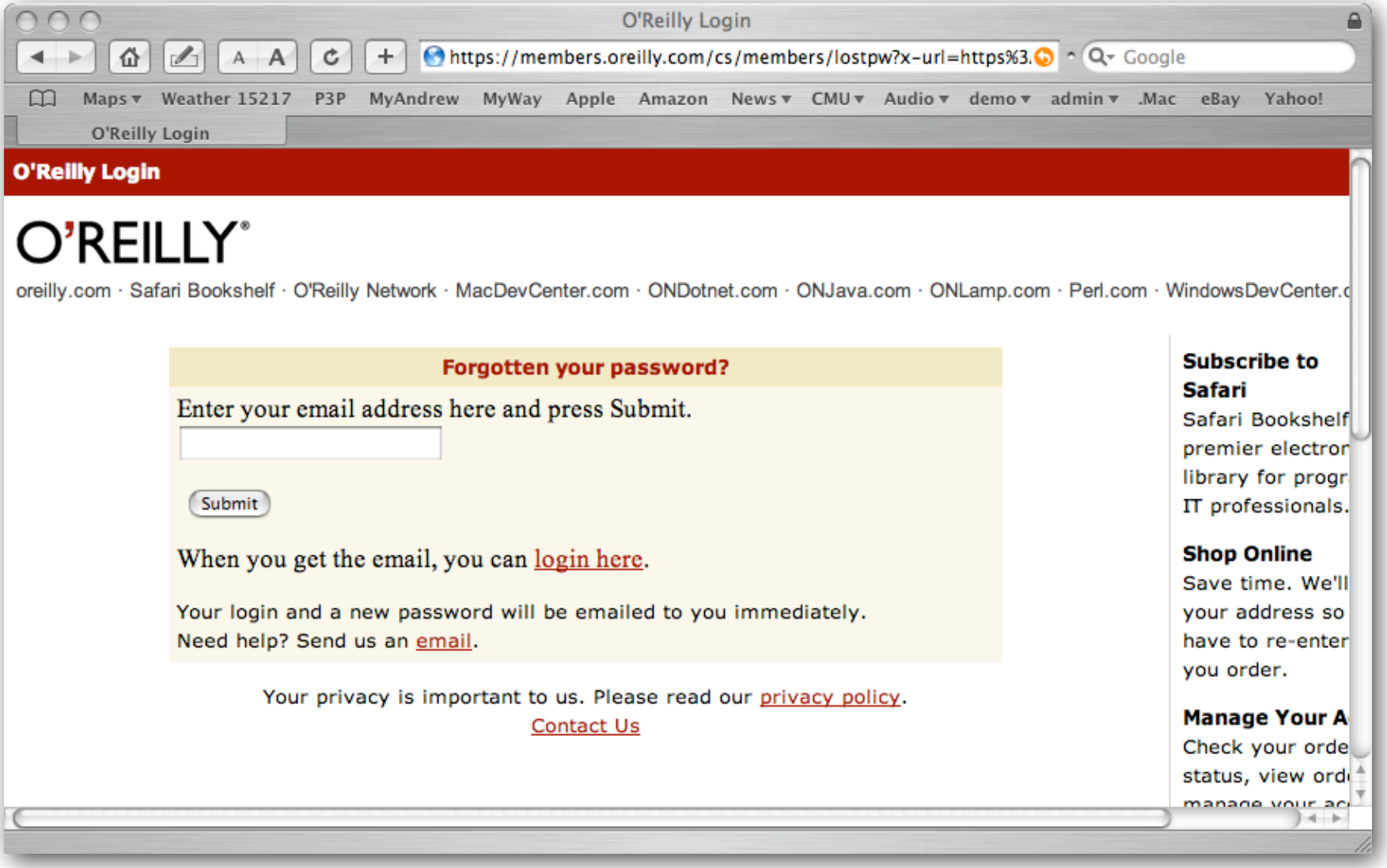






Rely on "forgotten password" mechanism

- Email password or magic URL to address on file
- Challenge questions


O'Reilly Login
https://members.oreilly.com/cs/members/lostpw?x-url=https%3.
Google
Maps
Weather 15217
P3P
MyAndrew
MyWay
Apple
Amazon
News
CMU
Audio
demo
admin
.Mac
eBay
Yahoo!
O'Reilly Login
O'Reilly Login
O'REILLY
oreilly.com · Safari Bookshelf · O'Reilly Network · MacDevCenter.com · ONDotnet.com · ONJava.com · ONLamp.com · Perl.com · WindowsDevCenter.
Forgotten your password?
Enter your email address here and press Submit.
Submit
When you get the email, you can login here.
Your login and a new password will be emailed to you immediately.
Need help? Send us an email.
Your privacy is important to us. Please read our privacy policy.
Contact Us
Subscribe to Safari
Safari Bookshelf
premier electron
library for progr
IT professionals.
Shop Online
Save time. We'll
your address so
have to re-enter
you order.
Manage Your A
Check your orde
status, view ord

Proposal

- Why not make this the normal way to access infrequently used sites?

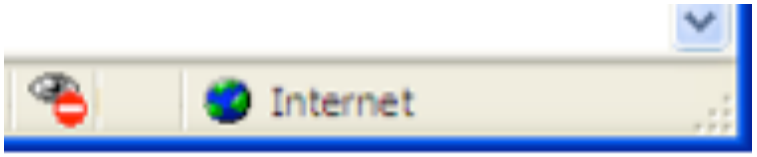
Symbols & Metaphors

3.

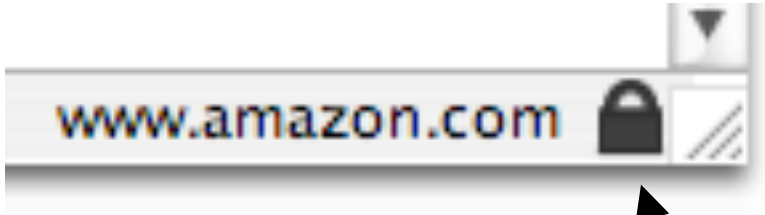

SPAM
SPAM
SPAM
SPAM

Cookie flag

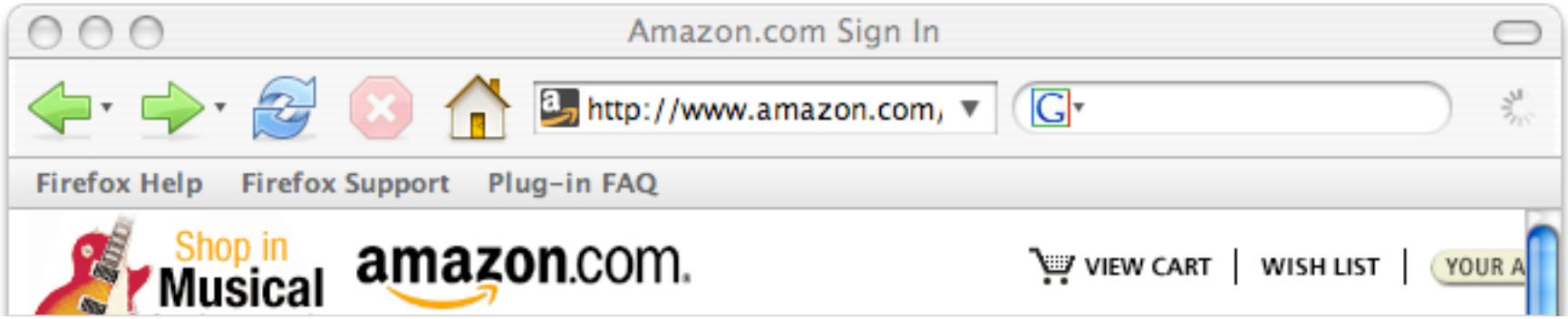
Netscape SSL icons

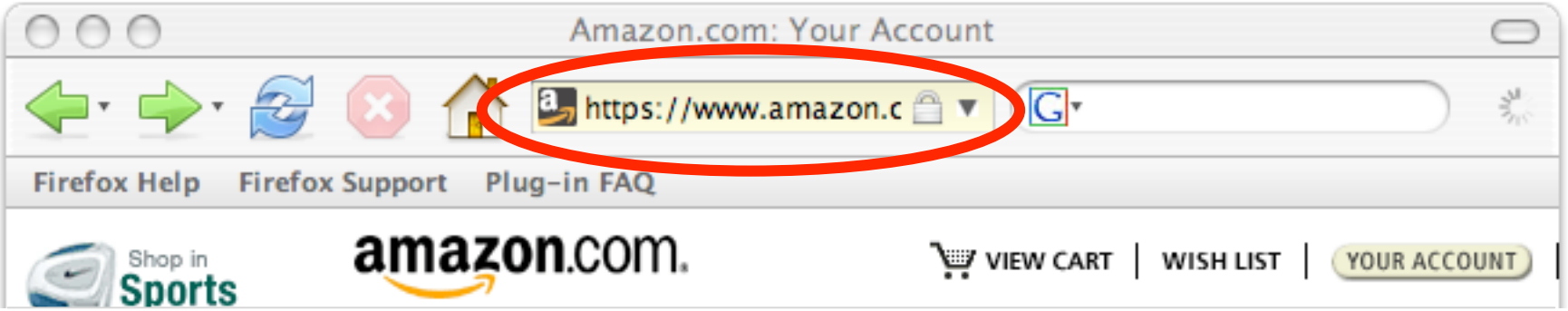


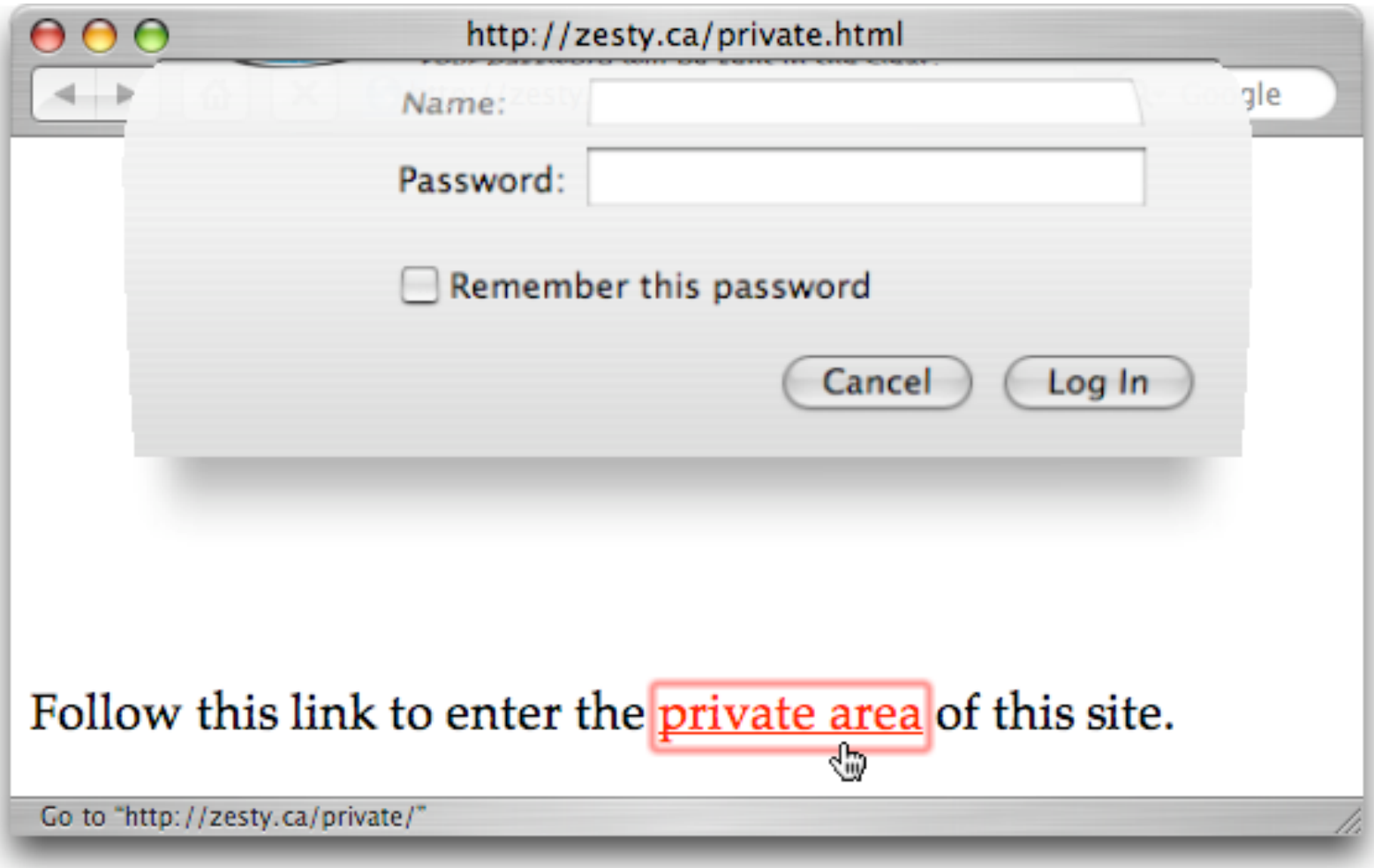
IE6 cookie flag



Firefox SSL icon


Amazon.com Sign In
http://www.amazon.com/
Firefox Help
Firefox Support
Plug-in FAQ
Shop in
Musical
amazon.com
VIEW CART
WISH LIST
YOUR A


Amazon.com: Your Account
https://www.amazon.c
Firefox Help
Firefox Support
Plug-in FAQ
Shop in
Sports
amazon.com
VIEW CART
WISH LIST
YOUR ACCOUNT


http://zesty.ca/private.html
Name:
Password:
Remember this password
Cancel
Log In
Follow this link to enter the private area of this site.
Go to "http://zesty.ca/private/"

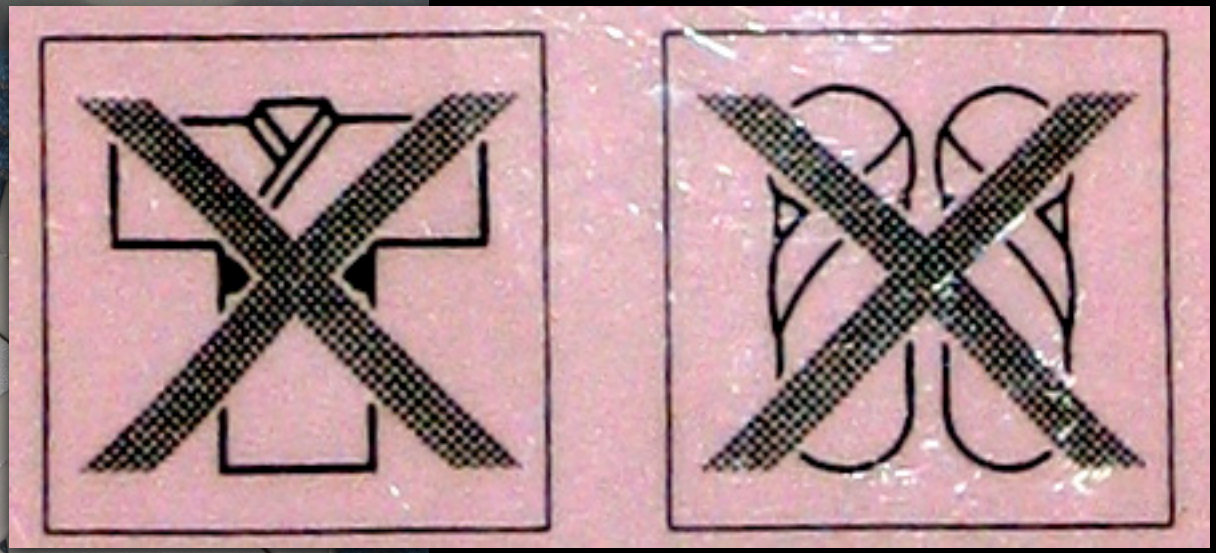
Why do I use a key rather than a pen to make a digital signature?

Privacy Bird icons

Privacy policy ***matches*** user's privacy preferences

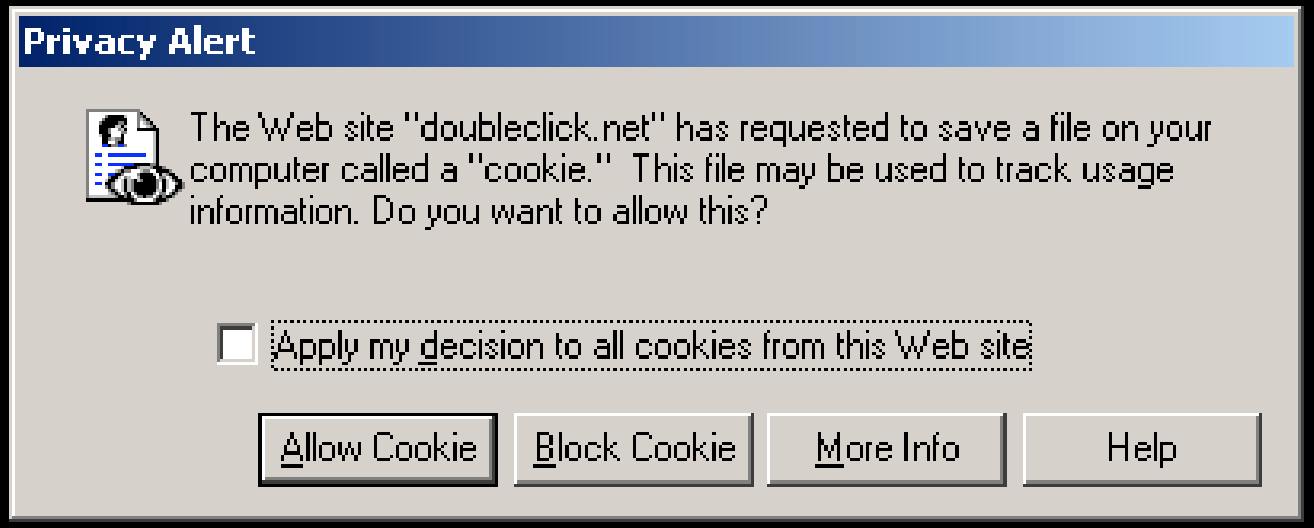
Privacy policy ***does not match*** user's privacy preferences

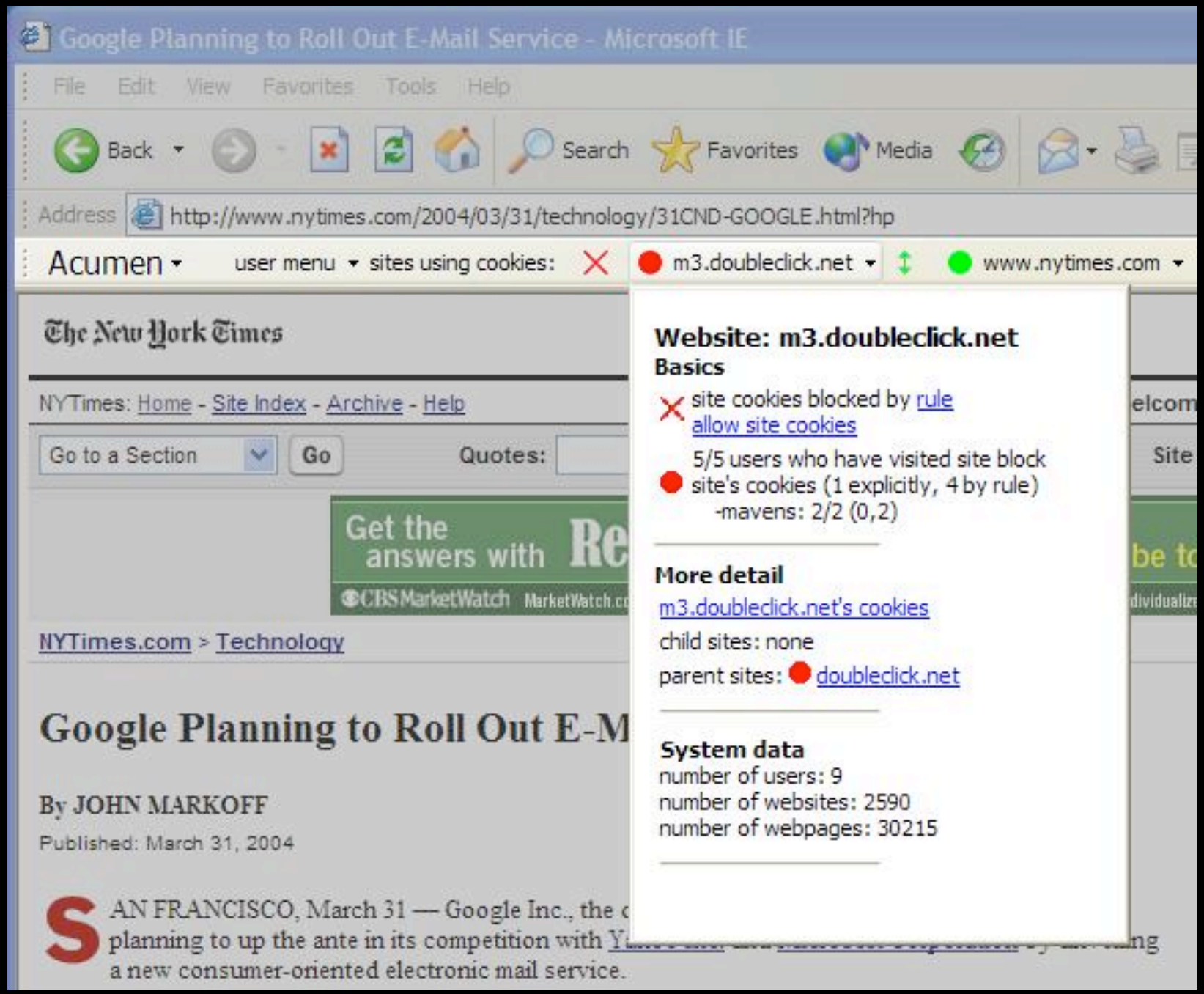

PRINCE HOTELS
浴衣・スリッパのままで、客室フロア（廊下）以外へ
お出になることは、非常時を除き、
ご遠慮ください。

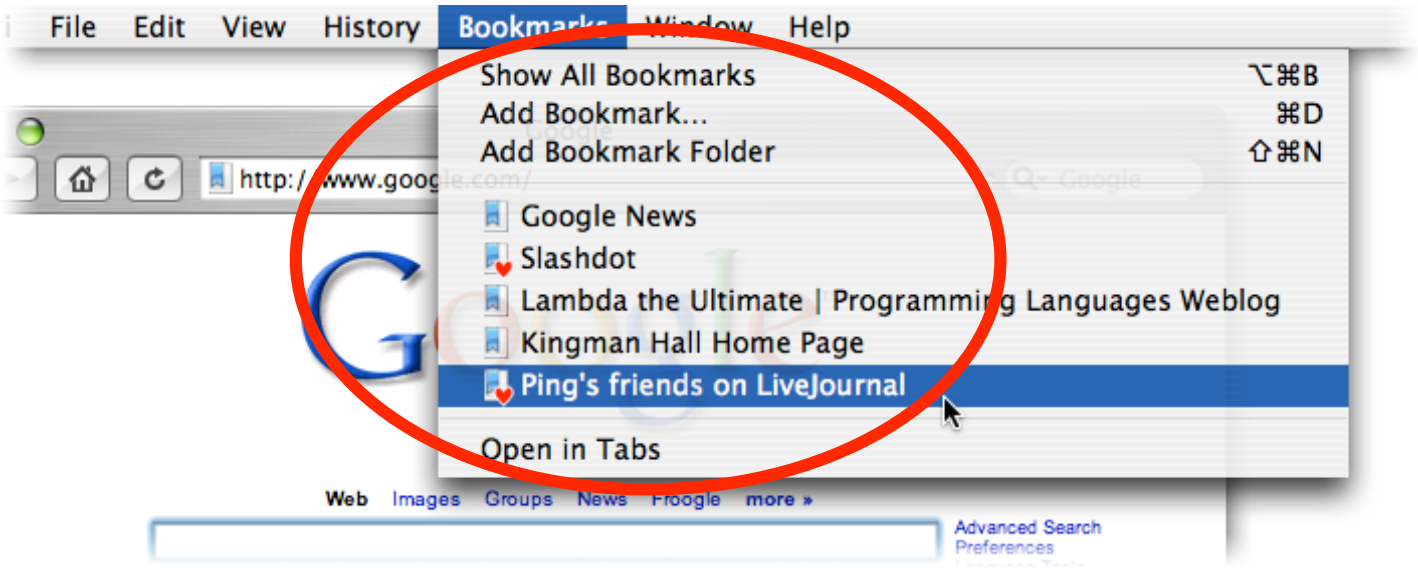


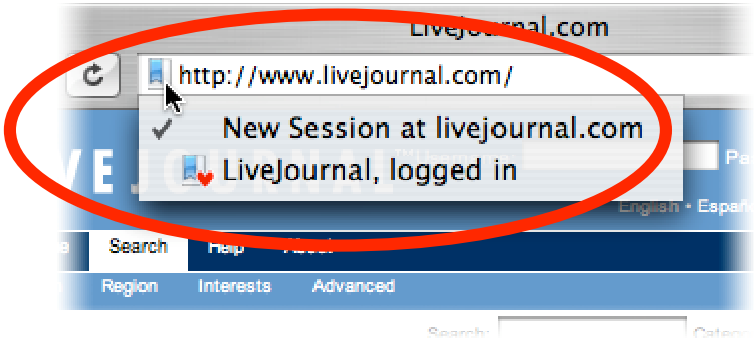
Rethinking cookies

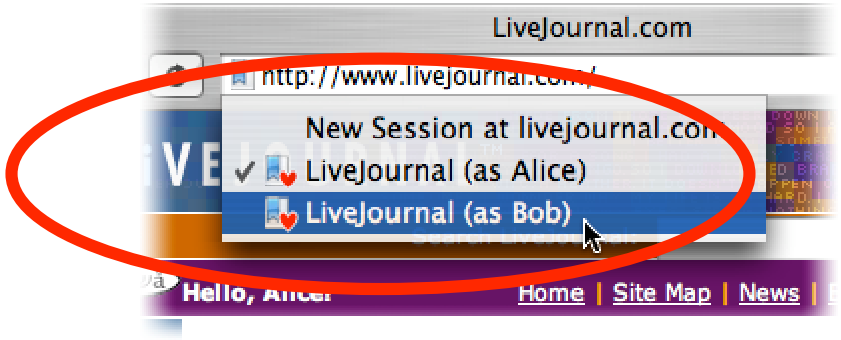
4.


Privacy Alert
The Web site "doubleclick.net" has requested to save a file on your computer called a "cookie." This file may be used to track usage information. Do you want to allow this?
Apply my decision to all cookies from this Web site
Allow Cookie
Block Cookie
More Info
Help


Google Planning to Roll Out E-Mail Service - Microsoft IE
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.nytimes.com/2004/03/31/technology/31CND-GOOGLE.html?hp
Acumen user menu sites using cookies: m3.doubleclick.net www.nytimes.com
The New York Times
NYTimes: Home - Site Index - Archive - Help
Go to a Section Go Quotes:
Get the answers with
CBSMarketWatch
NYTimes.com > Technology
Google Planning to Roll Out E-M
By JOHN MARKOFF
Published: March 31, 2004
SAN FRANCISCO, March 31 — Google Inc., the
planning to up the ante in its competition with
a new consumer-oriented electronic mail service.
Website: m3.doubleclick.net
Basics
site cookies blocked by rule
allow site cookies
5/5 users who have visited site block site's cookies (1 explicitly, 4 by rule)
-mavens: 2/2 (0,2)
More detail
m3.doubleclick.net's cookies
child sites: none
parent sites: doubleclick.net
System data
number of users: 9
number of websites: 2590
number of webpages: 30215


File
Edit
View
History
Bookmarks
Help
Show All Bookmarks
Add Bookmark...
Add Bookmark Folder
Google News
Slashdot
Lambda the Ultimate | Programming Languages Weblog
Kingman Hall Home Page
Ping's friends on LiveJournal
Open in Tabs
Web
Images
Groups
News
more »
Advanced Search
Preferences


http://www.livejournal.com/
New Session at livejournal.com
LiveJournal, logged in
Search
Region
Interests
Advanced


LiveJournal.com
New Session at livejournal.com
LiveJournal (as Alice)
LiveJournal (as Bob)
Home
Site Map
News

Making Web privacy visible

5.

Privacy

"the claim of individuals… to determine for themselves when, how, and to what extent information about them is communicated to others."

- Alan Westin, 1967

Process

"Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication...."

- Alan Westin, 1967

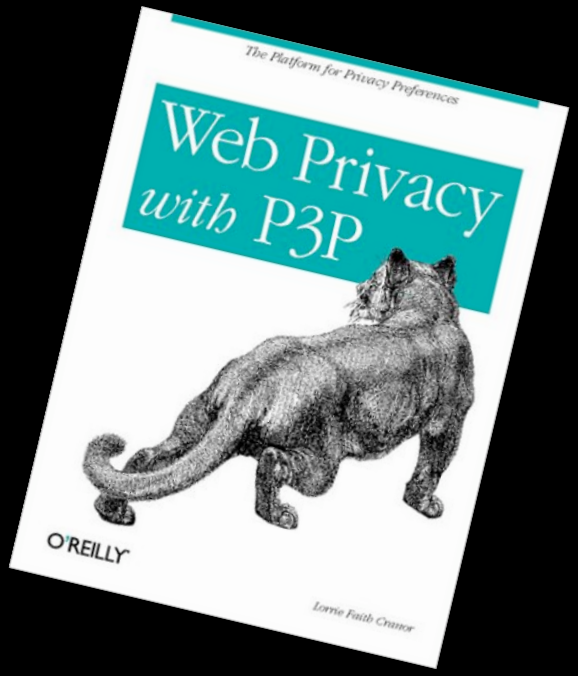
Web site privacy policies

- Many posted
- Few read

What if your browser could read privacy policies for you?

Platform for Privacy Preferences (P3P)

- 2002 W3C Recommendation
- XML format for Web privacy policies
- Protocol enables clients to locate and fetch policies from servers



P3P/XML encoding

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY discuri="http://p3pbook.com/privacy.html"
        name="policy">
  <ENTITY>
  <DATA-GROUP>
    <DATA
      ref="#business.contact-info.online.email">privacy@p3pbook.com
    </DATA>
    <DATA
      ref="#business.contact-info.online.uri">http://p3pbook.com/
    </DATA>
    <DATA ref="#business.name">Web Privacy With P3P</DATA>
  </DATA-GROUP>
  </ENTITY>
  <ACCESS><nonident/></ACCESS>
  <STATEMENT>
    <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
    <PURPOSE><admin/><current/><develop/></PURPOSE>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
       <DATA ref="#dynamic.clickstream"/>
       <DATA ref="#dynamic.http"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
</POLICIES>
```

P3P version

Location of human-readable privacy policy

P3P policy name

Site's name and contact info

Access disclosure

Human-readable explanation

How data may be used

Data recipients

Data retention policy

Types of data collected

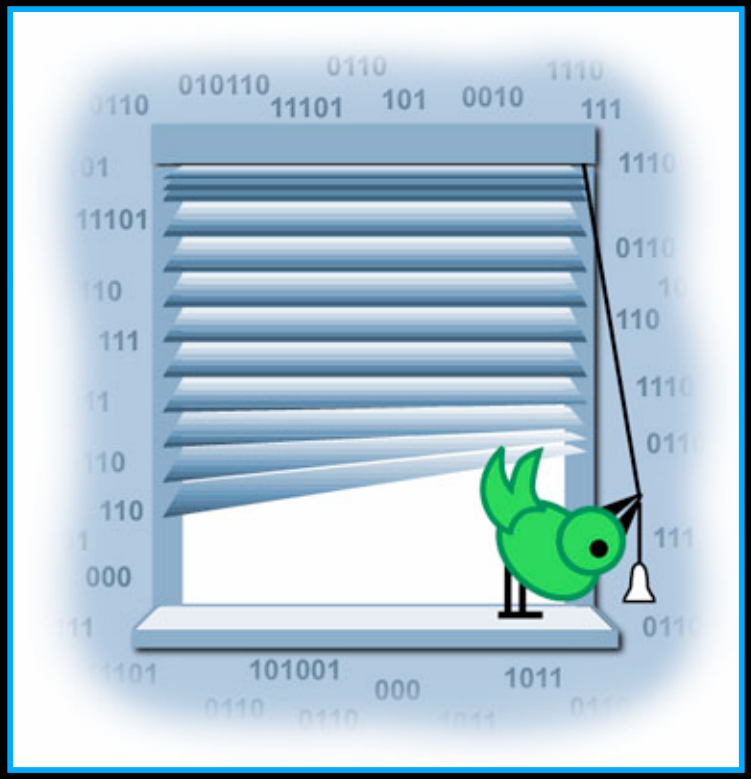
Statement

P3P adoption

- Web site adoption as of May 2005
  - 15% of top 2000 domains
  - 21% of top 500 domains
  - 29% of top 100 domains
- User agents
  - Limited P3P functionality in IE6 and Navigator 7
  - Other P3P user agents available

AT&T Privacy Bird

- P3P user agent
- Free download
  http://privacybird.com/
- Compares user preferences with P3P policies



Shane Zachary Cranor's Home Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://shane.cranor.org/ Go Links

Shane Zachary Cranor

Photo Album | Latest Photos | 2001 Favorite Photos | 2002 Favorite Photos | 2003 Favorite Photos

Watch a movie of Shane at 2 1/4 putting on his sandals and talking about mowing the lawn. "What am I doing?" he asks. "I'm putting them on slowly," he says (he really means "loosely"). If you are not sure what he's saying, read the transcript.

Shane's Photo Album

- Shane's First Year
- Shane's Second Year
- Shane at 24-25 Months
- Shane at 26-27 Months

Done Internet

Shane Zachary Cranor's Home Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://shane.cranor.org/ Go Links

Shane Zachary

Shane's Photo Albun

- Shane's First Year
- Shane's Second Year
- Shane at 24-25 Montl
- Shane at 26-27 Montl

Done

Policy Summary

Shane Cranor's Home Page Privacy Practices

Privacy Policy Check

Shane Cranor's Home Page's privacy policy *matches your preferences.*

Privacy Policy Summary

This site has the following statements in its policy:

- Site Statement 1

Site Statement 1

Types of Information Collected:

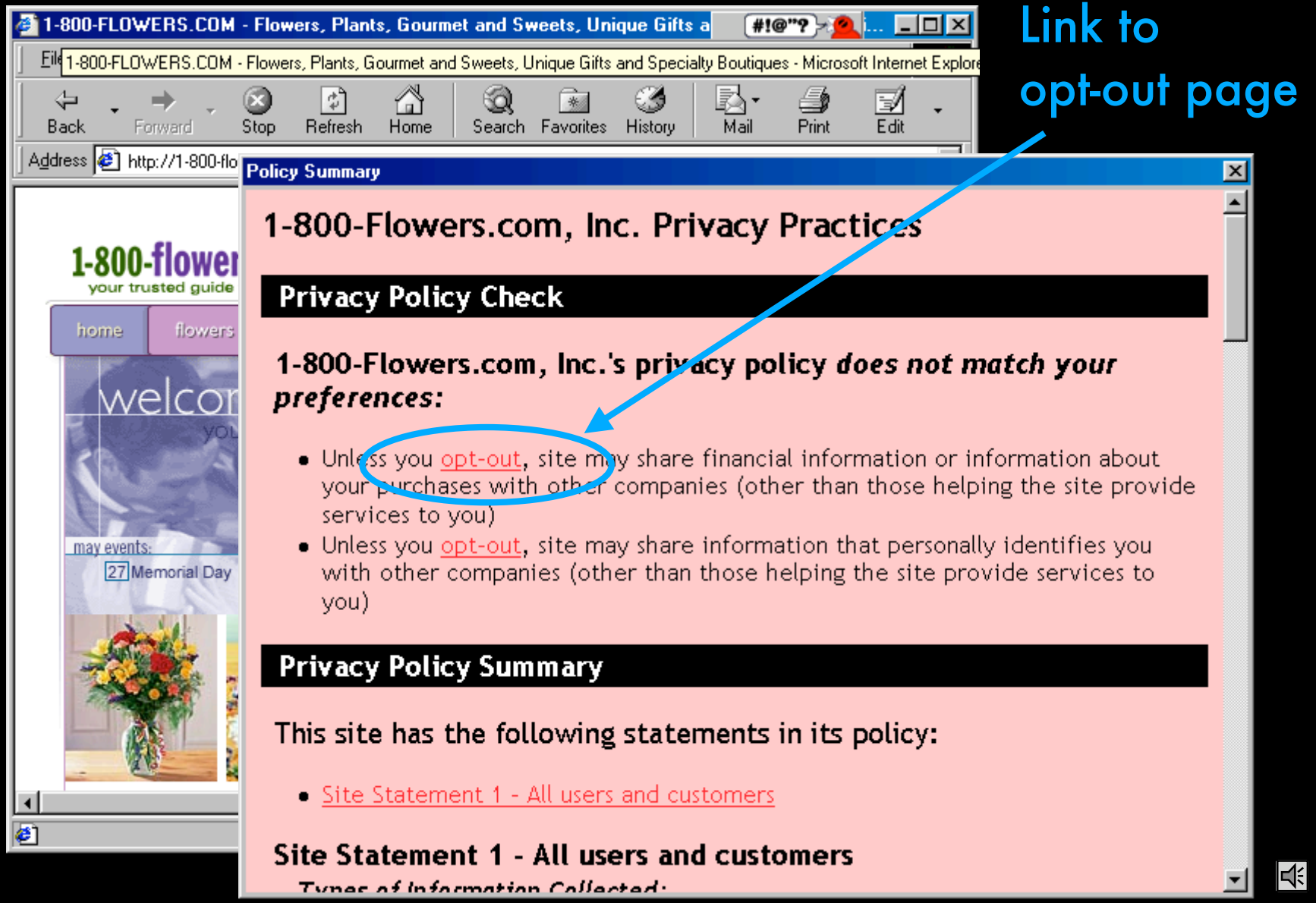
- HTTP protocol information
- Click-stream information

How your information will be used:

- Research and development
- To complete the activity for which the data was provided
- Web site and system administration

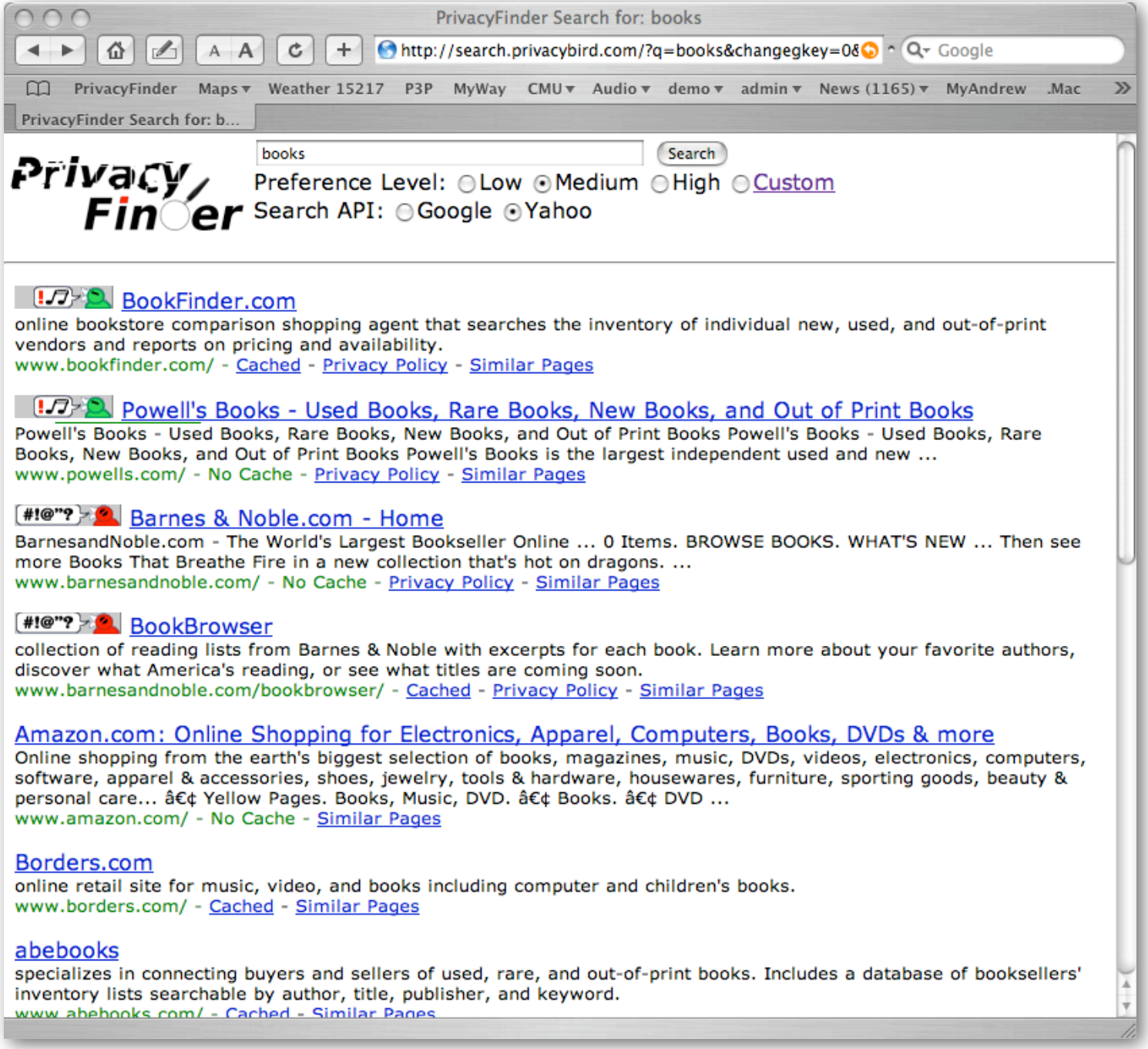
Who will use your information:

- This web site and its agents



Link to opt-out page

How can I find a site that will protect my privacy?


PrivacyFinder Search for: books
http://search.privacybird.com/?q=books&changegkey=0&
Google
PrivacyFinder
Maps
Weather 15217
P3P
MyWay
CMU
Audio
demo
admin
News (1165)
MyAndrew
.Mac
PrivacyFinder Search for: b...
Privacy Finder
books
Search
Preference Level: Low Medium High Custom
Search API: Google Yahoo
BookFinder.com
online bookstore comparison shopping agent that searches the inventory of individual new, used, and out-of-print vendors and reports on pricing and availability.
www.bookfinder.com/ - Cached - Privacy Policy - Similar Pages
Powell's Books - Used Books, Rare Books, New Books, and Out of Print Books
Powell's Books - Used Books, Rare Books, New Books, and Out of Print Books Powell's Books - Used Books, Rare Books, New Books, and Out of Print Books Powell's Books is the largest independent used and new ...
www.powells.com/ - No Cache - Privacy Policy - Similar Pages
Barnes & Noble.com - Home
BarnesandNoble.com - The World's Largest Bookseller Online ... 0 Items. BROWSE BOOKS. WHAT'S NEW ... Then see more Books That Breathe Fire in a new collection that's hot on dragons. ...
www.barnesandnoble.com/ - No Cache - Privacy Policy - Similar Pages
BookBrowser
collection of reading lists from Barnes & Noble with excerpts for each book. Learn more about your favorite authors, discover what America's reading, or see what titles are coming soon.
www.barnesandnoble.com/bookbrowser/ - Cached - Privacy Policy - Similar Pages
Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more
Online shopping from the earth's biggest selection of books, magazines, music, DVDs, videos, electronics, computers, software, apparel & accessories, shoes, jewelry, tools & hardware, housewares, furniture, sporting goods, beauty & personal care... â€¢ Yellow Pages. Books, Music, DVD. â€¢ Books. â€¢ DVD ...
www.amazon.com/ - No Cache - Similar Pages
Borders.com
online retail site for music, video, and books including computer and children's books.
www.borders.com/ - Cached - Similar Pages
abebooks
specializes in connecting buyers and sellers of used, rare, and out-of-print books. Includes a database of booksellers' inventory lists searchable by author, title, publisher, and keyword.

Wireless privacy

- Many users unaware that communications over wireless computer networks are not private

Wall of sheep

Photo credit: Kyoorius @ techfreakz.org http://www.techfreakz.org/defcon10/?slide=38

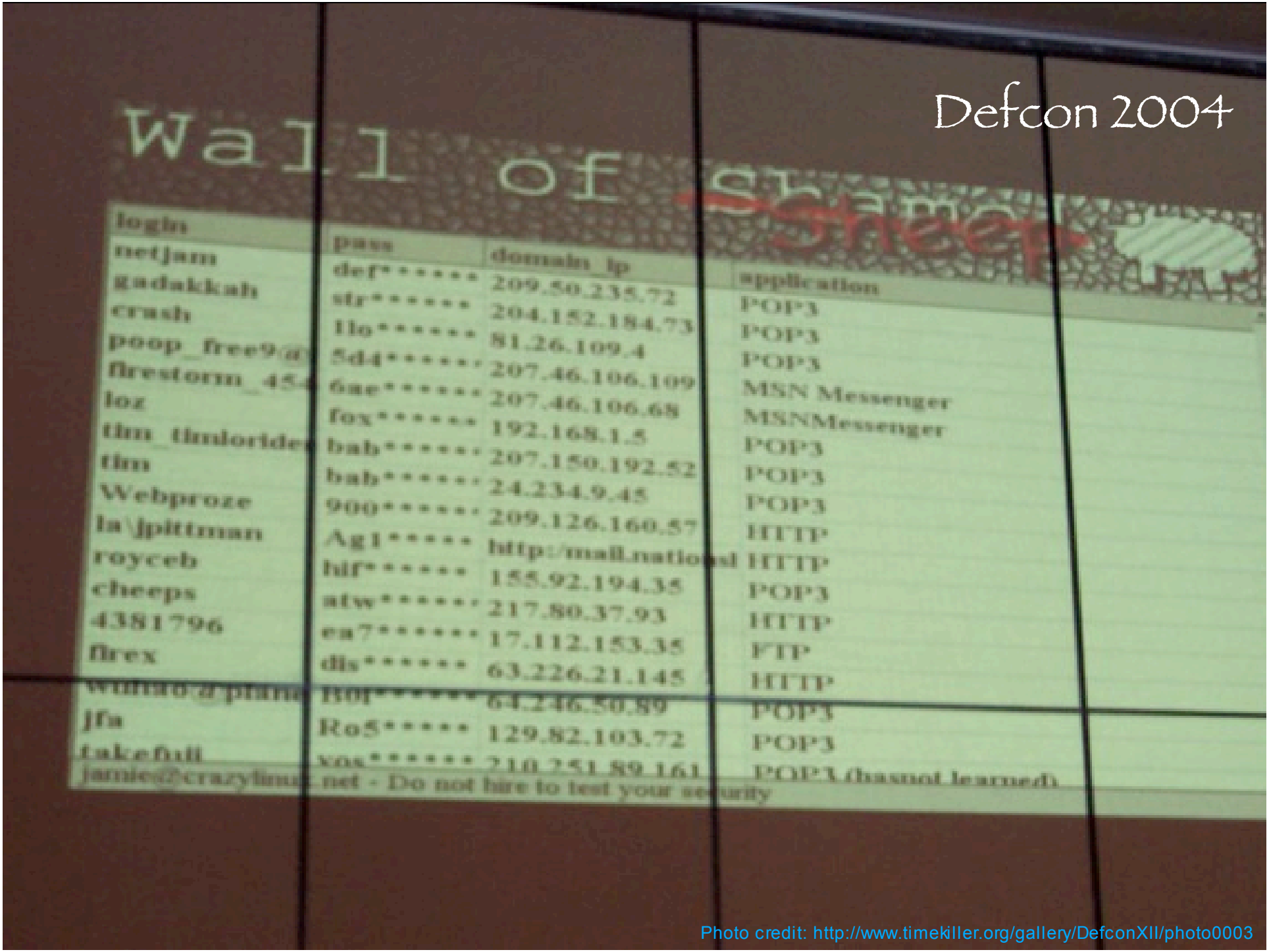


Photo credit: http://www.timekiller.org/gallery/DefconXII/photo0003

Peripheral display

- Help users form more accurate expectations of privacy
- Without making the problem worse


network
privacy
wireless

Experimental trial

- 11 subjects in student workspace
- Data collected by survey and traffic analysis
- Did they refine their expectations of privacy?

Results

- No change in behavior
- Peripheral display raised privacy awareness in student workspace
- But they didn't really get it

Privacy awareness increased

"I feel like my information /activity / privacy are not being protected .... seems like someone can monitor or get my information from my computer, or even publish them."

But only while the display was on

"Now that words [projected on the wall] are gone, I'll go back to the same."

Questions to ask about a security or privacy cue

- Do users notice it?
- Do they know what it means?
- Do they know what they are supposed to do when they see it?
- Will they actually do it?
- Will they keep doing it?

security controls they can understand

privacy they can control

CMU Usable Privacy and Security Laboratory

http://cups.cs.cmu.edu/

Carnegie Mellon