

Towards Usable Web Privacy and Security



Lorrie Faith Cranor

12 May 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.”

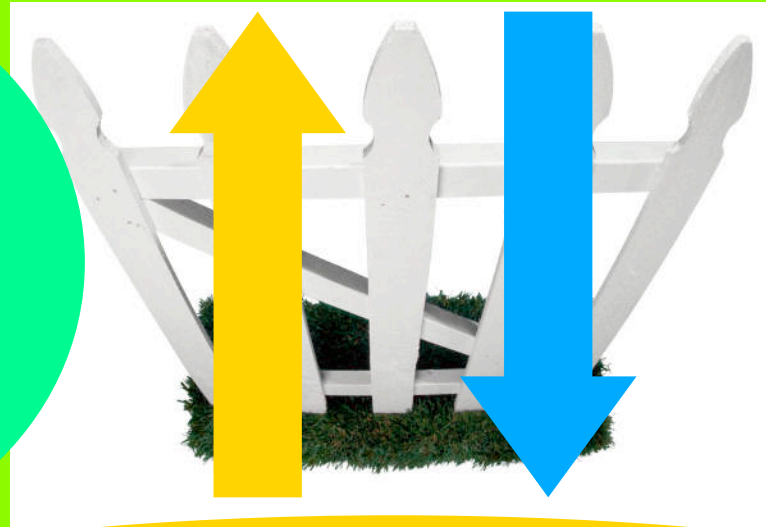
- Computing Research Association 2003

security controls they can understand
privacy they can control

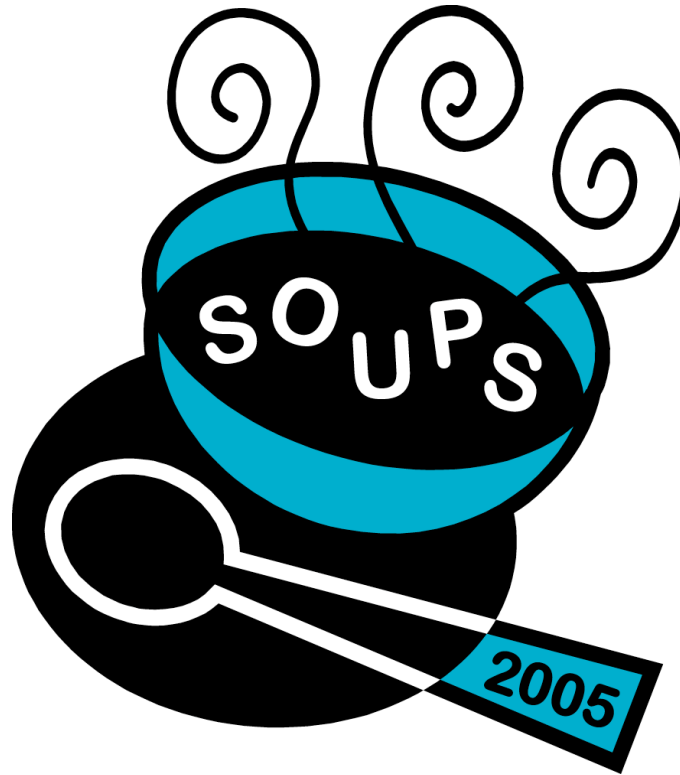
Just work

**security/privacy researchers
and system developers**

**Web
standards
authors and
user agent
developers**



**human computer interaction researchers
and usability professionals**



Symposium On Usable Privacy and Security (SOUPS)

July 6-8, 2005

Pittsburgh, PA USA

<http://cups.cs.cmu.edu/soups/>

Agenda

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

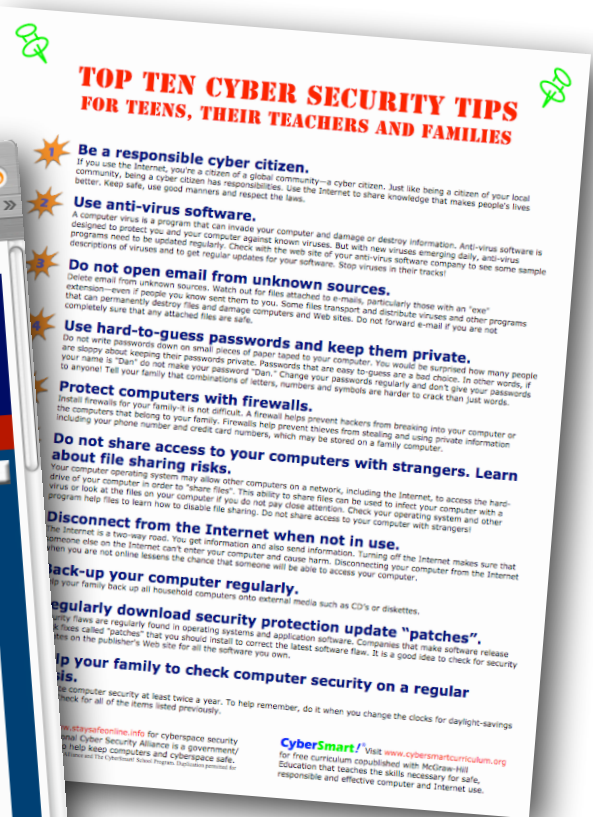
Problems and approaches



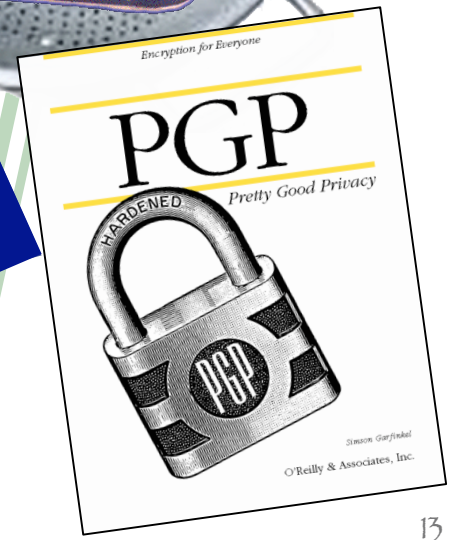
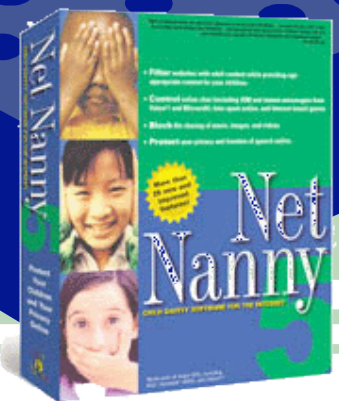
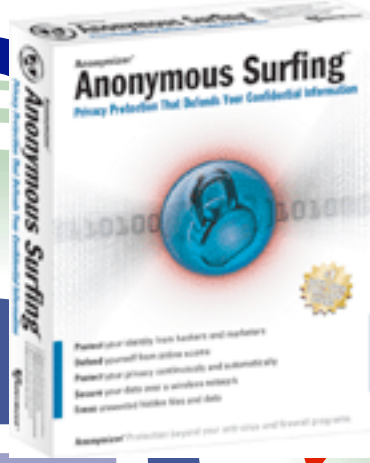
1.

How do you stay safe
online?

Advice



Experts recommend...



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

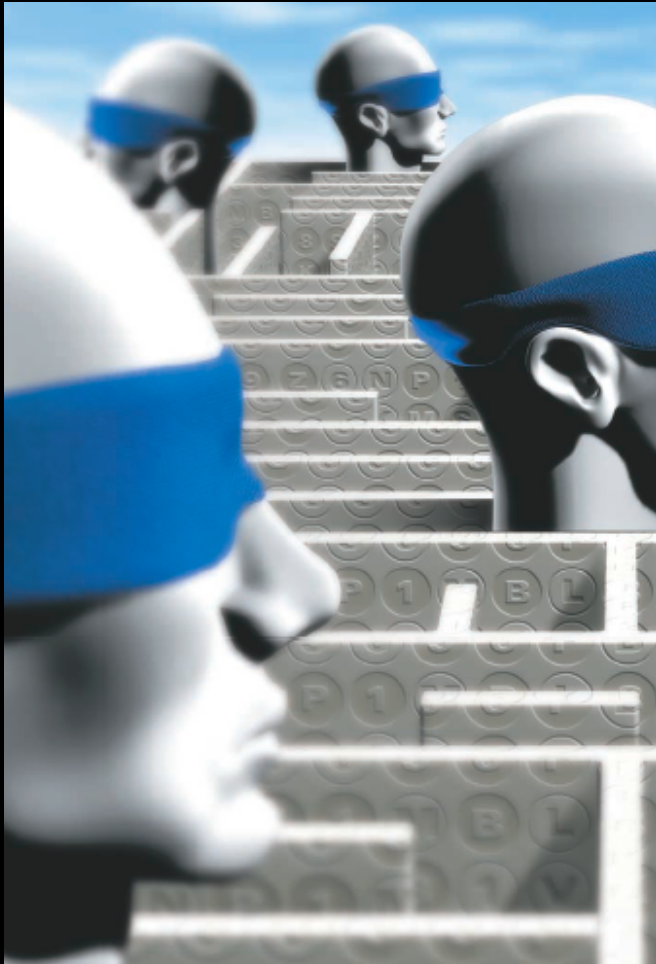


Firefox security assumptions

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



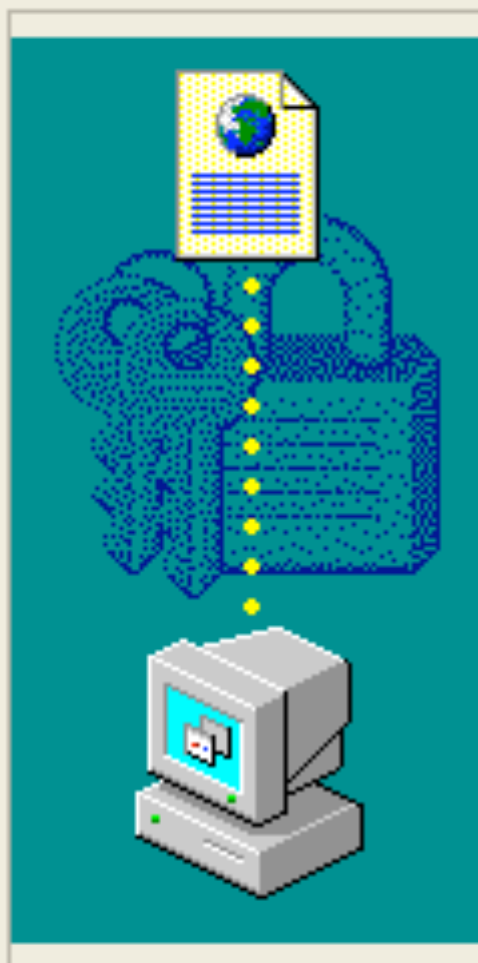
A script from "http://zesty.ca" has requested UniversalXPConnect privileges. You should grant these privileges only if you are comfortable downloading and executing a program from this source. Do you wish to allow these privileges?

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?](#)

Summary:

Problems and approaches

- Users don't want to spend time actively dealing with security and privacy
- Security and privacy are secondary tasks
- General approaches
 - Make it just work
 - Make security/privacy understandable
 - Train the user
- Present choices, not dilemmas

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 = p\$2\$ta1



Password keeper software

- Run on PC or handheld
- Only remember one password

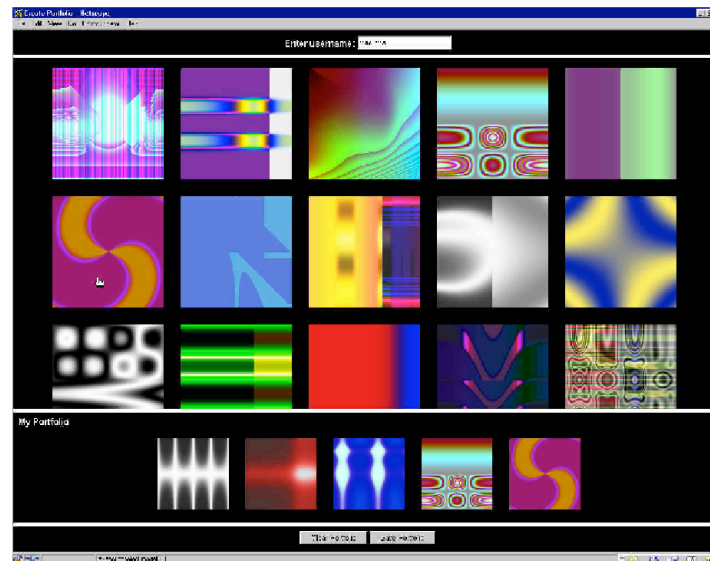
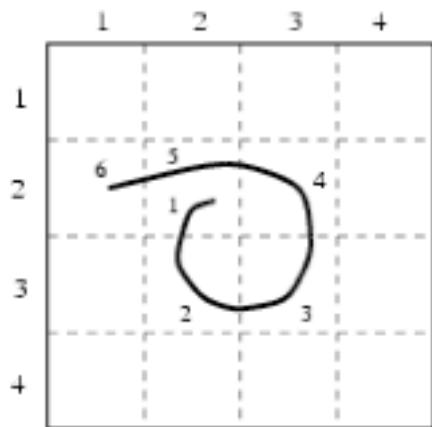
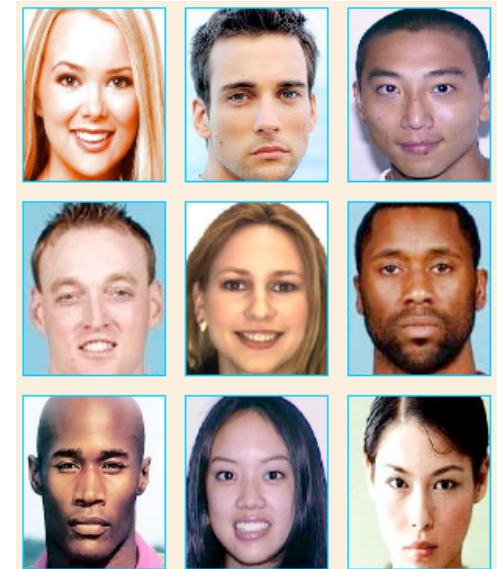
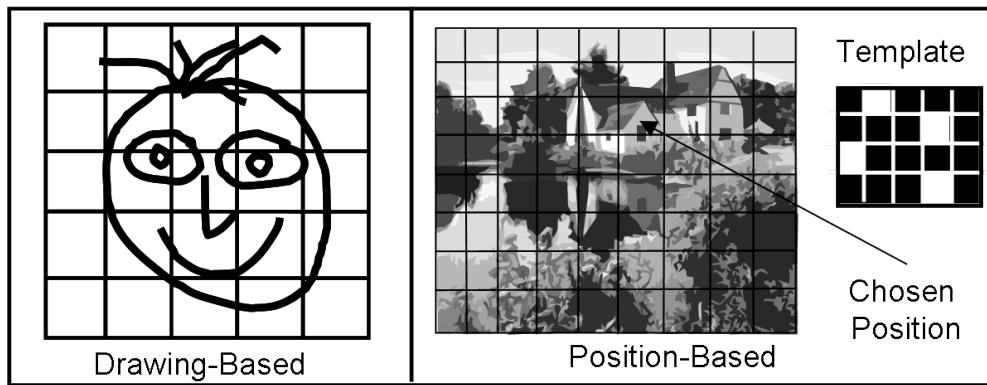
Single sign-on

- Login once to get access to all your passwords

Biometrics

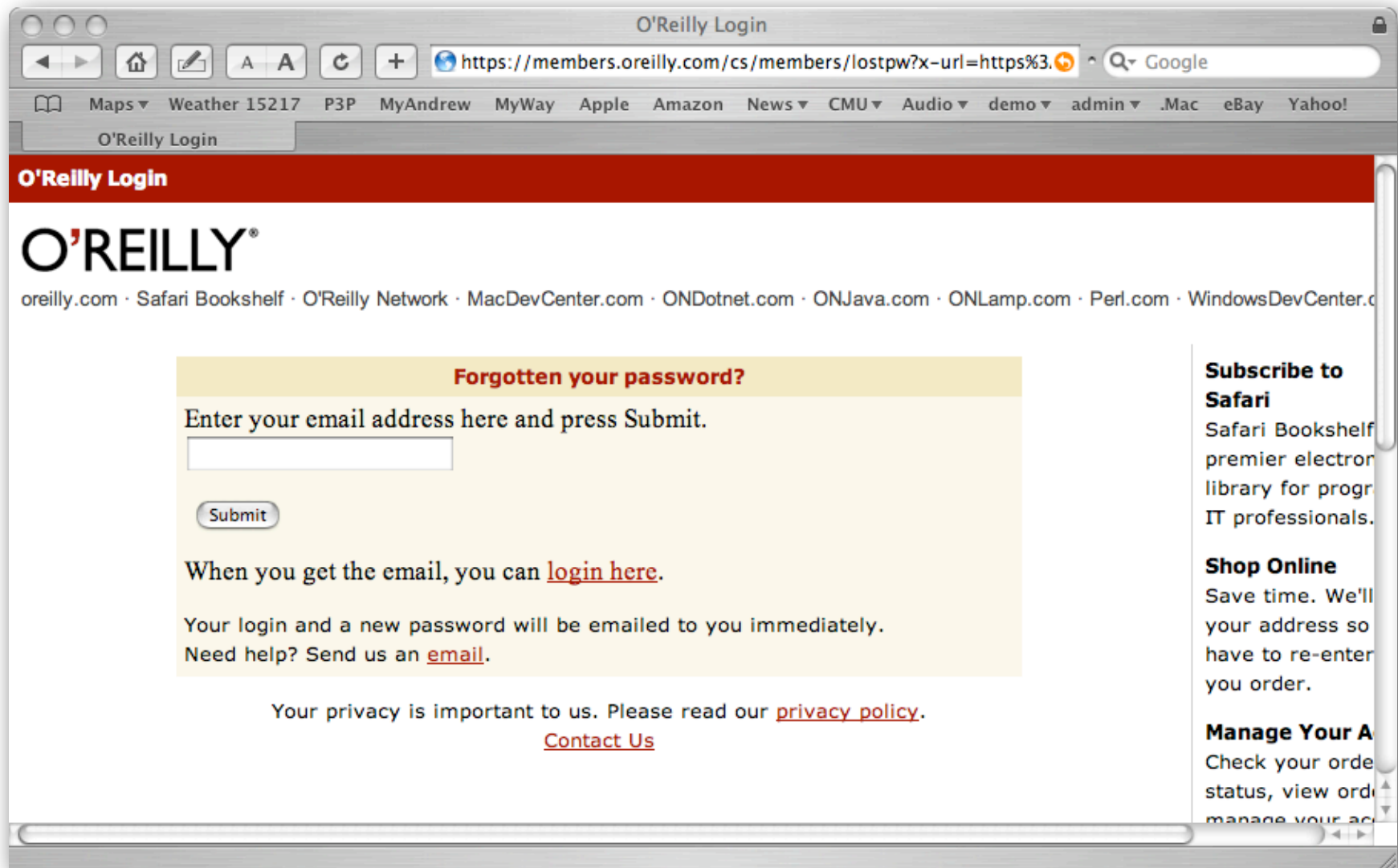


Graphical passwords



Rely on “forgotten password” mechanism

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



Proposal

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

Summary: Solving the password proliferation problem

- Existing solutions such as password keepers and fingerprint readers allow users to cope, but still have problems
- Graphical passwords look promising, but more research needed
- Need to think about solutions that eliminate passwords altogether

Symbols & Metaphors



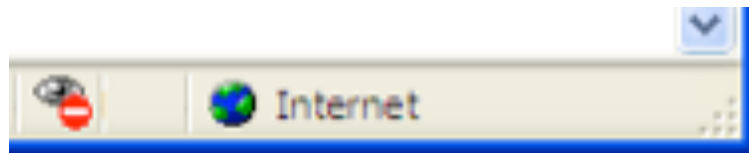
3.



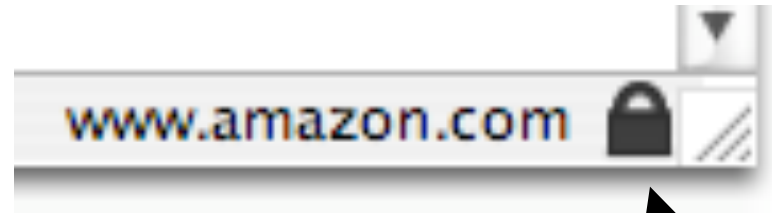
Cookie flag



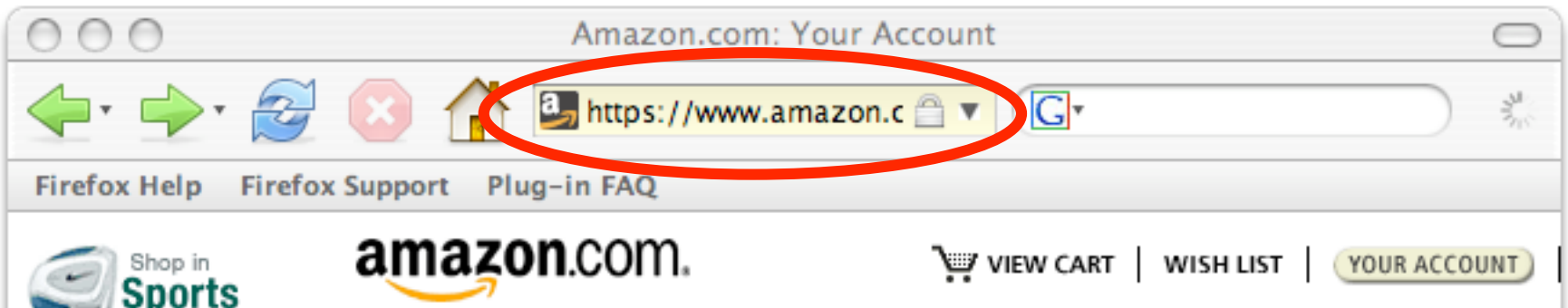
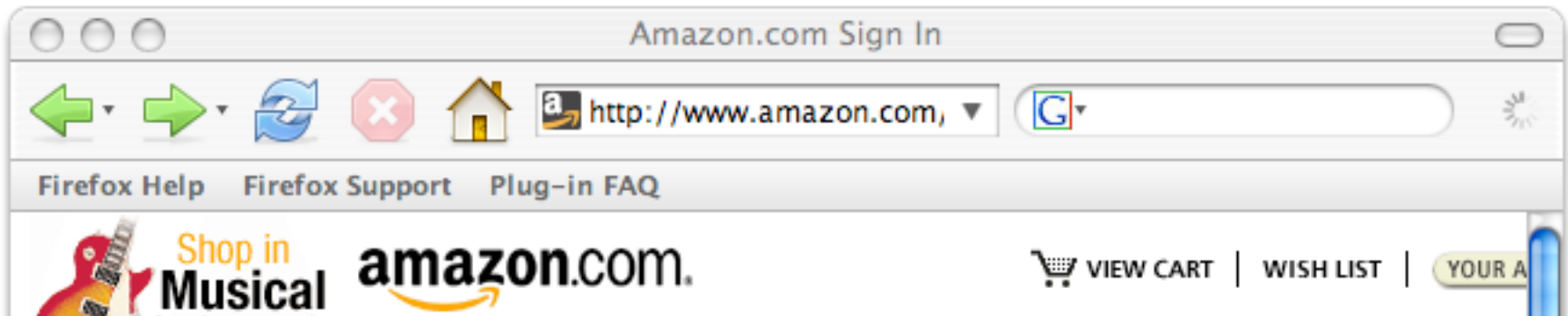
Netscape SSL icons

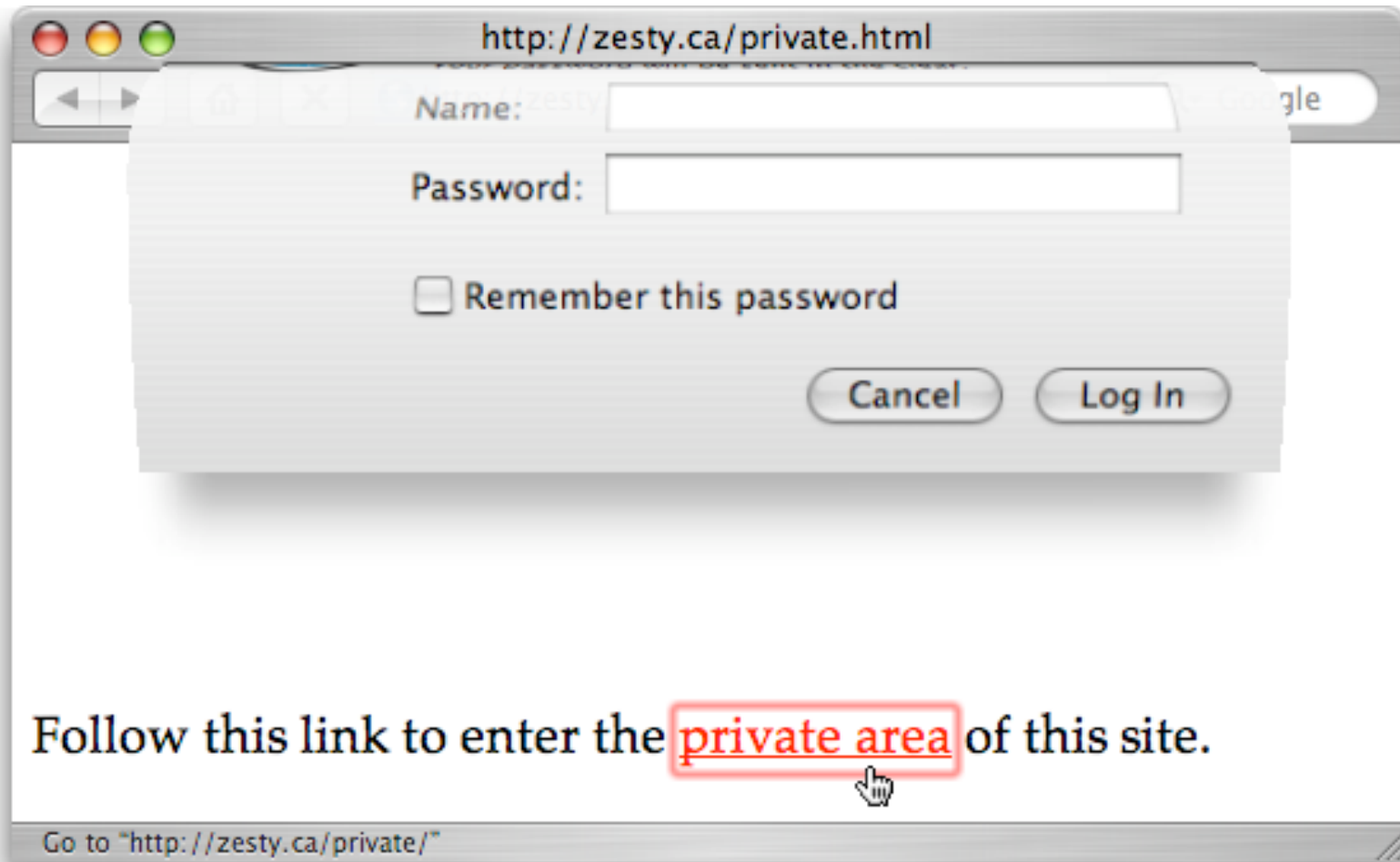


IE6 cookie flag



Firefox SSL icon





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



Privacy Bird icons

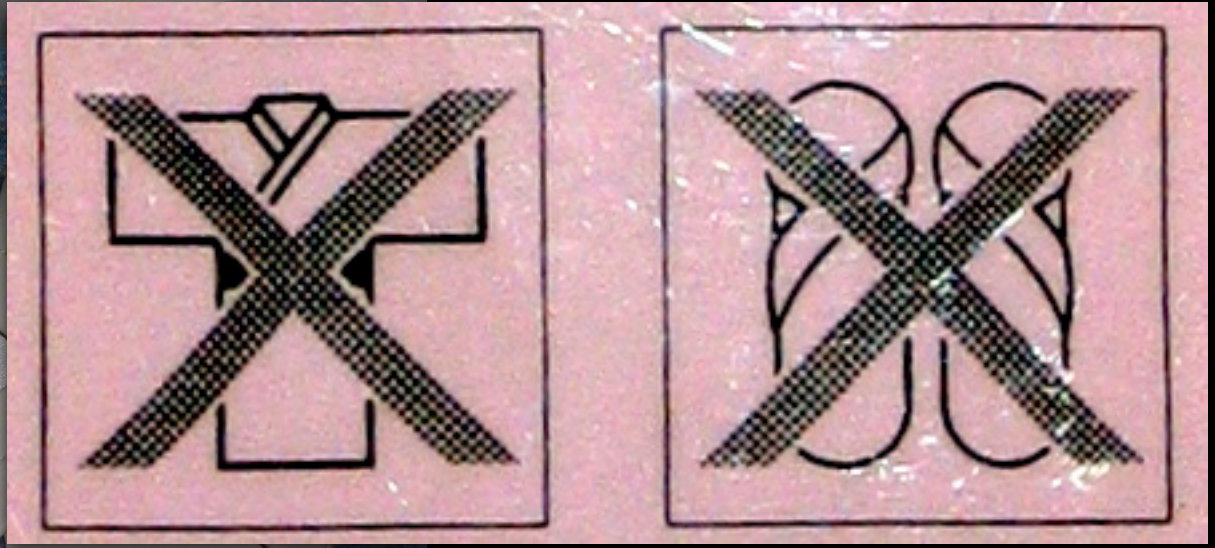
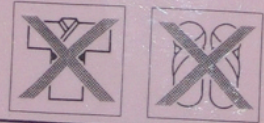


Privacy policy
matches user's
privacy preferences

Privacy policy
does not
match user's
privacy
preferences



浴衣・スリッパのまま、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。



Summary: Symbols & Metaphors

- Potential to make security and privacy concepts understandable
- Many are non-intuitive, too subtle, and easily misinterpreted
- Need to rethink some of the symbols and metaphors we have been using

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

The image shows a Mozilla browser window with the address bar displaying `http://www.ibm.com/e-business/index.jsp`. The browser's sidebar is open to the 'Cookies' section, which lists several cookies. A 'Cookie Manager' dialog box is overlaid on the browser, showing a table of stored cookies and detailed information for the selected 'SYSTEM_USER_ID' cookie from 'Microsoft.com'.

Peripheral Awareness Sidebar (points to the sidebar area)

Individual Cookie Entry (points to the selected 'Microsoft.com: SYSTEM_USER_ID' entry in the sidebar)

Cookie Manager (points to the 'Cookie Manager' dialog box)

Learn About Cookies (points to the 'Learn About Cookies' button at the bottom of the sidebar)

Site	Cookie Name
Microsoft.com	SYSTEM_USER_ID
bankofamerica.com	BOACCOOKIE
ibm.com	EISession

Information about the selected Cookie	
Name:	SYSTEM_USER_ID
Information:	(7938CB31-9279-49b2-45A9-61182816896E)
Host:	Microsoft.com
Path:	/
Serve Secure:	no
Expires:	Friday, December 31, 2010 15:13:45

Google Planning to Roll Out E-Mail Service - Microsoft IE

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print

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 Quotes:

Get the answers with **Re**
 CBSMarketWatch MarketWatch.com

[NYTimes.com](#) > [Technology](#)

Google Planning to Roll Out E-M

By JOHN MARKOFF
 Published: March 31, 2004

SAN FRANCISCO, March 31 — Google Inc., the c
 planning to up the ante in its competition with Y
 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

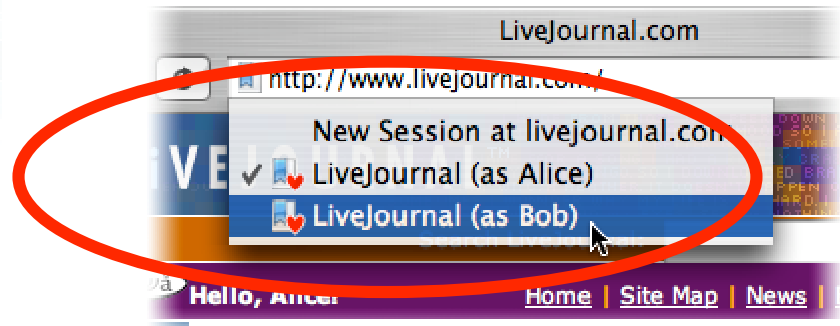
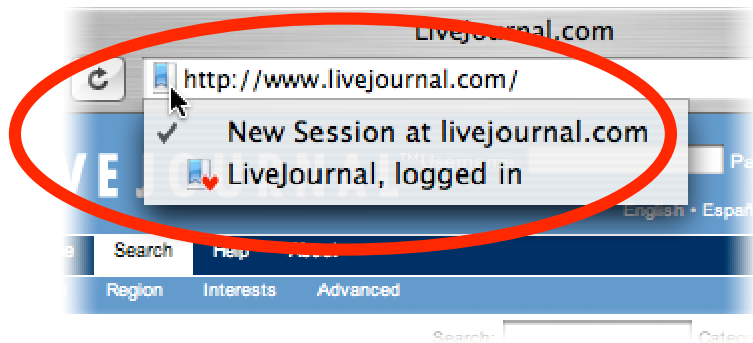
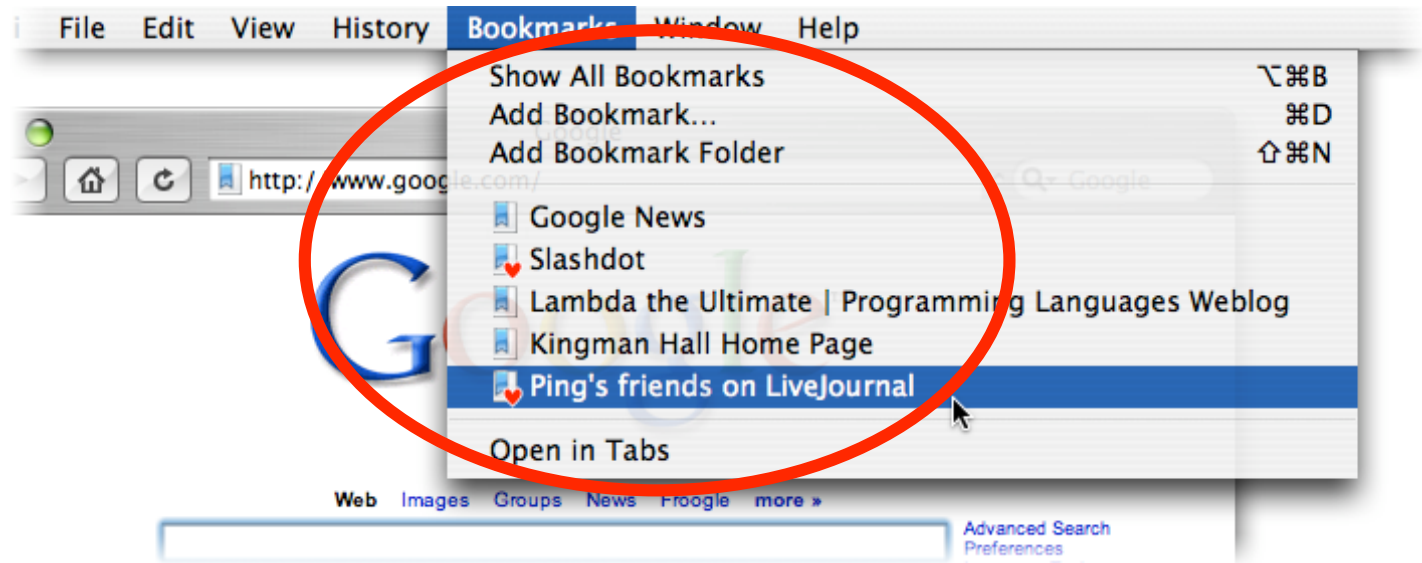
[m3.doubleclick.net's cookies](#)

child sites: none

parent sites: ● [doubleclick.net](#)

System data

number of users: 9
 number of websites: 2590
 number of webpages: 30215



Summary:

Rethinking cookies

- Current browser cookie interfaces still don't make sense to users
- New approaches should be explored and tested
 - Make cookies more visible
 - Use community recommendations to manage cookies
 - Replace cookies with personalized bookmarks in the user interface

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

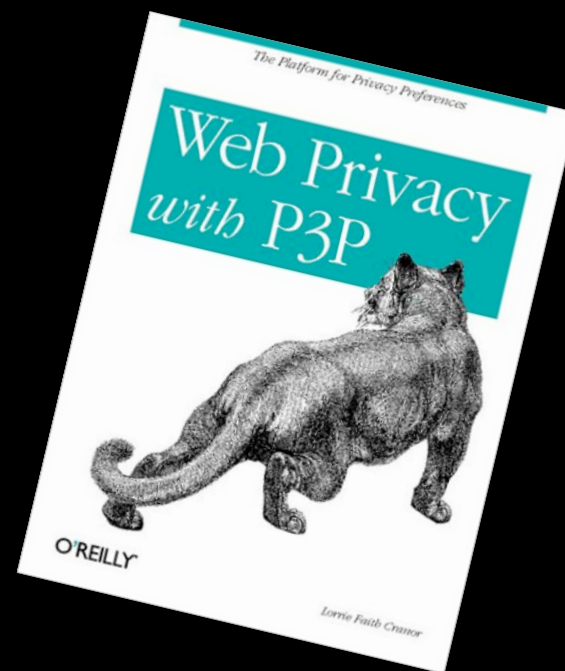
Web site privacy policies

- 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">
```

P3P version

```
<POLICY discuri="http://p3pbook.com/privacy.html"  
  name="policy">
```

Location of
human-readable
privacy policy

```
<ENTITY>
```

P3P policy name

```
<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 disclosure

```
<ACCESS><nonident/></ACCESS>
```

Human-readable
explanation

```
<STATEMENT>
```

```
<CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
```

```
<PURPOSE><admin/><current/><develop/></PURPOSE>
```

How data may
be used

```
<RECIPIENT><ours/></RECIPIENT>
```

Data recipients

```
<RETENTION><indefinitely/></RETENTION>
```

Data retention policy

```
<DATA-GROUP>
```

```
<DATA ref="#dynamic.clickstream"/>
```

```
<DATA ref="#dynamic.http"/>
```

Types of data collected

```
</DATA-GROUP>
```

```
</STATEMENT>
```

```
</POLICY>
```

```
</POLICIES>
```

Site's
name
and
contact
info

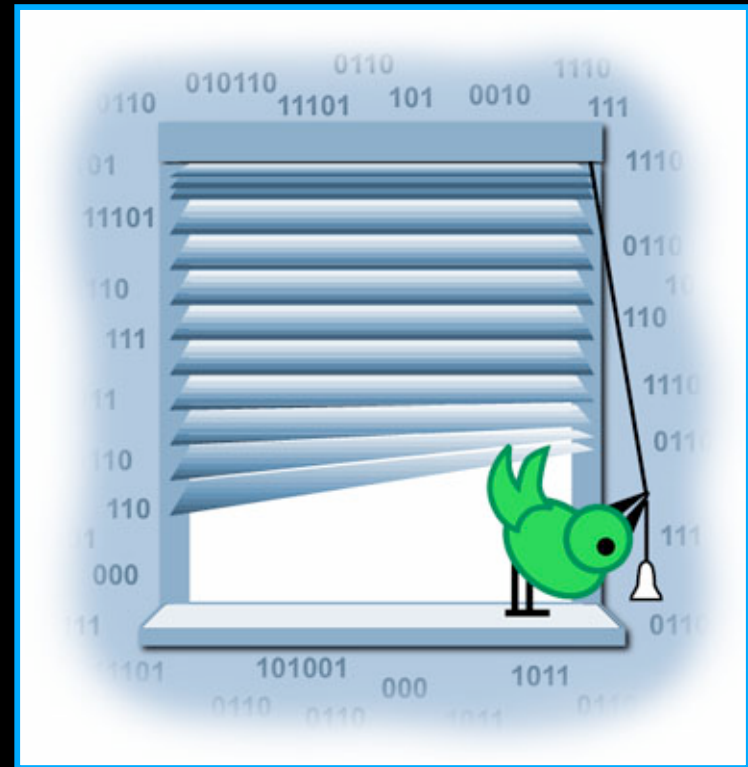
Statement

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 Forward Stop Home Search Favorites Media Print

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 Forward Stop Home Search Favorites Media Print

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

Shane Zachary



Shane's Photo Album

- [Shane's First Year](#)
- [Shane's Second Year](#)
- [Shane at 24-25 Months](#)
- [Shane at 26-27 Months](#)

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:

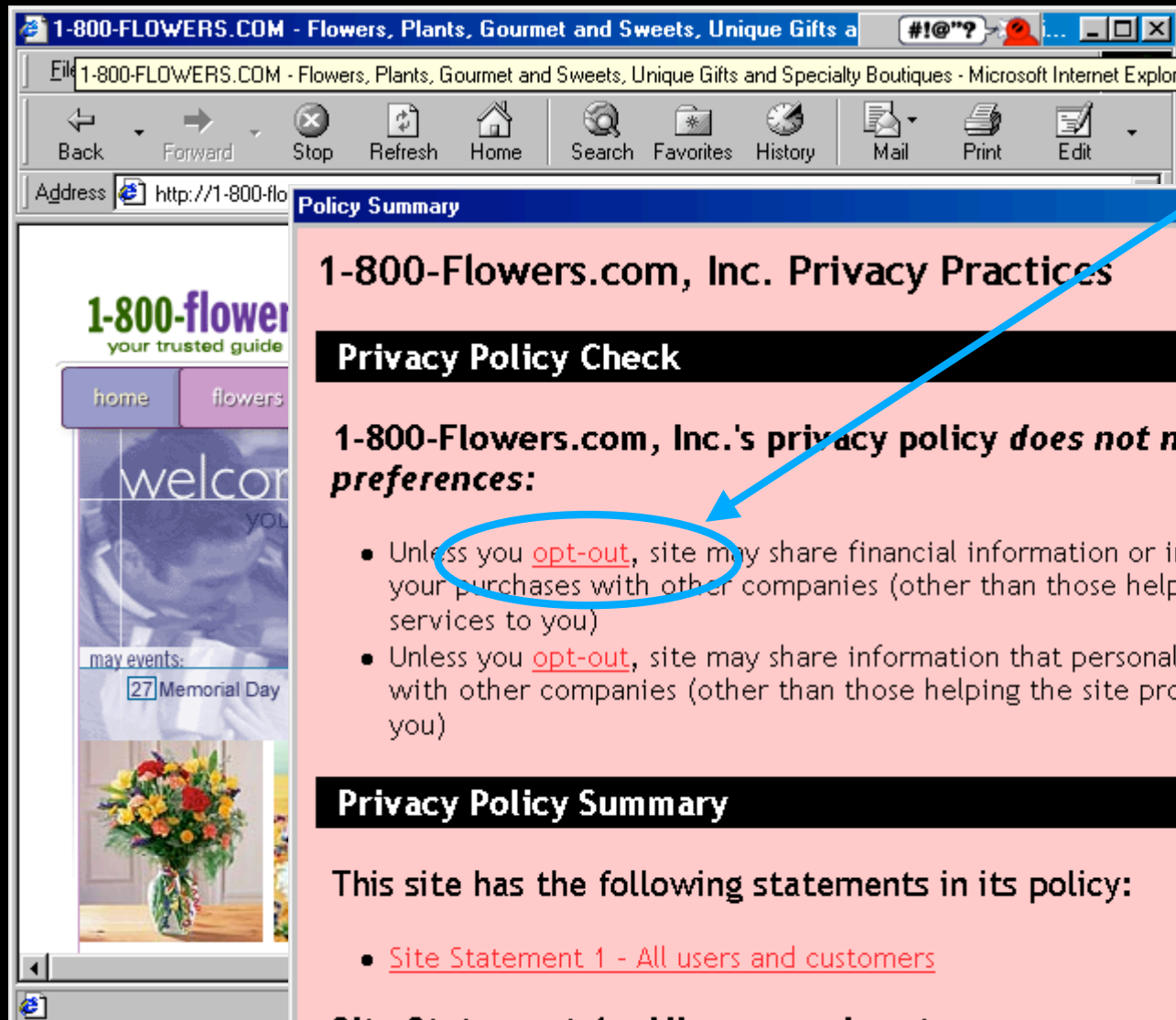
- HTTP protocol information
- Click-stream information

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

1-800-Flowers.com, Inc. Privacy Practices

Privacy Policy Check

1-800-Flowers.com, Inc.'s privacy policy does not match your preferences:

- Unless you [opt-out](#), site may share financial information or information about your purchases with other companies (other than those helping the site provide services to you)
- Unless you [opt-out](#), site may share information that personally identifies you with other companies (other than those helping the site provide services to you)

Privacy Policy Summary

This site has the following statements in its policy:

- [Site Statement 1 - All users and customers](#)

Site Statement 1 - All users and customers

Types of Information Collected:


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

P3P enabled Google Search for: send flowers

http://err.cos.cs.cmu.edu/p3psear Google

Maps Weather 15217 P3P MyAndrew MyWay Apple Amazon News CMU



P3P enabled Google Search ...





send flowers P3P Google Search Preference Level: ○ ● ○ ○

Change Google API Key

One search today using this Google API key.



  [Send Fresh FLOWERS 35% - 55% OFF](#)

www.flower-delivery-flowers.com/ - 33k - [Cached](#) - [Similar Pages](#)
Policy retrieval time: 0 secs

  [FLOWERS FLORIST - Send Flowers Online at 1-800-FLORALS Florist ...](#)

Send flowers online! Award-winning online florist delivery. Same-day and next-day fresh flower delivery in the USA and Canada. Order flowers, roses ...

www.800florals.com/ - 44k - [Cached](#) - [Similar Pages](#)
Policy retrieval time: 0 secs

  [1-800-FLOWERS.COM, welcome to our store](#)

1-800-FLOWERS.COM, welcome to our store.

www.1800flowers.com/ - 2k - [Cached](#) - [Similar Pages](#)
Policy retrieval time: 1 secs

[FTD.COM - Welcome to FTD.COM - Flower Bouquets and Gifts for All ...](#)

FTD.COM - Same day delivery of flower arrangements, roses, bouquets, plants and other gifts for anniversaries, birthdays, new babies, housewarming, ...

www.ftd.com/ - 51k - [Cached](#) - [Similar Pages](#)
Policy retrieval time: 0 secs

[FLORIST FLOWERS - Florist flower delivery and Mother's Day Flowers ...](#)

Wireless privacy

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

Wall of sheep

Defcon 2001



Defcon 2004

Wall of Shame

login	pass	domain ip	application
netjam	def*****	209.50.235.72	POP3
gadakkah	str*****	204.152.184.73	POP3
crash	llo*****	81.26.109.4	POP3
poop_free9@	5d4*****	207.46.106.109	MSN Messenger
frestorm_454	6ae*****	207.46.106.68	MSN Messenger
loz	fox*****	192.168.1.5	POP3
tim_tindorides	bab*****	207.150.192.52	POP3
tim	bab*****	24.234.9.45	POP3
Webproze	900*****	209.126.160.57	HTTP
la\jpittman	Ag1*****	http://mail.national	HTTP
royceb	hlF*****	155.92.194.35	POP3
cheeps	atw*****	217.80.37.93	HTTP
4381796	ea7*****	17.112.153.35	FTP
frex	dis*****	63.226.21.145	HTTP
wunab@ptana	B0f*****	64.246.50.89	POP3
jfa	Ro5*****	129.82.103.72	POP3
takefull	vae*****	210.251.89.161	POP3 (has not learned)
janie@crazylinux	net - Do not hire to test your security		

Peripheral display

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



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.”

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

security controls they can understand
privacy they can control



CMU Usable Privacy and Security Laboratory
<http://cups.cs.cmu.edu/>

CarnegieMellon