W3C, P3P & DNT

Lorrie Faith Cranor

October 2, 2014

8-533 / 8-733 / 19-608 / 95-818:
Privacy Policy, Law, and Technology

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

Today's agenda

- Quiz
- What's on the midterm?
- Lots of TLAs
  - W3C
  - P3P
  - DNT

By the end of class you will be able to:

- Understand what W3C is and what it does, and how to read a W3C specification
- Understand the history of of P3P
- Understand the major components of P3P
- Understand the history and current status of DNT

W3C

- International member organization
- Founded in 1994 by Web inventor Tim Berners-Lee
- Mission: Lead the web to its full potential
- Most work revolves around standardization of web technologies
  - Structured process for developing standards
  - Working drafts -> Last call ->
Candidate Recommendation ->
Proposed Recommendation -> Recommendation

Original Idea behind P3P

- A framework for automated privacy discussions
  - Web sites disclose their privacy practices in standard machine-readable formats
  - Web browsers automatically retrieve P3P privacy policies and compare them to users' privacy preferences
  - Sites and browsers can then negotiate about privacy terms

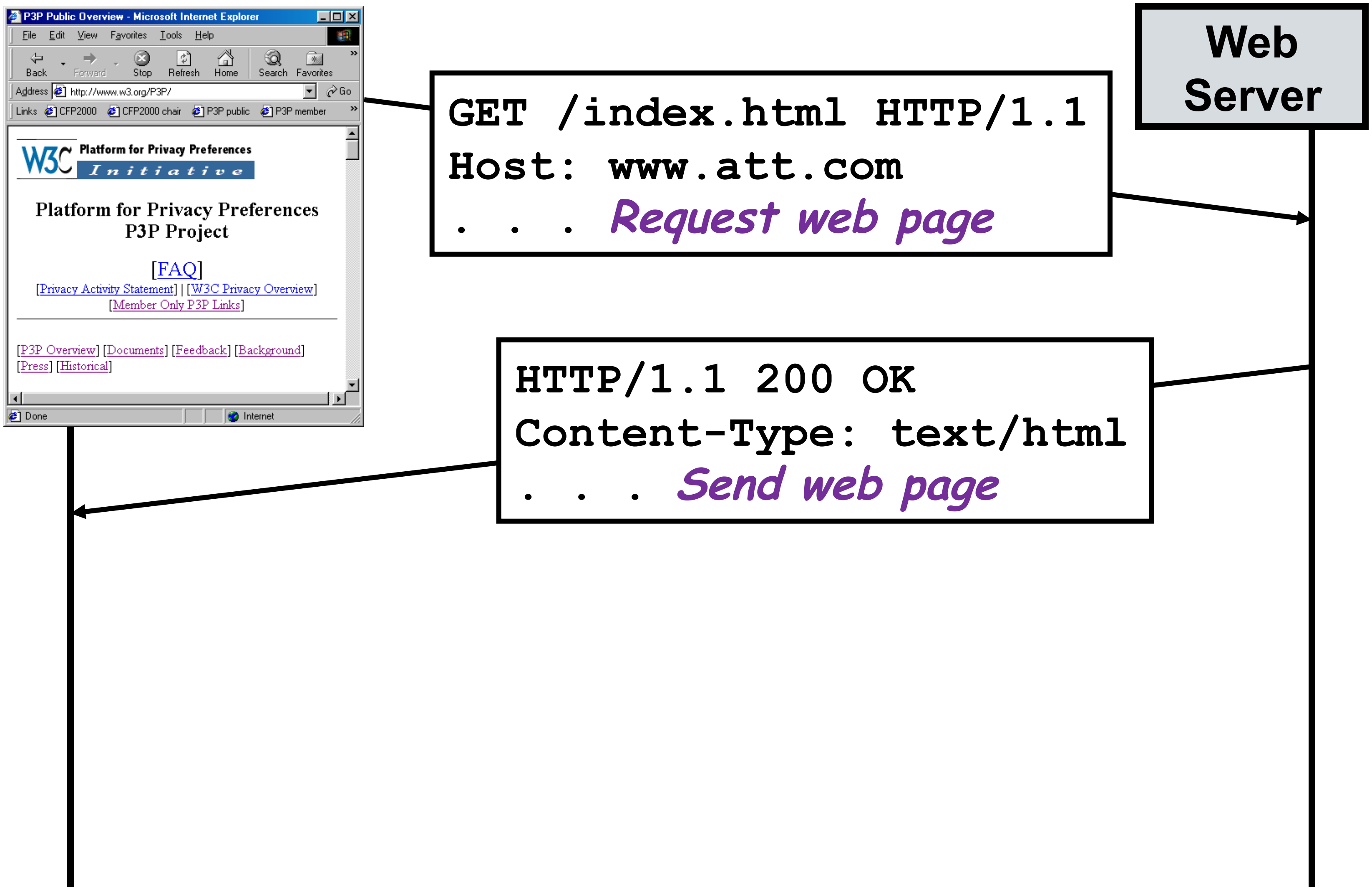
P3P history

- November 1995 - Idea discussed at FTC meeting
- Fall 1996 - Ad Hoc “Internet Privacy Working Group” convened
- Summer 1997 - W3C began working on P3P
  - Several working groups chartered with dozens of participants from industry, non-profits, academia, government
  - Numerous public working drafts issued, many changes
  - Early ideas about negotiation and agreement ultimately removed
  - Automatic data transfer added and then removed
  - Patent issue stalled progress, but ultimately became non-issue
- April 16, 2002 - P3P issued as official W3C Recommendation http://www.w3.org/TR/P3P/
- 2012 – Microsoft complains that companies are circumventing P3P

P3P1.0 Spec

- A standard vocabulary for describing set of uses, recipients, data categories, and other privacy disclosures
- A standard schema for data a Web site may wish to collect (base data schema)
- An XML format for expressing a privacy policy in a machine readable way
- A means of associating privacy policies with Web pages or sites
- A protocol for transporting P3P policies over HTTP
  - A format for expressing optional P3P compact policy headers

A simple HTTP transaction



P3P Public Overview - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites
Address http://www.w3.org/P3P/
Go
Links CFP2000 CFP2000 chair P3P public P3P member
W3C Platform for Privacy Preferences Initiative
Done
Internet
Web Server

Platform for Privacy Preferences
P3P Project

[FAQ]
[Privacy Activity Statement] | [W3C Privacy Overview]
[Member Only P3P Links]

[P3P Overview] [Documents] [Feedback] [Background]
[Press] [Historical]

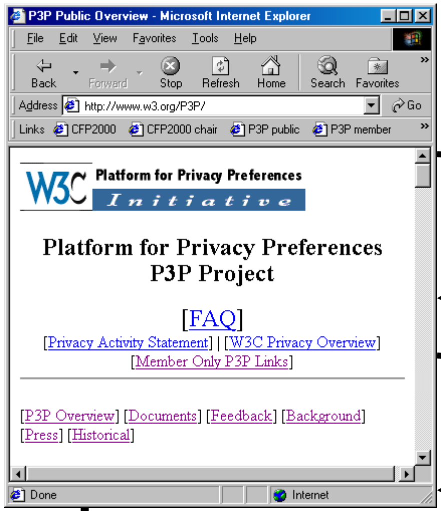
```
GET /index.html HTTP/1.1
Host: www.att.com
. . .
```

Request web page

```
HTTP/1.1 200 OK
Content-Type: text/html
. . .
```

Send web page

… with P3P 1.0 added


P3P Public Overview - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites
Address
Go
Links CFP2000 CFP2000 chair P3P public P3P member
Done
Internet

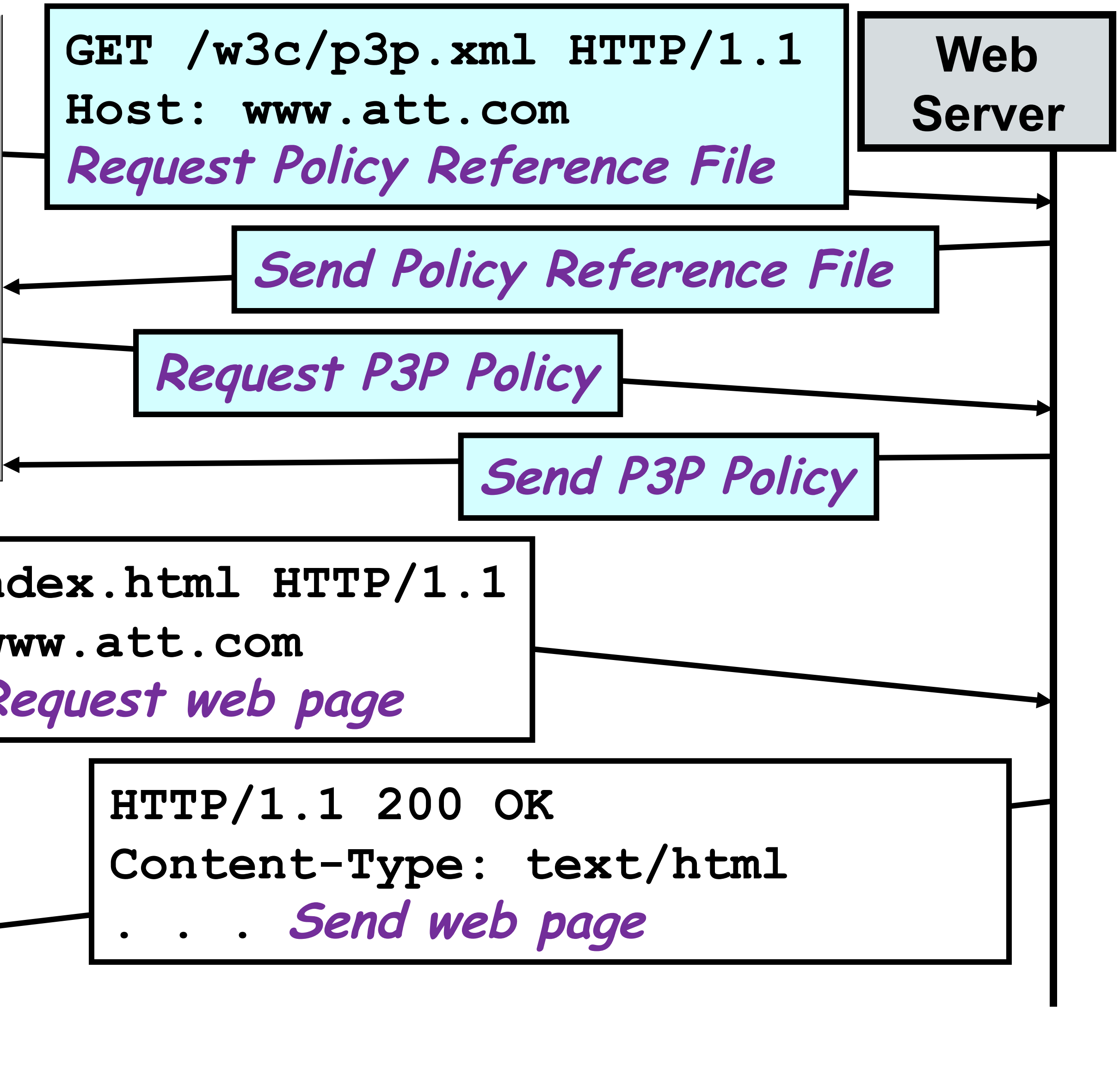
http://www.w3.org/P3P/

Platform for Privacy Preferences Initiative

Platform for Privacy Preferences
P3P Project

[FAQ]
[Privacy Activity Statement] | [W3C Privacy Overview]
[Member Only P3P Links]

[P3P Overview] [Documents] [Feedback] [Background]
[Press] [Historical]



Web Server

```
GET /w3c/p3p.xml HTTP/1.1
Host: www.att.com
```
Request Policy Reference File

Send Policy Reference File

Request P3P Policy

Send P3P Policy

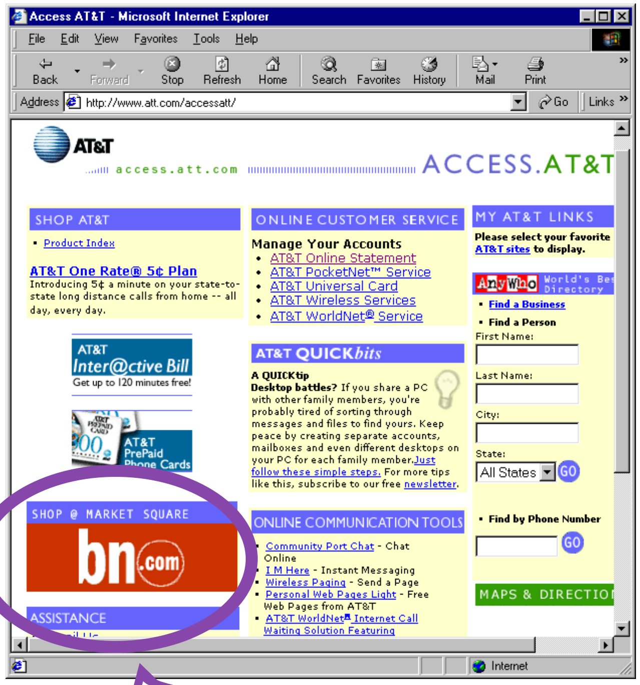
```
GET /index.html HTTP/1.1
Host: www.att.com
. . .
```
Request web page

```
HTTP/1.1 200 OK
Content-Type: text/html
. . .
```
Send web page

Transparency

- P3P clients can check a privacy policy each time it changes
- P3P clients can check privacy policies on all objects in a web page, including ads and invisible images

http://www.att.com/accessatt/



- Product Index

AT&T One Rate® 5¢ Plan
Introducing 5¢ a minute on your state-to-state long distance calls from home -- all day, every day.

Get up to 120 minutes free!

Manage Your Accounts

- AT&T Online Statement
- AT&T PocketNet™ Service
- AT&T Universal Card
- AT&T Wireless Services
- AT&T WorldNet® Service

A QUICKtip
Desktop battles? If you share a PC with other family members, you're probably tired of sorting through messages and files to find yours. Keep peace by creating separate accounts, mailboxes and even different desktops on your PC for each family member. Just follow these simple steps. For more tips like this, subscribe to our free newsletter.

- Community Port Chat - Chat Online
- I M Here - Instant Messaging
- Wireless Paging - Send a Page
- Personal Web Pages Light - Free Web Pages from AT&T
- AT&T WorldNet® Internet Call Waiting Solution Featuring

Please select your favorite AT&T sites to display.

- **Find a Business**
- **Find a Person**

First Name:

Last Name:

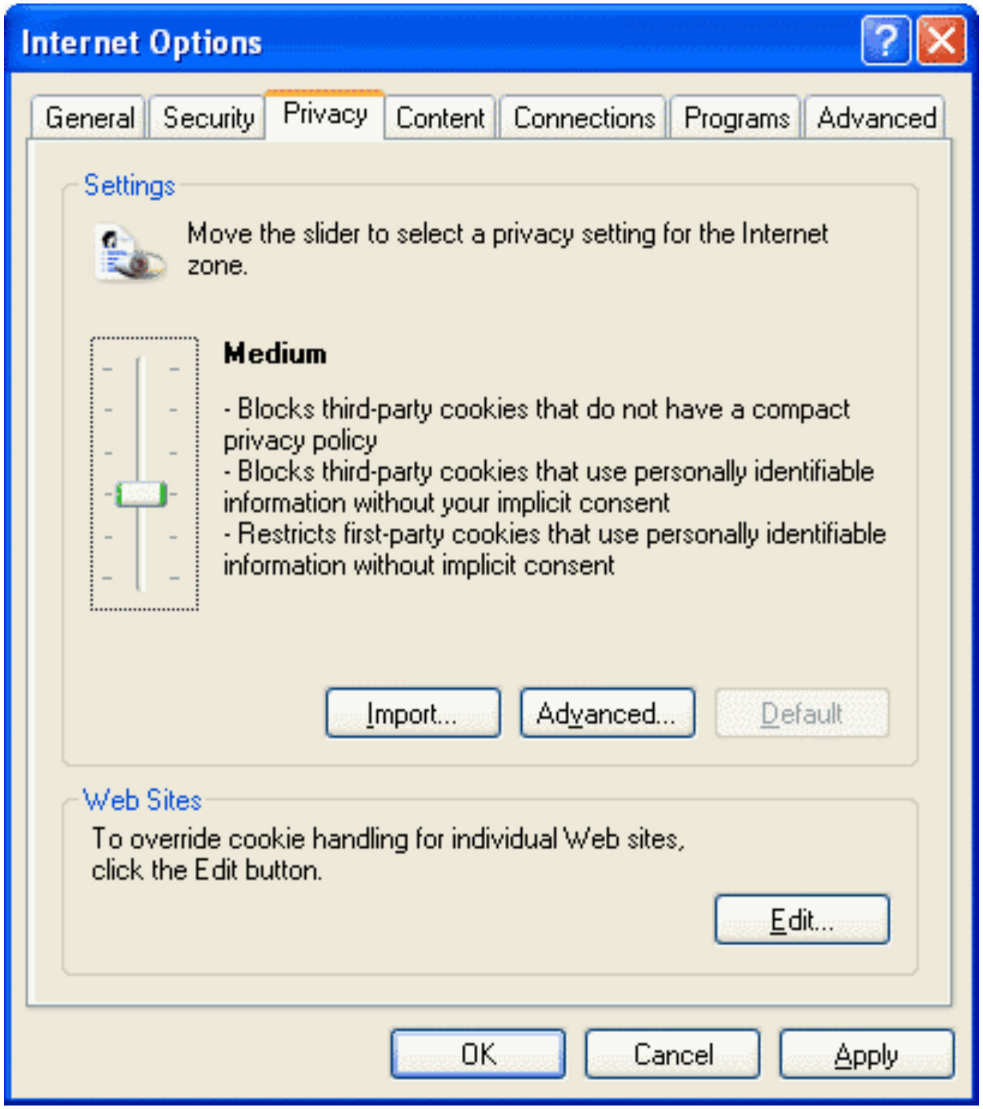
City:

State: All States

- **Find by Phone Number**

http://adforce.imgis.com/?adlink|2|68523|1|146|ADFORCE

P3P in IE6



Settings

Move the slider to select a privacy setting for the Internet zone.

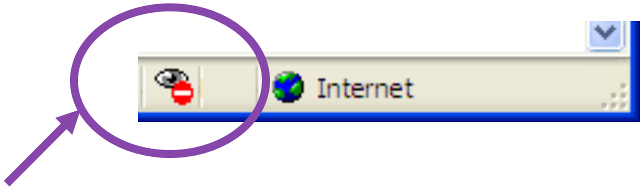
Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

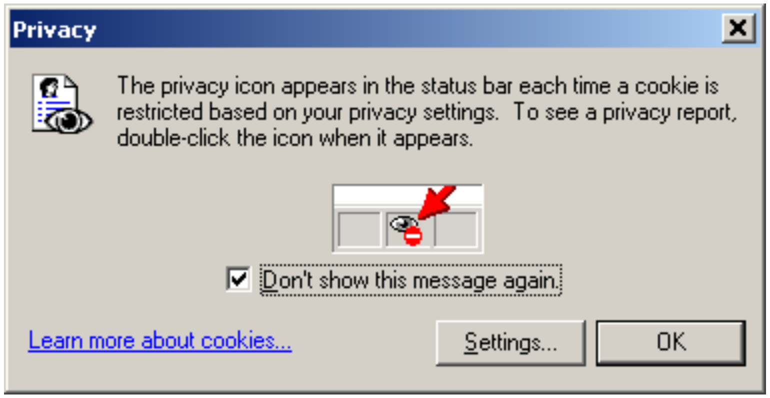
Web Sites

To override cookie handling for individual Web sites, click the Edit button.

Automatic processing of compact policies only; third-party cookies without compact policies blocked by default

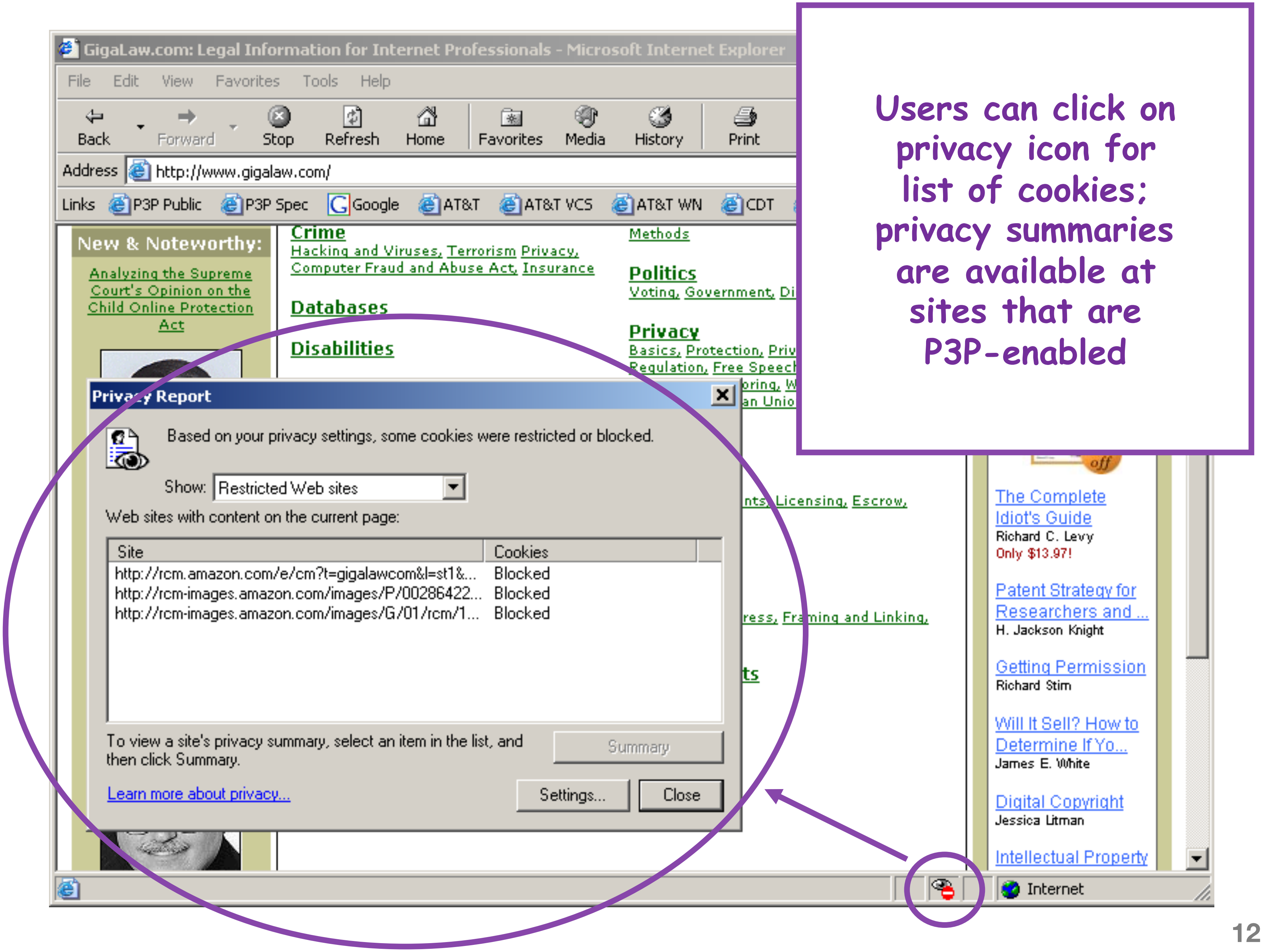


Privacy icon on status bar indicates that a cookie has been blocked – pop-up appears the first time the privacy icon appears



The privacy icon appears in the status bar each time a cookie is restricted based on your privacy settings. To see a privacy report, double-click the icon when it appears.

☑ Don't show this message again.


GigaLaw.com: Legal Information for Internet Professionals - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Favorites
Media
History
Print
Address http://www.gigalaw.com/
Links P3P Public P3P Spec Google AT&T AT&T VCS AT&T WN CDT
New & Noteworthy:
Analyzing the Supreme Court's Opinion on the Child Online Protection Act
Crime
Hacking and Viruses, Terrorism Privacy, Computer Fraud and Abuse Act, Insurance
Databases
Disabilities
Methods
Politics
Voting, Government, Di
Privacy
Basics, Protection, Priv
Regulation, Free Speech
nts, Licensing, Escrow,
ress, Framing and Linking,
ts
The Complete Idiot's Guide
Richard C. Levy
Only $13.97!
Patent Strategy for Researchers and ...
H. Jackson Knight
Getting Permission
Richard Stim
Will It Sell? How to Determine If Yo...
James E. White
Digital Copyright
Jessica Litman
Intellectual Property
Internet

Privacy Report

Based on your privacy settings, some cookies were restricted or blocked.

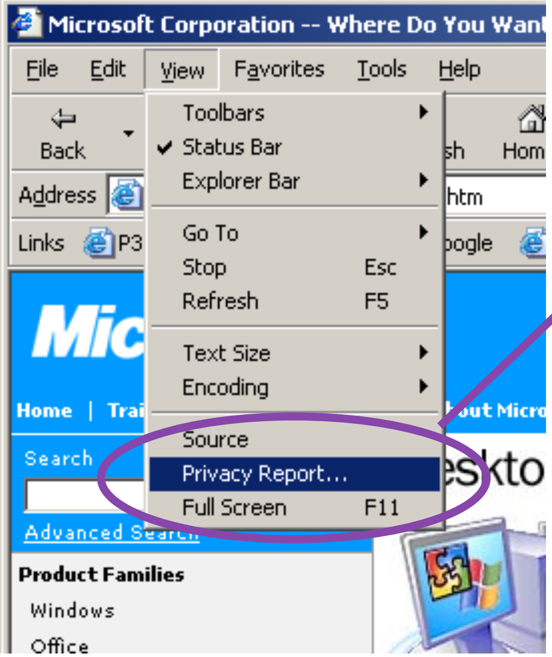
Show: Restricted Web sites

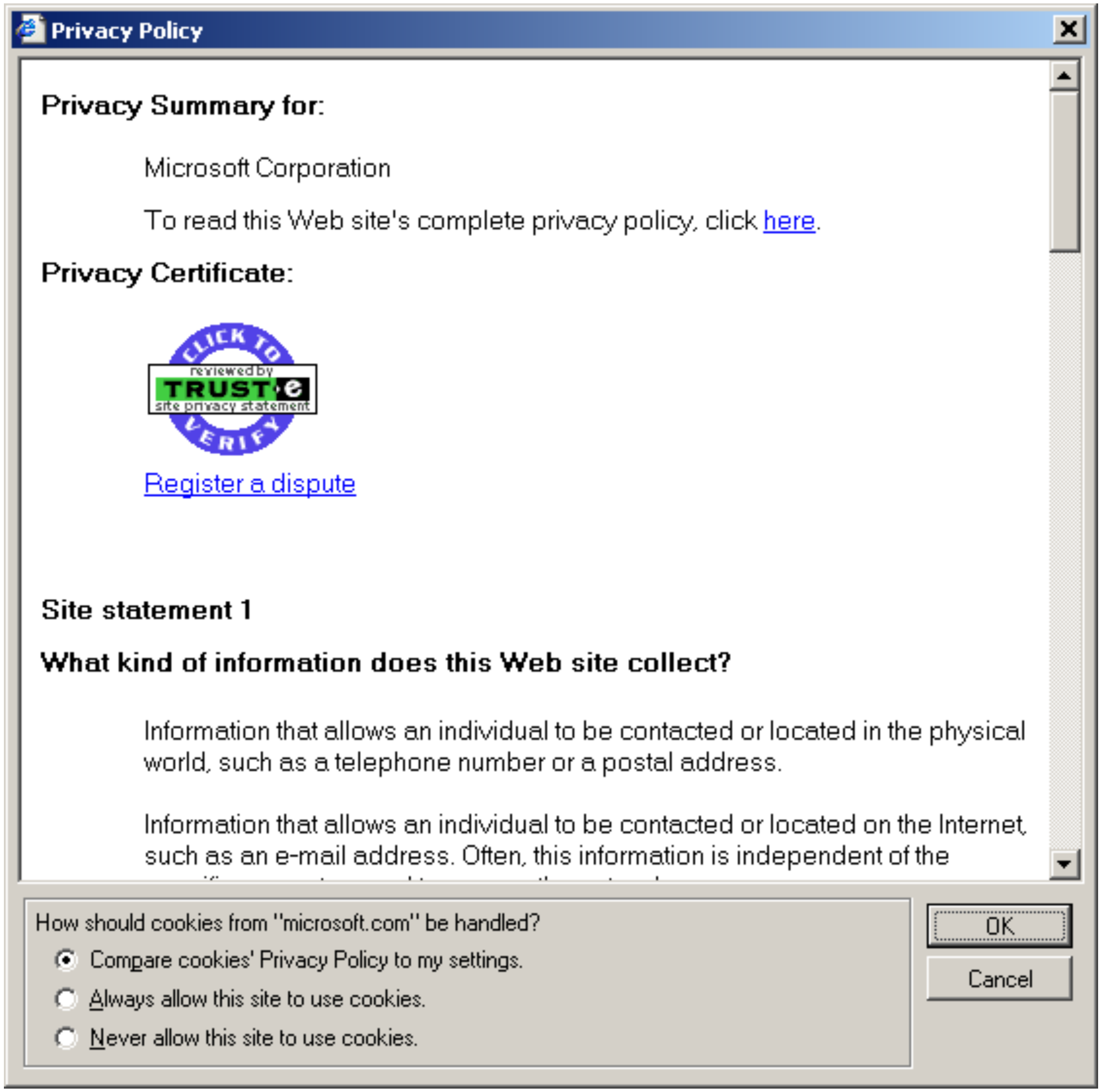
Web sites with content on the current page:

Site	Cookies
http://rcm.amazon.com/e/cm?t=gigalawcom&l=st1&...	Blocked
http://rcm-images.amazon.com/images/P/00286422...	Blocked
http://rcm-images.amazon.com/images/G/01/rcm/1...	Blocked

To view a site's privacy summary, select an item in the list, and then click Summary.

Users can click on privacy icon for list of cookies; privacy summaries are available at sites that are P3P-enabled





Privacy Summary for:

Microsoft Corporation

To read this Web site's complete privacy policy, click here.

Privacy Certificate:

Register a dispute

Site statement 1

What kind of information does this Web site collect?

Information that allows an individual to be contacted or located in the physical world, such as a telephone number or a postal address.

Information that allows an individual to be contacted or located on the Internet, such as an e-mail address. Often, this information is independent of the

How should cookies from "microsoft.com" be handled?

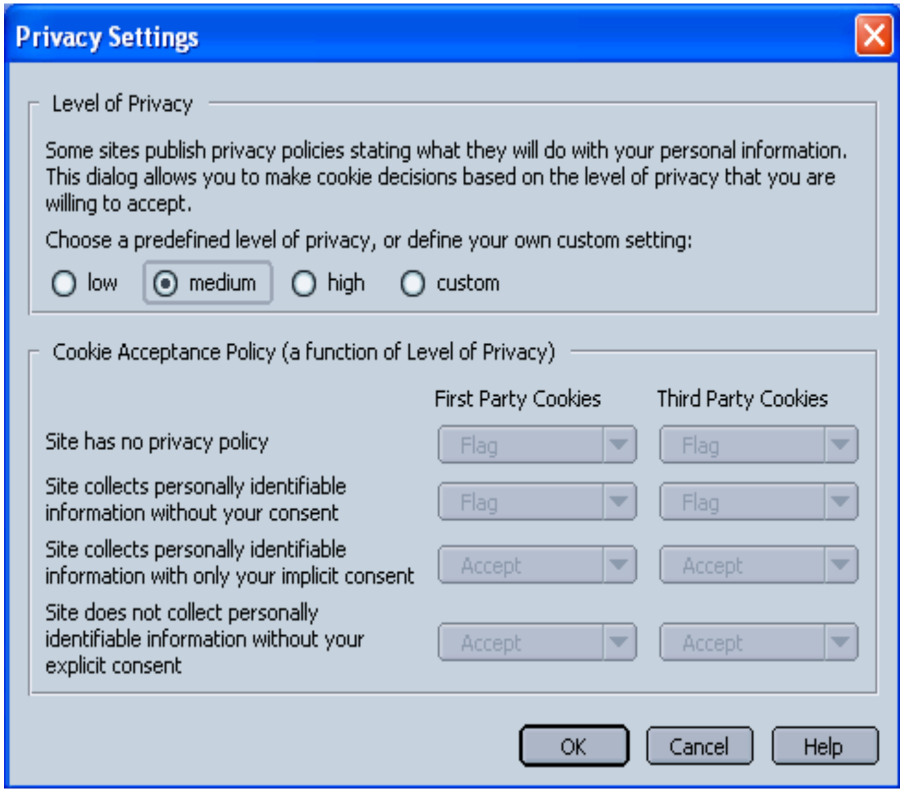
● Compare cookies' Privacy Policy to my settings.

○ Always allow this site to use cookies.

○ Never allow this site to use cookies.

Privacy summary report is generated automatically from full P3P policy

P3P in Netscape 7



Privacy Settings

Level of Privacy

Some sites publish privacy policies stating what they will do with your personal information. This dialog allows you to make cookie decisions based on the level of privacy that you are willing to accept.

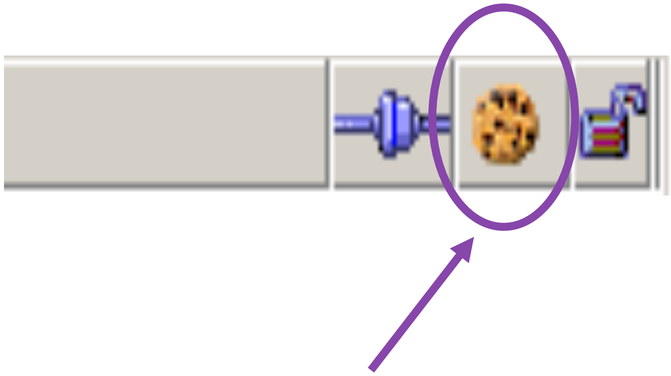
Choose a predefined level of privacy, or define your own custom setting:

○ low ● medium ○ high ○ custom

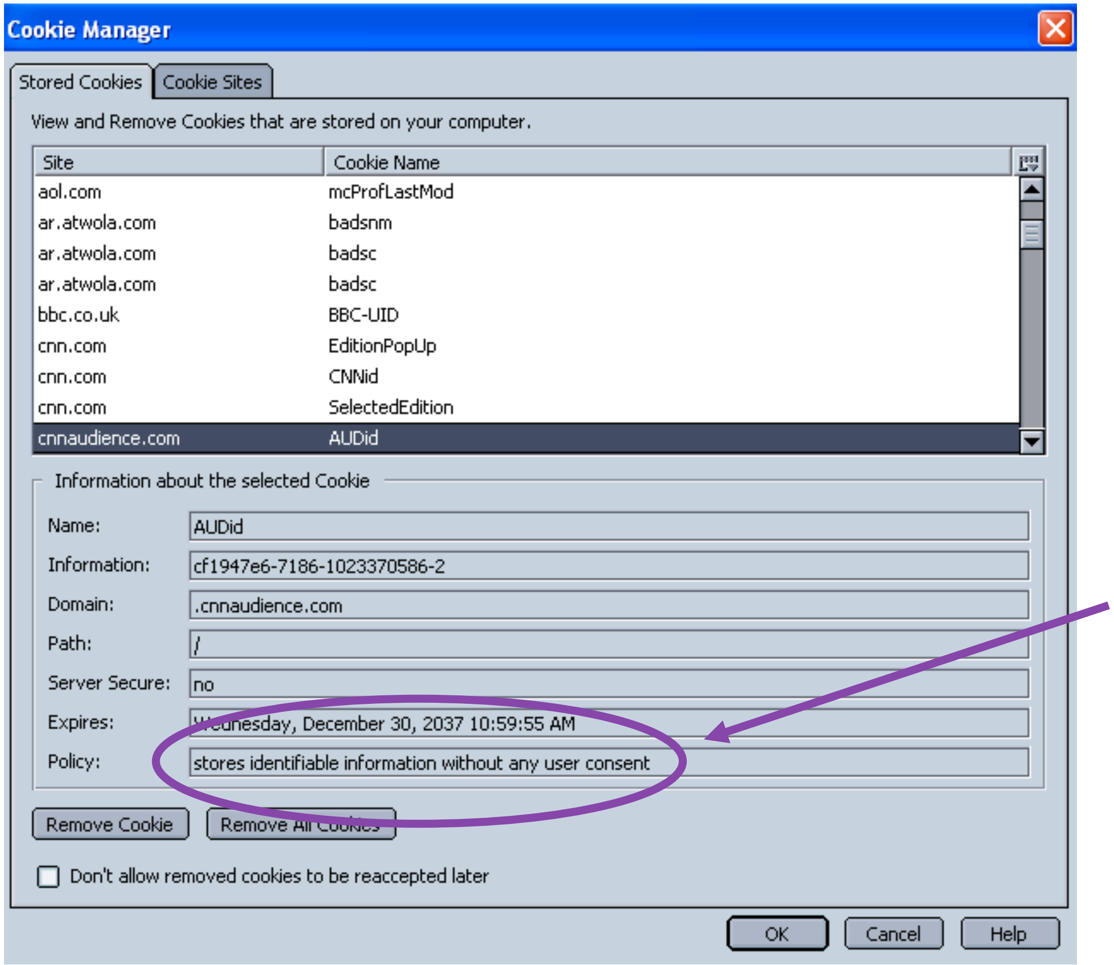
Cookie Acceptance Policy (a function of Level of Privacy)

	First Party Cookies	Third Party Cookies
Site has no privacy policy	Flag	Flag
Site collects personally identifiable information without your consent	Flag	Flag
Site collects personally identifiable information with only your implicit consent	Accept	Accept
Site does not collect personally identifiable information without your explicit consent	Accept	Accept

Preview version similar to IE6, focusing, on cookies; cookies without compact policies (both first-party and third-party) are "flagged" rather than blocked by default



Indicates flagged cookie



View and Remove Cookies that are stored on your computer.

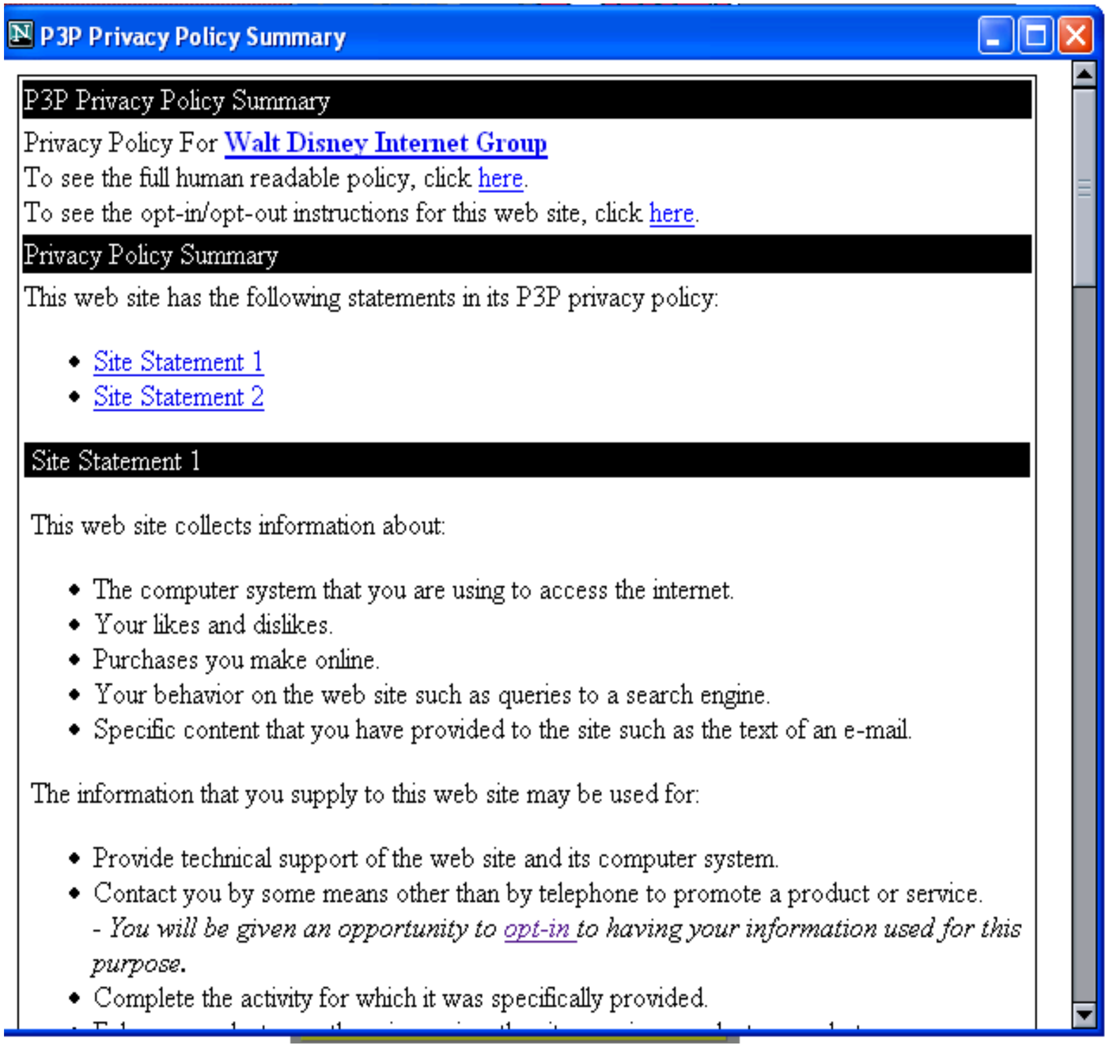
Site	Cookie Name
aol.com	mcProfLastMod
ar.atwola.com	badsnm
ar.atwola.com	badsc
ar.atwola.com	badsc
bbc.co.uk	BBC-UID
cnn.com	EditionPopUp
cnn.com	CNNid
cnn.com	SelectedEdition
cnnaudience.com	AUDid

Information about the selected Cookie

Name:	AUDid
Information:	cf1947e6-7186-1023370586-2
Domain:	.cnnaudience.com
Path:	/
Server Secure:	no
Expires:	Wednesday, December 30, 2037 10:59:55 AM
Policy:	stores identifiable information without any user consent

□ Don't allow removed cookies to be reaccepted later

Users can view English translation of (part of) compact policy in Cookie Manager



P3P Privacy Policy Summary

Privacy Policy For **Walt Disney Internet Group**

To see the full human readable policy, click here.

To see the opt-in/opt-out instructions for this web site, click here.

Privacy Policy Summary

This web site has the following statements in its P3P privacy policy:

- Site Statement 1
- Site Statement 2

Site Statement 1

This web site collects information about:

- The computer system that you are using to access the internet.
- Your likes and dislikes.
- Purchases you make online.
- Your behavior on the web site such as queries to a search engine.
- Specific content that you have provided to the site such as the text of an e-mail.

The information that you supply to this web site may be used for:

- Provide technical support of the web site and its computer system.
- Contact you by some means other than by telephone to promote a product or service.
  - *You will be given an opportunity to opt-in to having your information used for this purpose.*
- Complete the activity for which it was specifically provided.

A policy summary can be generated automatically from full P3P policy

What’s in a P3P policy?

- Name and contact information for site
- The kind of access provided
- Mechanisms for resolving privacy disputes
- The kinds of data collected
- How collected data is used, and whether individuals can opt-in or opt-out of any of these uses
- Whether/when data may be shared and whether there is opt-in or opt-out
- Data retention policy

Assertions in a P3P policy

- General assertions
  - Location of human-readable policies and opt-out mechanisms – discuri, opturi attributes of <POLICY>
  - Indication that policy is for testing only – <TEST> (optional)
  - Web site contact information – <ENTITY>
  - Access information – <ACCESS>
  - Information about dispute resolution – <DISPUTES> (optional)
- Data-Specific Assertions
  - Consequence of providing data – <CONSEQUENCE> (optional)
  - Indication that no identifiable data is collected – <NON-IDENTIFIABLE> (optional)
  - How data will be used – <PURPOSE>
  - With whom data may be shared – <RECIPIENT>
  - Whether opt-in and/or opt-out is available – required attribute of <PURPOSE> and <RECIPIENT>
  - Data retention policy – <RETENTION>
  - What kind of data is collected – <DATA>

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

Why web sites adopt P3P

- Demonstrate corporate leadership on privacy issues
  - Show customers they respect their privacy
  - Demonstrate to regulators that industry is taking voluntary steps to address consumer privacy concerns
- Distinguish brand as privacy friendly
- Prevent IE6 from blocking their cookies
- Anticipation that consumers will soon come to expect P3P on all web sites
- Individuals who run sites value personal privacy

P3P early adopters

- News and information sites – CNET, About.com, BusinessWeek
- Search engines – Yahoo, Lycos
- Ad networks – DoubleClick, Avenue A
- Telecom companies – AT&T
- Financial institutions – Fidelity
- Computer hardware and software vendors – IBM, Dell, Microsoft, McAfee
- Retail stores – Fortunoff, Ritz Camera
- Government agencies – FTC, Dept. of Commerce, Ontario Information and Privacy Commissioner
- Non-profits - CDT

Web site adoption of P3P

- AT&T study surveyed 5,856 websites in 2003, found 538 P3P policies
  - Adoption highest among popular websites (~30% of top 100 sites)
  - Web site adoption increasing slowly, but steadily
  - Low adoption for government sites – but changed with new regulations
- Large number of P3P policies contain technical errors
  - Most errors due to old version of P3P spec or minor technical issues
  - 7% have severe errors such as missing required components

Byers, S., Cranor, L. F., and Kormann, D. 2003. Automated analysis of P3P-enabled Web sites. ICEC '03, vol. 50. ACM Press, New York, NY, 326-338. DOI= http://doi.acm.org/10.1145/948005.948048

Legal issues

- P3P specification does not address legal standing of P3P policies or include enforcement mechanisms
- P3P specification requires P3P policies to be consistent with natural-language privacy policies
  - P3P policies and natural-language policies are not required to contain same level of detail
  - Typically natural-language policies contain more detailed explanations
- In some jurisdictions, regulators and courts may treat P3P policies equivalently to natural language privacy policies
- The same attorneys and policy makers involved in drafting natural-language policy should help create P3P policy

Privacy policy	P3P policy
Designed to be read by a human	Designed to be read by a computer
Can contain fuzzy language with “wiggle room”	Mostly multiple choice – sites must place themselves in one “bucket” or another
Can include as much or as little information as a site wants	Must include disclosures in every required area
Easy to provide detailed explanations	Limited ability to provide detailed explanations
Sometimes difficult for users to determine boundaries of what it applies to and when it might change	Precisely scoped
Web site controls presentation	User agent controls presentation

P3P Interface design challenges

- P3P 1.0 specification focuses on interoperability, says little about user interface
  - P3P 1.1 spec will provide explanations of P3P vocabulary elements suitable for display to end users
- P3P user agents typically need user interfaces for:
  - informing users about web site privacy policies
  - configuring the agent to take actions on the basis of a user's privacy preferences

Informing users about privacy is difficult

- Privacy policies are complex
  - Over 36K combinations of P3P “multiple choice” elements
- Users are generally unfamiliar with much of the terminology used by privacy experts
- Users generally do not understand the implications of data practices
- Users are not interested in all of the detail of most privacy policies
- Which details and the level of detail each user is interested in varies

Specifying privacy preferences is difficult

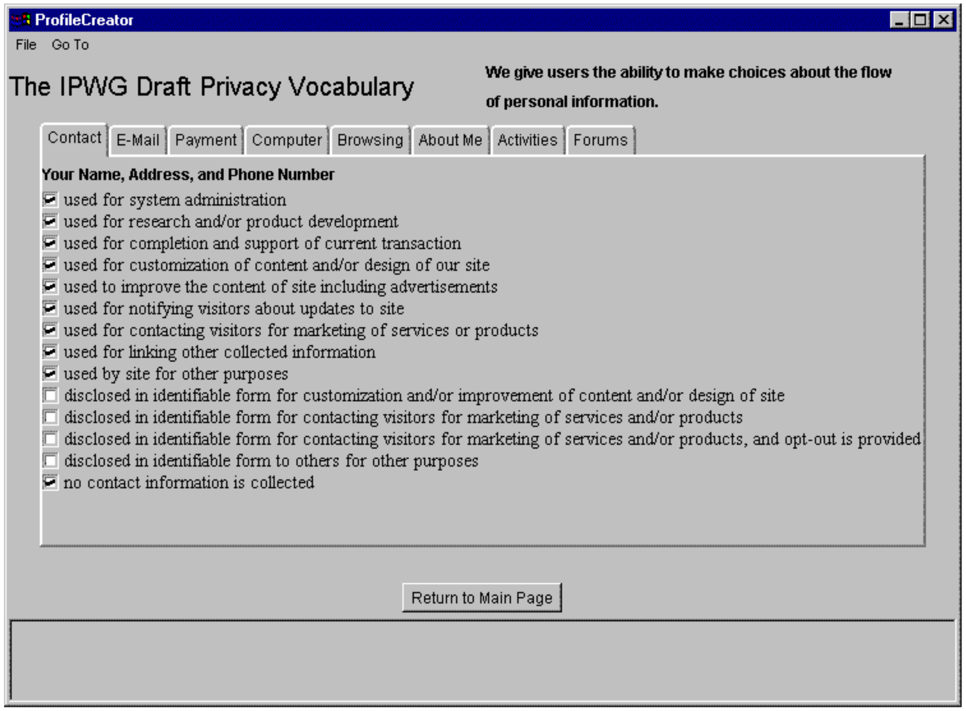
- Privacy policies are complex
- User privacy preferences are often complex and nuanced
- Users tend to have little experience articulating their privacy preferences
- Users are generally unfamiliar with much of the terminology used by privacy experts

Iterative design approach

- Four P3P user agent prototypes developed over 4-year period while P3P specification was under development
- AT&T Privacy Bird beta released Feb. 2002
  - August 2002 user study
  - Beta 1.2 released Feb. 2003

W3C prototype

- Based on pre-W3C draft of P3P vocabulary with 3 fields, 7x9x2=126 combinations of elements
- Preference interface eliminated the impractical combos, combined 2 dimensions → 7x14=98 combinations
- Matrix represented by tabbed interface
- Feedback: too complicated, too many choices



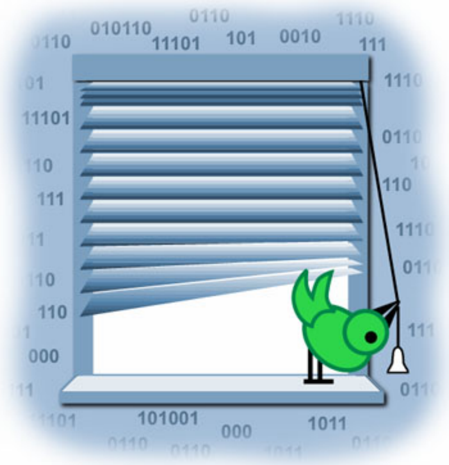
The IPWG Draft Privacy Vocabulary

We give users the ability to make choices about the flow of personal information.

Your Name, Address, and Phone Number

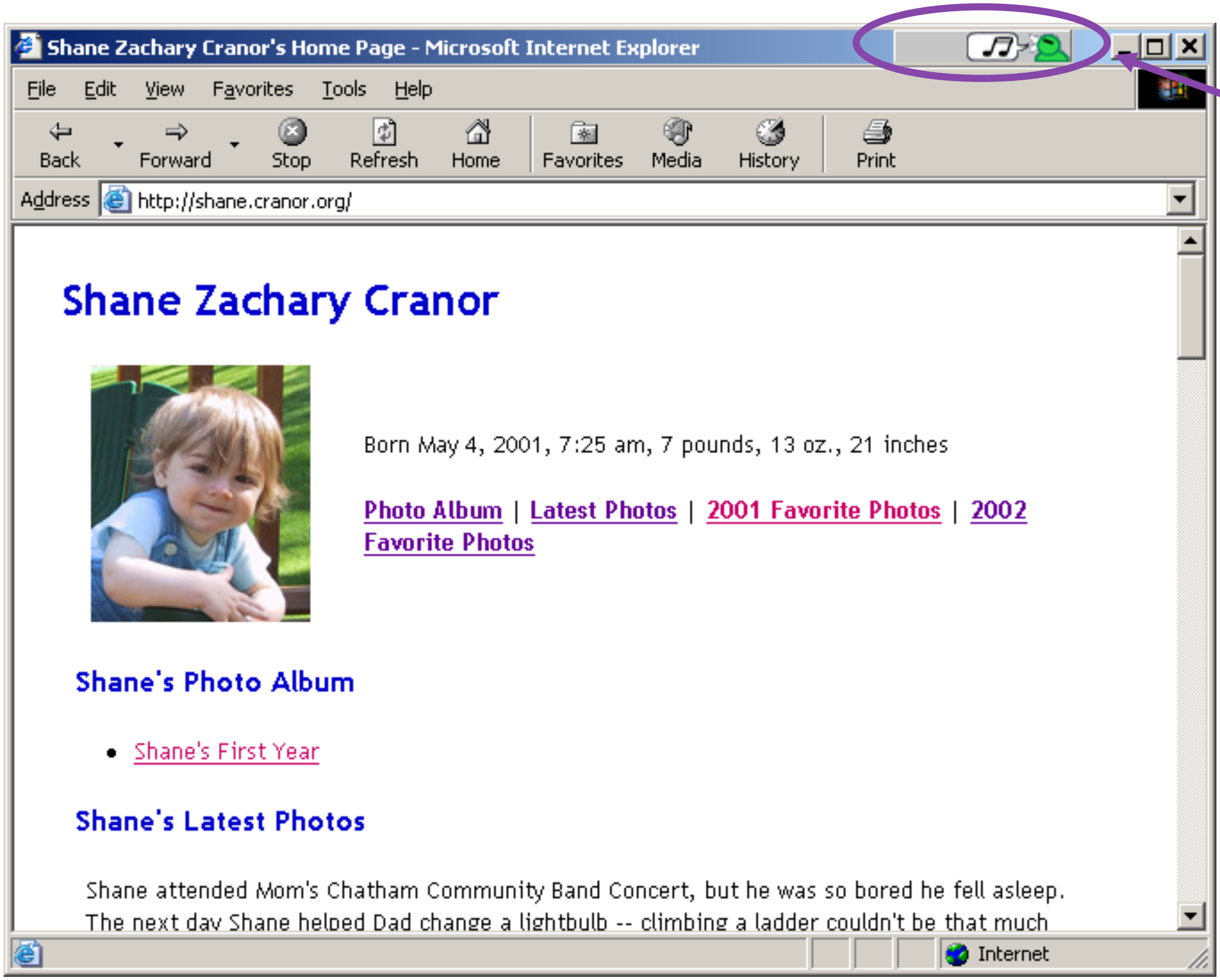
☑ used for system administration
☑ used for research and/or product development
☑ used for completion and support of current transaction
☑ used for customization of content and/or design of our site
☑ used to improve the content of site including advertisements
☑ used for notifying visitors about updates to site
☑ used for contacting visitors for marketing of services or products
☑ used for linking other collected information
☑ used by site for other purposes
☐ disclosed in identifiable form for customization and/or improvement of content and/or design of site
☐ disclosed in identifiable form for contacting visitors for marketing of services and/or products
☐ disclosed in identifiable form for contacting visitors for marketing of services and/or products, and opt-out is provided
☐ disclosed in identifiable form to others for other purposes
☑ no contact information is collected

AT&T Privacy Bird



- Free download of beta from http://privacybird.com/
- “Browser helper object” for IE 5.01/5.5/6.0
- Reads P3P policies at all P3P-enabled sites automatically
- Puts bird icon at top of browser window that changes to indicate whether site matches user’s privacy preferences
- Clicking on bird icon gives more information
- Current version is information only – no cookie blocking

Chirping bird is privacy indicator


Shane Zachary Cranor's Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Favorites Media History Print
Address http://shane.cranor.org/
Internet

Shane Zachary Cranor

Born May 4, 2001, 7:25 am, 7 pounds, 13 oz., 21 inches

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

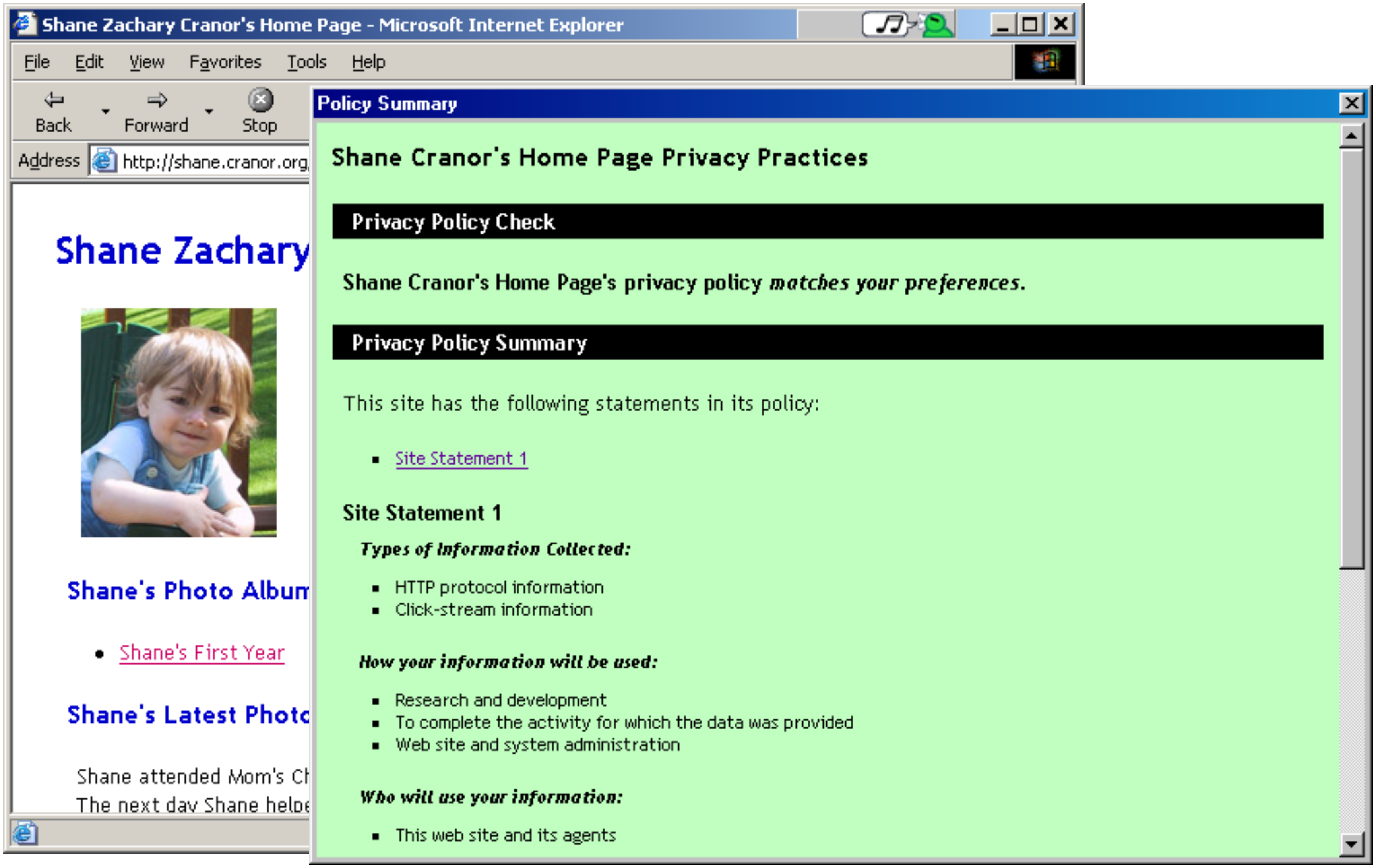
Shane's Photo Album

- Shane's First Year

Shane's Latest Photos

Shane attended Mom's Chatham Community Band Concert, but he was so bored he fell asleep. The next day Shane helped Dad change a lightbulb -- climbing a ladder couldn't be that much

Click on the bird for more info



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

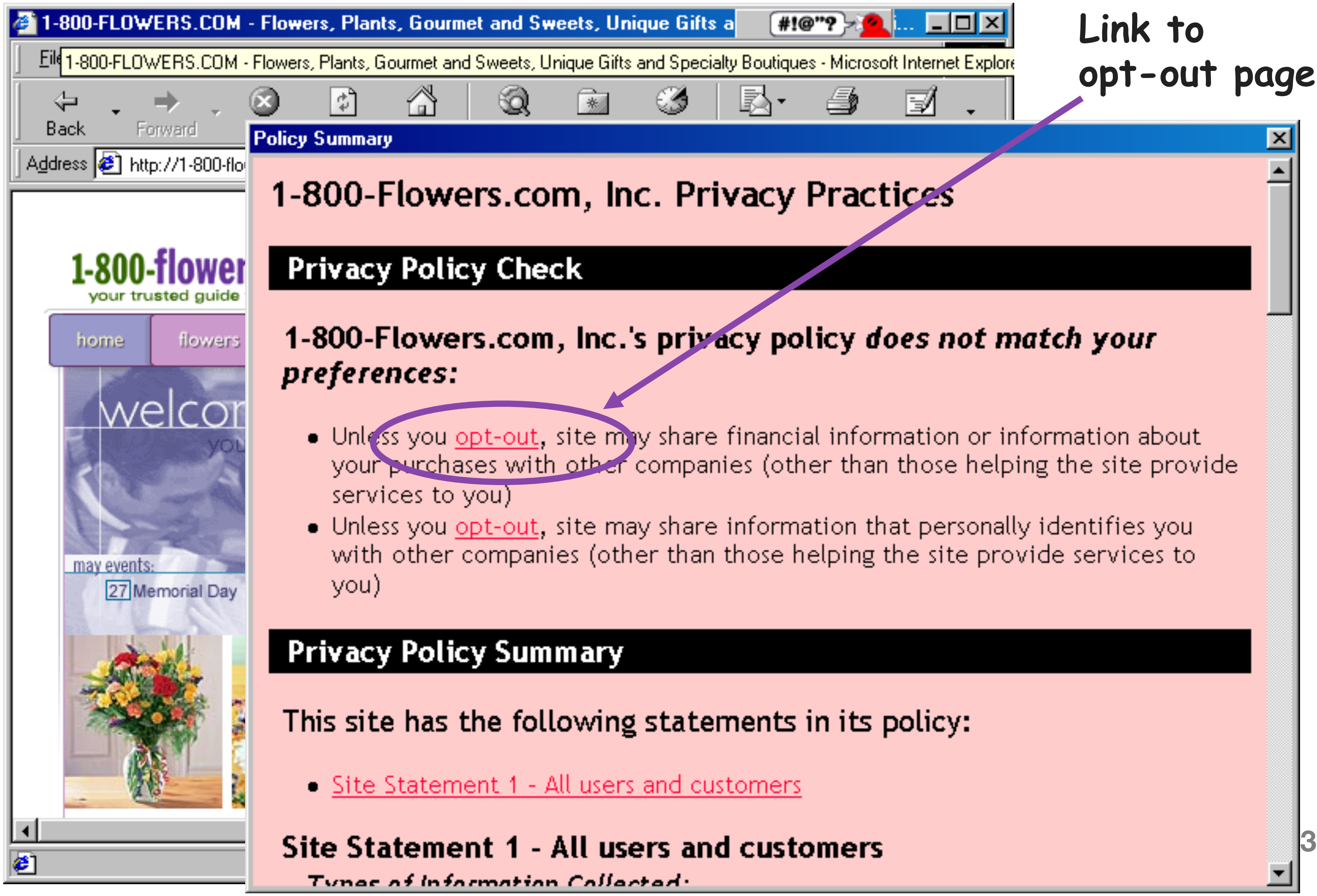
How your information will be used:

- 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

Privacy policy summary - mismatch


1-800-FLOWERS.COM - Flowers, Plants, Gourmet and Sweets, Unique Gifts a
#!@"?
File
1-800-FLOWERS.COM - Flowers, Plants, Gourmet and Sweets, Unique Gifts and Specialty Boutiques - Microsoft Internet Explore
Back
Forward
Address
http://1-800-flo
1-800-flower
your trusted guide
home
flowers
welcor
you
may events:
27 Memorial Day
Policy Summary

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:

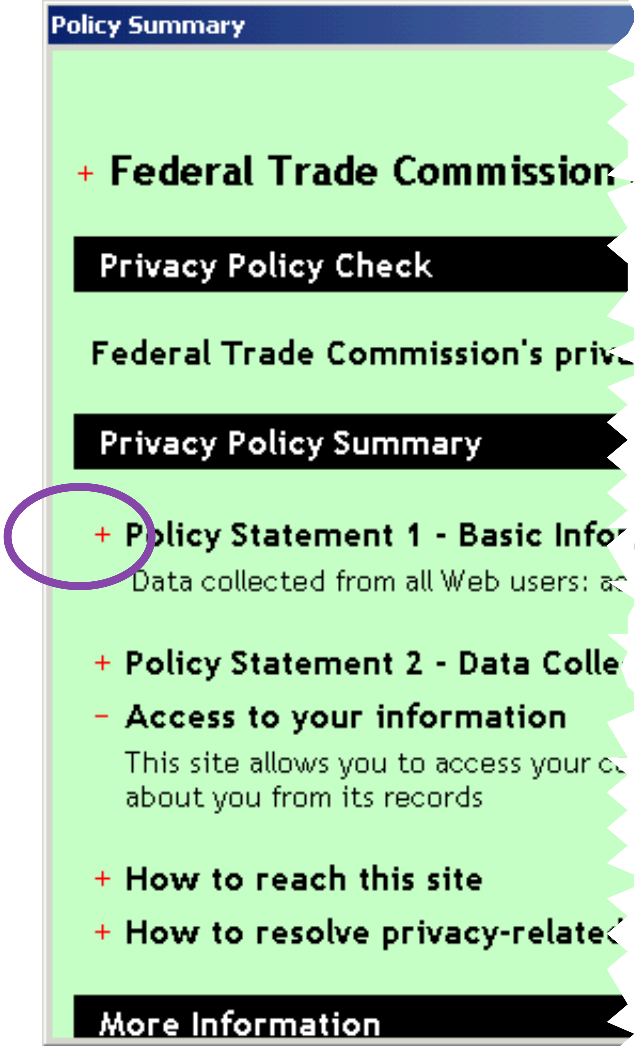
- Site Statement 1 - All users and customers

Site Statement 1 - All users and customers

Types of Information Collected:

Link to opt-out page

Expand/collapse added in beta 1.2



Policy Summary

+ Federal Trade Commission

Privacy Policy Check

Federal Trade Commission's priv

Privacy Policy Summary

+ Policy Statement 1 - Basic Infor

Data collected from all Web users: ac

+ Policy Statement 2 - Data Colle

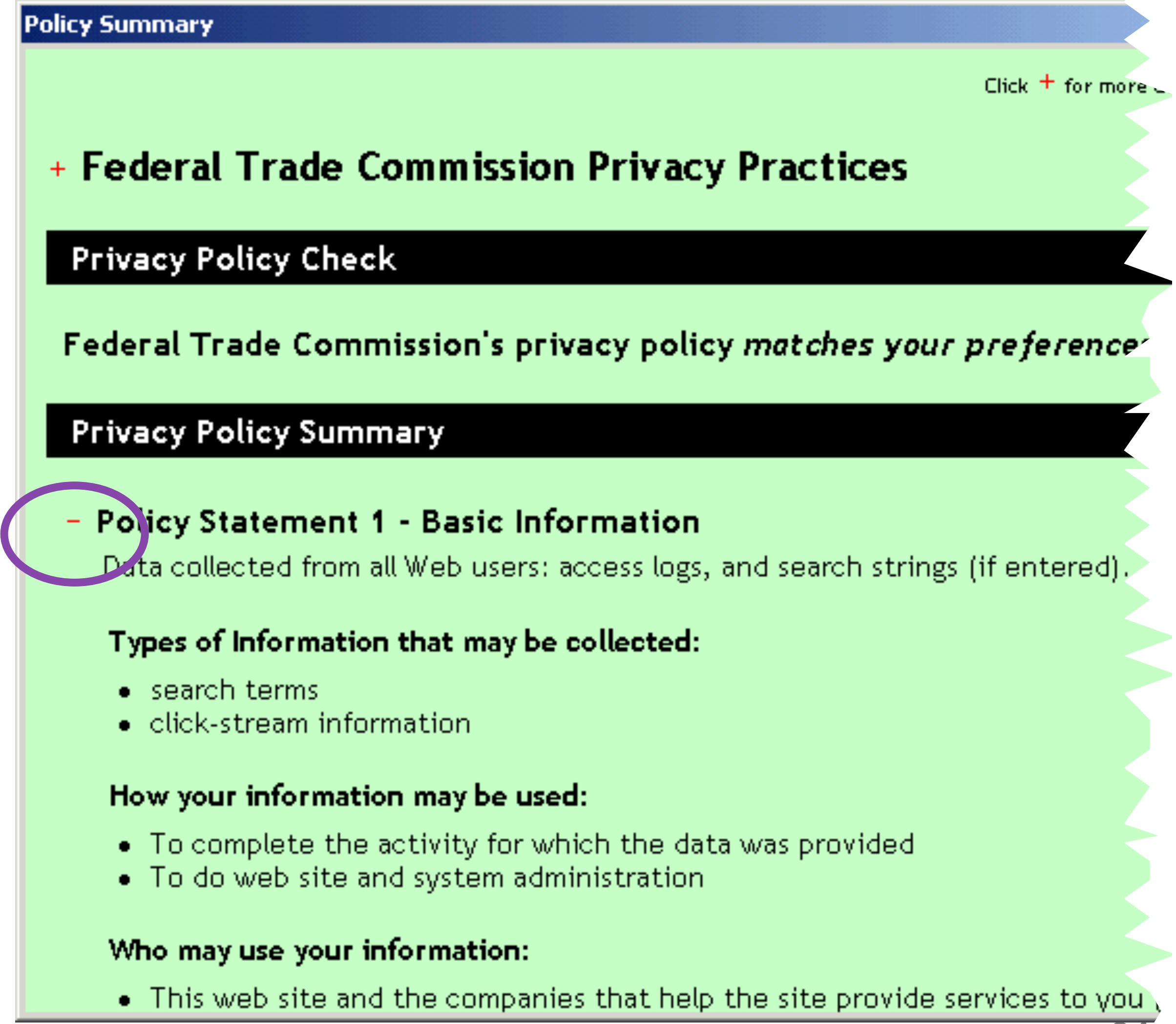
− Access to your information

This site allows you to access your c
about you from its records

+ How to reach this site

+ How to resolve privacy-relate

More Information



Policy Summary

Click + for more

+ Federal Trade Commission Privacy Practices

Privacy Policy Check

Federal Trade Commission's privacy policy *matches your preference*

Privacy Policy Summary

− Policy Statement 1 - Basic Information

Data collected from all Web users: access logs, and search strings (if entered).

Types of Information that may be collected:

- search terms
- click-stream information

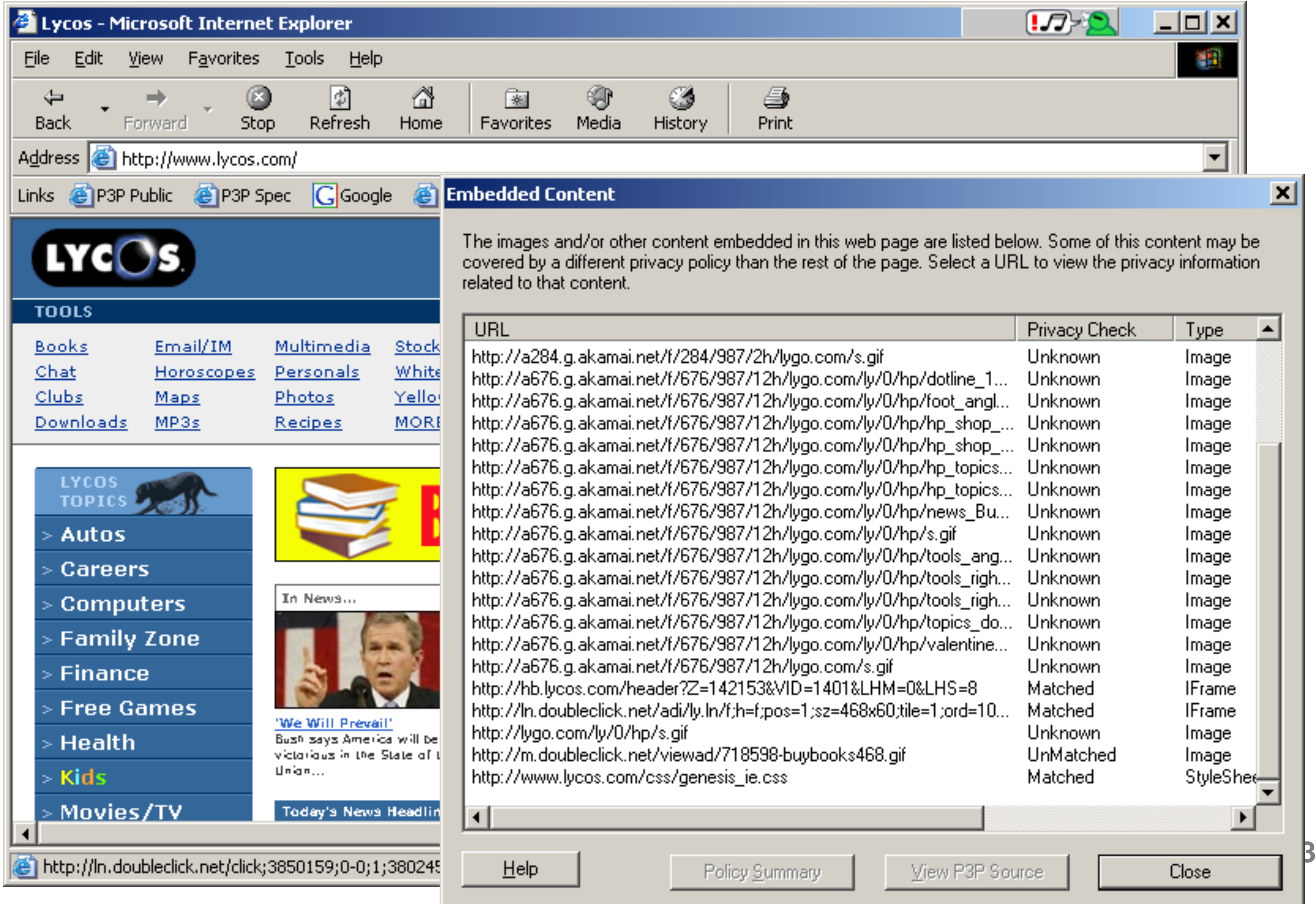
How your information may be used:

- To complete the activity for which the data was provided
- To do web site and system administration

Who may use your information:

- This web site and the companies that help the site provide services to you

Bird checks policies for embedded content



Address http://www.lycos.com/

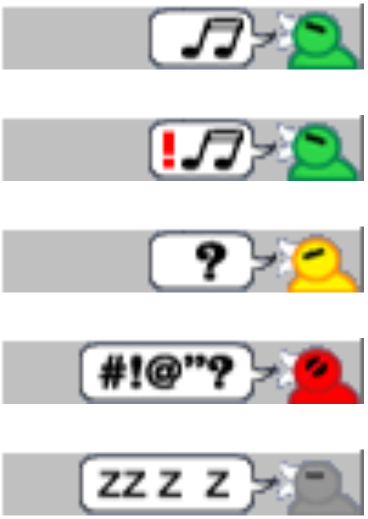
http://ln.doubleclick.net/click;3850159;0-0;1;380245

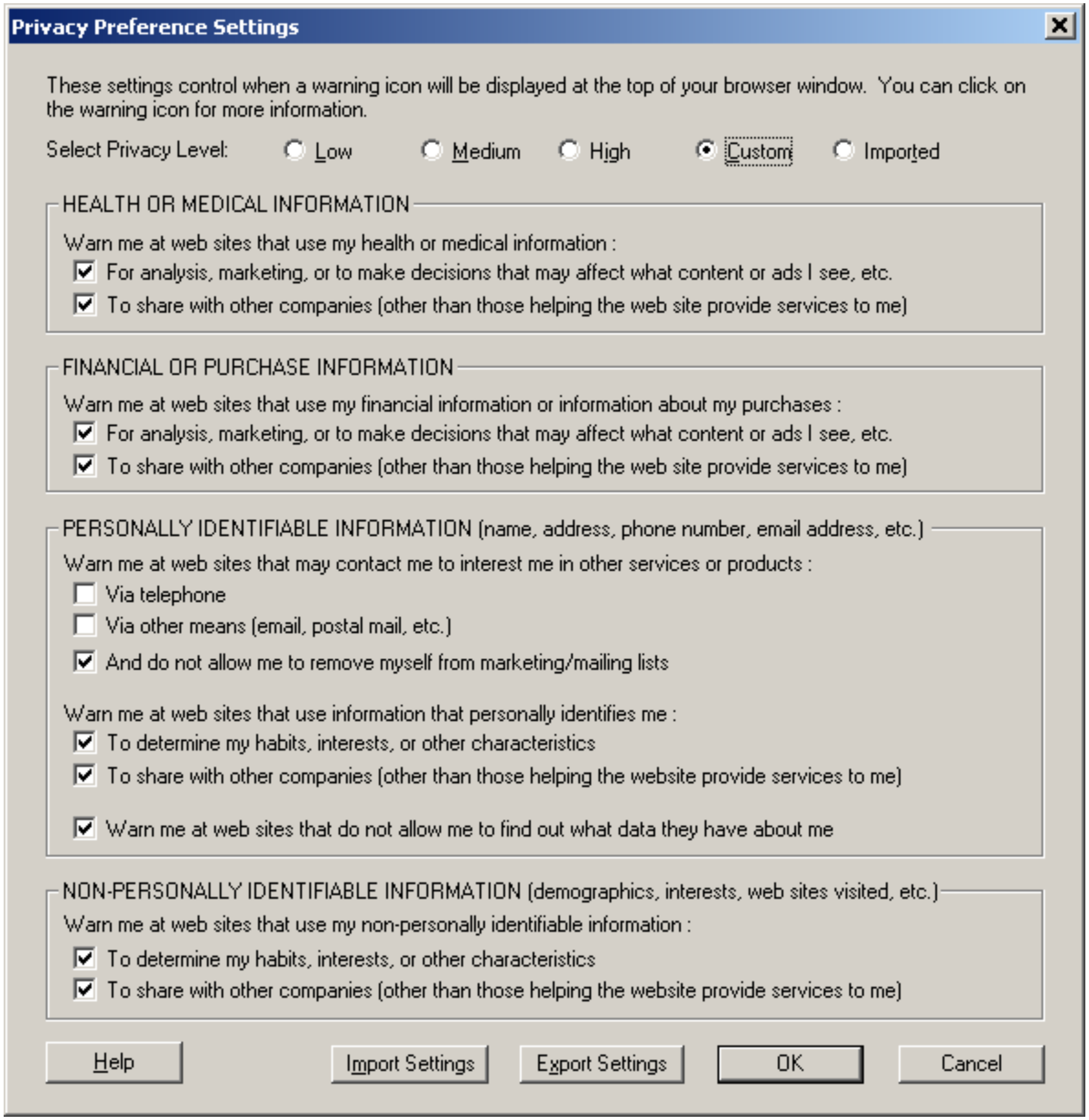
Embedded Content

The images and/or other content embedded in this web page are listed below. Some of this content may be covered by a different privacy policy than the rest of the page. Select a URL to view the privacy information related to that content.

URL	Privacy Check	Type
http://a284.g.akamai.net/f/284/987/2h/lygo.com/s.gif	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/dotline_1...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/foot_angl...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/hp_shop_...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/hp_shop_...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/hp_topics...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/hp_topics...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/news_Bu...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/s.gif	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/tools_ang...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/tools_righ...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/tools_righ...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/topics_do...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/valentine...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/s.gif	Unknown	Image
http://hb.lycos.com/header?Z=142153&VID=1401&LHM=0&LHS=8	Matched	IFrame
http://ln.doubleclick.net/adi/ly.ln/f;h=f;pos=1;sz=468x60;tile=1;ord=10...	Matched	IFrame
http://lygo.com/ly/0/hp/s.gif	Unknown	Image
http://m.doubleclick.net/viewad/718598-buybooks468.gif	UnMatched	Image
http://www.lycos.com/css/genesis_ie.css	Matched	StyleShee

Privacy Bird icons





Privacy Preference Settings

These settings control when a warning icon will be displayed at the top of your browser window. You can click on the warning icon for more information.

Select Privacy Level: ○ Low ○ Medium ○ High ● Custom ○ Imported

HEALTH OR MEDICAL INFORMATION

Warn me at web sites that use my health or medical information :

- ☑ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.
- ☑ To share with other companies (other than those helping the web site provide services to me)

FINANCIAL OR PURCHASE INFORMATION

Warn me at web sites that use my financial information or information about my purchases :

- ☑ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.
- ☑ To share with other companies (other than those helping the web site provide services to me)

PERSONALLY IDENTIFIABLE INFORMATION (name, address, phone number, email address, etc.)

Warn me at web sites that may contact me to interest me in other services or products :

- □ Via telephone
- □ Via other means (email, postal mail, etc.)
- ☑ And do not allow me to remove myself from marketing/mailing lists

Warn me at web sites that use information that personally identifies me :

- ☑ To determine my habits, interests, or other characteristics
- ☑ To share with other companies (other than those helping the website provide services to me)

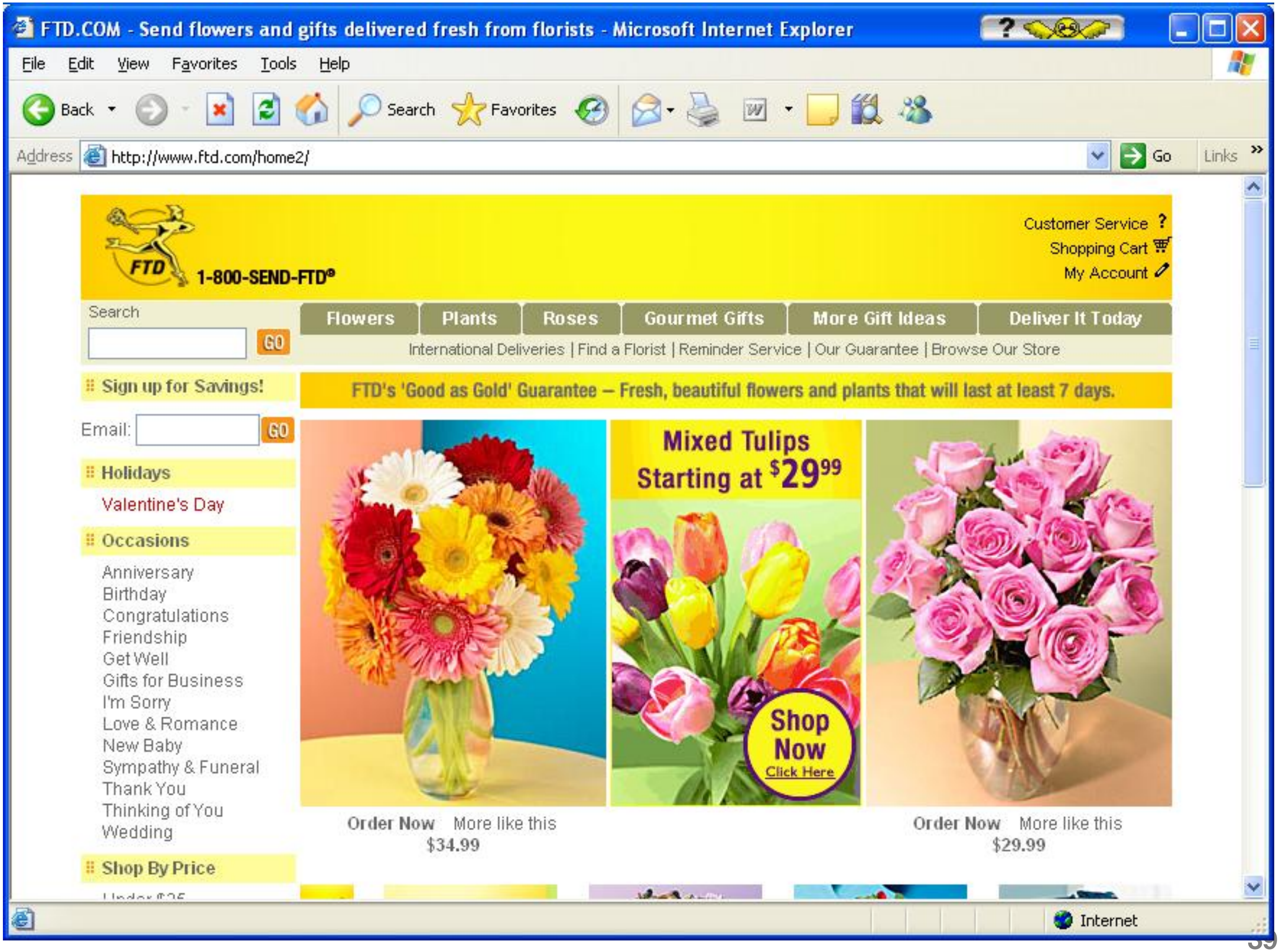
☑ Warn me at web sites that do not allow me to find out what data they have about me

NON-PERSONALLY IDENTIFIABLE INFORMATION (demographics, interests, web sites visited, etc.)

Warn me at web sites that use my non-personally identifiable information :

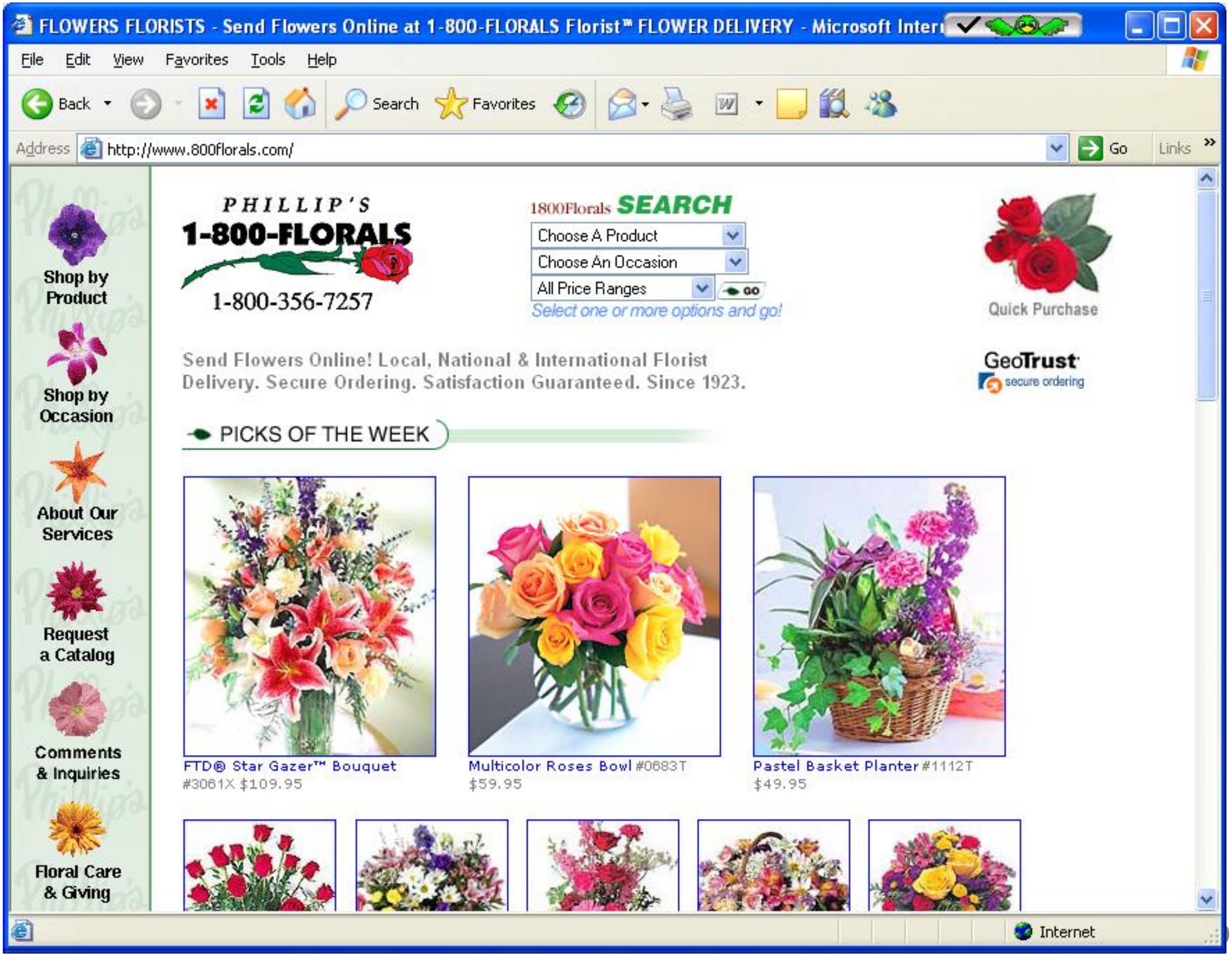
- ☑ To determine my habits, interests, or other characteristics
- ☑ To share with other companies (other than those helping the website provide services to me)

But how do you find sites with good policies?


FTD.COM - Send flowers and gifts delivered fresh from florists - Microsoft Internet Explorer

Address: http://www.ftd.com/home2/

FTD's 'Good as Gold' Guarantee – Fresh, beautiful flowers and plants that will last at least 7 days.



http://www.800florals.com/

Select one or more options and go!

Send Flowers Online! Local, National & International Florist Delivery. Secure Ordering. Satisfaction Guaranteed. Since 1923.

PICKS OF THE WEEK

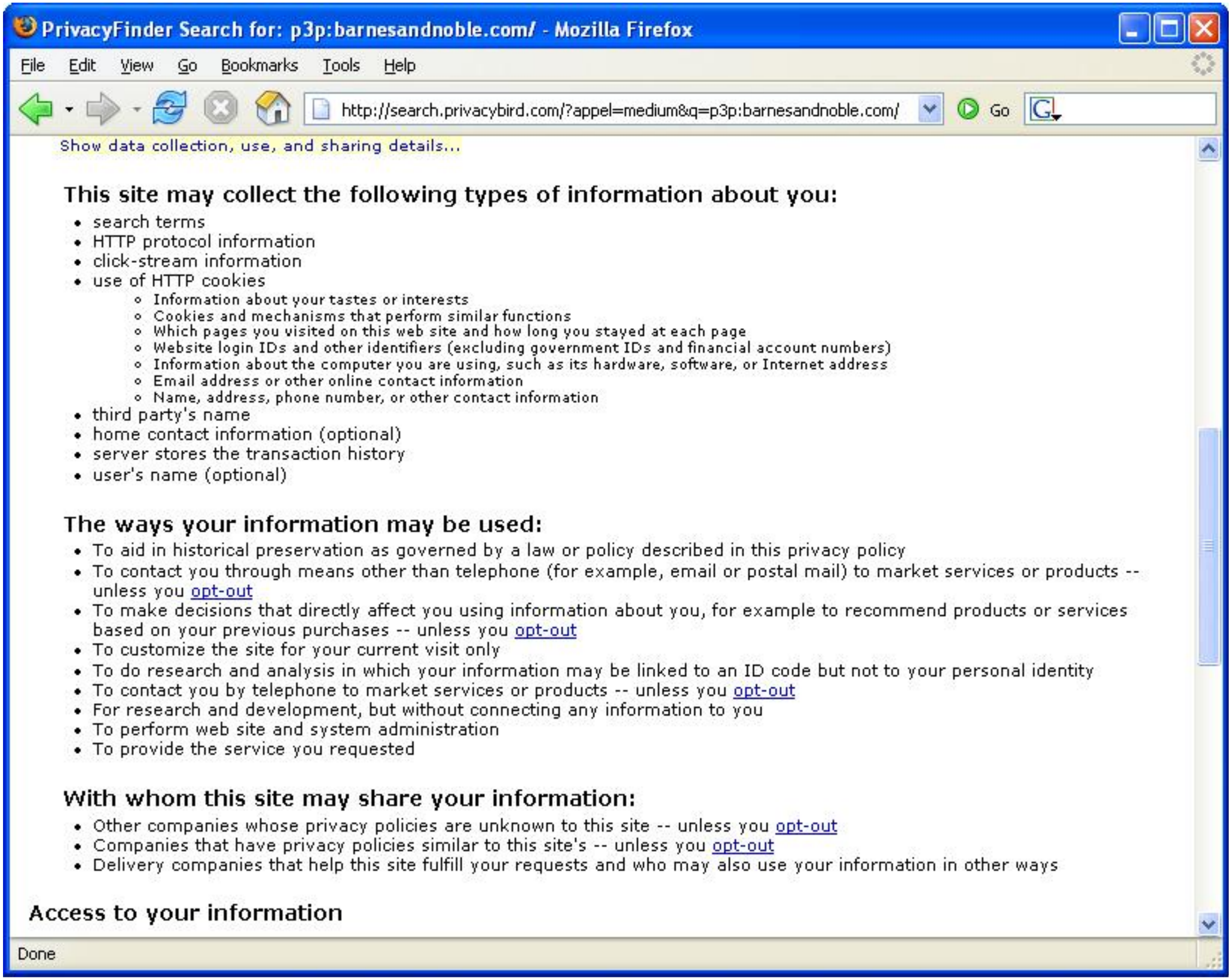
FTD® Star Gazer™ Bouquet #3061X $109.95

Multicolor Roses Bowl #0683T $59.95

Pastel Basket Planter #1112T $49.95

Privacy Finder

- Prototype developed at AT&T Labs, improved and deployed by CUPS
- Uses Google or Yahoo! API to retrieve search results
- Checks each result for P3P policy
- Evaluates P3P policy against user's preferences
- Reorders search results
- Composes search result page with privacy annotations next to each P3P-enabled result
- Users can retrieve "Privacy Report" similar to Privacy Bird policy summary


PrivacyFinder Search for: p3p:barnesandnoble.com/ - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://search.privacybird.com/?appel=medium&q=p3p:barnesandnoble.com/
Go
Done

Show data collection, use, and sharing details...

This site may collect the following types of information about you:

- search terms
- HTTP protocol information
- click-stream information
- use of HTTP cookies
  - Information about your tastes or interests
  - Cookies and mechanisms that perform similar functions
  - Which pages you visited on this web site and how long you stayed at each page
  - Website login IDs and other identifiers (excluding government IDs and financial account numbers)
  - Information about the computer you are using, such as its hardware, software, or Internet address
  - Email address or other online contact information
  - Name, address, phone number, or other contact information
- third party's name
- home contact information (optional)
- server stores the transaction history
- user's name (optional)

The ways your information may be used:

- To aid in historical preservation as governed by a law or policy described in this privacy policy
- To contact you through means other than telephone (for example, email or postal mail) to market services or products -- unless you opt-out
- To make decisions that directly affect you using information about you, for example to recommend products or services based on your previous purchases -- unless you opt-out
- To customize the site for your current visit only
- To do research and analysis in which your information may be linked to an ID code but not to your personal identity
- To contact you by telephone to market services or products -- unless you opt-out
- For research and development, but without connecting any information to you
- To perform web site and system administration
- To provide the service you requested

With whom this site may share your information:

- Other companies whose privacy policies are unknown to this site -- unless you opt-out
- Companies that have privacy policies similar to this site's -- unless you opt-out
- Delivery companies that help this site fulfill your requests and who may also use your information in other ways

Access to your information

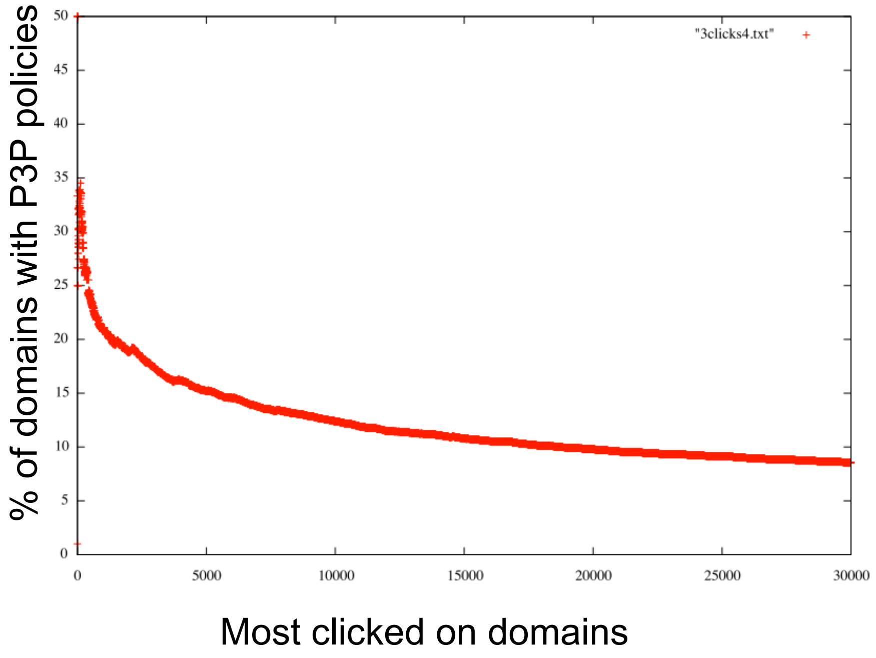
P3P Adoption Studies

- Compiled two lists of search terms:
  - Typical: 20,000 terms randomly sampled from one week of AOL user search queries
  - Ecommerce: 940 terms screen scraped from Froogle front page
- Submitted search terms to Google, Yahoo!, and AOL search engines and collected top 20 results for each term
- Checked each result for P3P policy and evaluated policies against 5 “rulesets” and P3P validator
- Saved 1,232,955 annotated search results in database
- Separately checked for P3P policies on 30,000 domains most clicked on by AOL search engine users

L. Cranor, S. Egelman, S. Sheng, A. McDonald, and A. Chowdhury. P3P Deployment on Websites. Electronic Commerce Research and Applications, 2008.

Results: P3P deployment

- 10% of results from typical search terms have P3P
- 21% of results from ecommerce search terms have P3P
- More popular sites are more likely to have P3P



Results: Frequency of P3P-enabled hits

- 83% of searches had at least one P3P-enabled site in top 20 results
- 68% of searches had at least one P3P-enabled site in top 10 results
- For top 20 search results returned by AOL search engine for typical search terms:
  - 29% return at least 1 P3P-enabled hit that matches medium privacy preferences
  - 34% return at least 1 P3P-enabled hit in that does not share data
  - 31% return at least 1 P3P-enabled hit that does not market without opt-in
  - Thus, ~ 1/3 of the time AOL users will find site with “good” privacy policy in first 2 pages of results

Does Privacy Finder influence purchases?

- Yes!
- J. Tsai, S. Egelman, L. Cranor, and A. Acquisti. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.

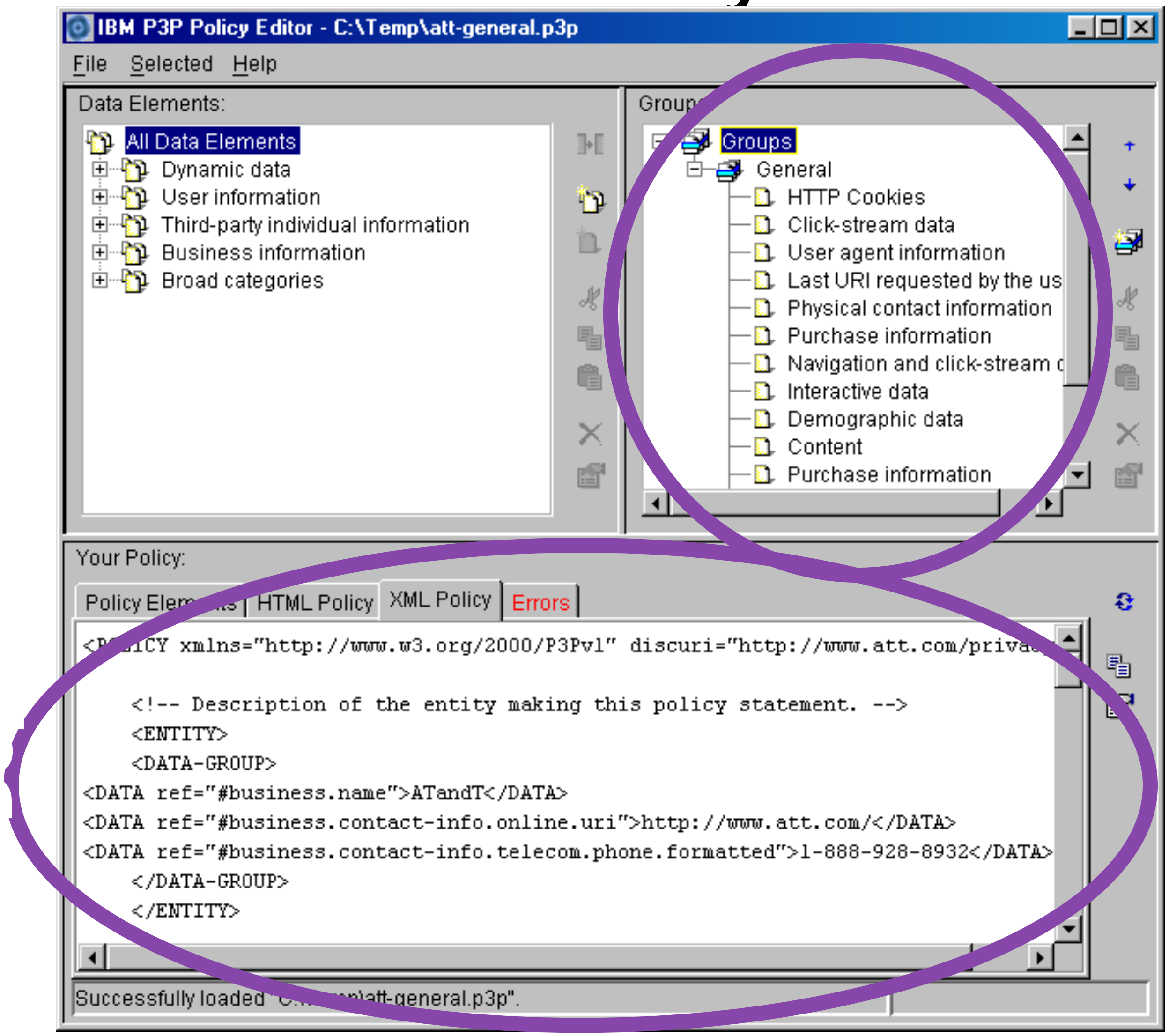
P3P deployment overview

- Create a privacy policy
- Analyze the use of cookies and third-party content on your site
- Determine whether you want to have one P3P policy for your entire site or different P3P policies for different parts of your site
- Create a P3P policy (or policies) for your site
- Create a policy reference file for your site
- Configure your server for P3P
- Test your site to make sure it is properly P3P enabled

Generating a P3P policy

- Edit by hand
  - Cut and paste from an example
- Use a P3P policy generator
  - Recommended: IBM P3P policy editor
    http://www.alphaworks.ibm.com/tech/p3peditor
- Generate compact policy and policy reference file the same way (by hand or with policy editor)
- Get a book
  - Web Privacy with P3P
    by Lorrie Faith Cranor
    http://p3pbook.com/

IBM P3P Policy Editor



```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1" discuri="http://www.att.com/priva

    <!-- Description of the entity making this policy statement. -->
    <ENTITY>
    <DATA-GROUP>
<DATA ref="#business.name">ATandT</DATA>
<DATA ref="#business.contact-info.online.uri">http://www.att.com/</DATA>
<DATA ref="#business.contact-info.telecom.phone.formatted">1-888-928-8932</DATA>
    </DATA-GROUP>
    </ENTITY>
```

Successfully loaded "C:\Temp\att-general.p3p".

Sites can list the types of data they collect

And view the corresponding P3P policy

Compact policies

- HTTP header with short summary of full P3P policy for cookies (not for URLs)
- Not required
- Must be used in addition to full policy
- Must commit to following policy for lifetime of cookies
- May over simplify site’s policy
- IE6 relies heavily on compact policies for cookie filtering – especially an issue for third-party cookies

Server configuration

- Only needed for compact policies and/or sites that use P3P HTTP header
- Need to configure server to insert extra headers

Reading the P3P specification

- http://www.w3.org/TR/P3P11/

DNT history

- 2007 – Public interest groups propose Do Not Track (like Do Not Call) to FTC
- 2009 – Google ad-on to make opt-out cookies permanent, Mozilla ad-on implements DNT header
- 2010 – FTC Chairman discusses DNT with Senate committee
- 2011 – W3C launches working group, browsers implement DNT
- 2012 – Advertising industry pledges to support DNT, Microsoft enables DNT by default in IE10
- 2013 – Working group votes to continue working, ad industry quits
- 2014 – W3C issues LC working draft
- 2015 – W3C issues CR draft, EFF issues their own DNT policy

Headlines

- Do Not Track proposal is DOA (July 16, 2013)
  http://money.cnn.com/2013/07/16/technology/do-not-track/

- The Internet’s best hope for a Do Not Track standard is falling apart. Here’s why. (October 11, 2013)
  http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/11/the-internets-best-hope-for-a-do-not-track-standard-is-falling-apart-heres-why/

- How bickering and greed neutered the 'Do Not Track' privacy initiative (May 22, 2014)
  http://www.pcworld.com/article/2158220/do-not-track-oh-what-the-heck-go-ahead.html

- ADVERTISING ALLIANCE TO WEB STANDARDS GROUP: DROP "DO NOT TRACK” (June 23, 2014)
  http://associationsnow.com/2014/06/advertising-alliance-web-standards-group-drop-do-not-track/

- Do-Not-Track Will Benefit Our Whole Industry (August 29, 2014)
  http://www.mediapost.com/publications/article/233197/do-not-track-will-benefit-our-whole-industry.html

- Why We Oppose Do Not Track and How to Fix It: Rules Need to Apply to All Data Collectors -- Including Facebook and Google (July 25, 2014)
  http://adage.com/article/guest-columnists/oppose-track-fix/294319/

What type of protocol?

- List of trackers to block?
- One-way signal from browser to website?
- Two-way communication
  - Browser signals to website
  - Website signals back

Conflicting signals

- What if users have opted out with opt-out cookie or other mechanism but not DNT?
- What if users have opt-in but send DNT=1?

Exceptions

- How can users make an exception for some sites? For some trackers? For some site/tracker combinations?
- How do we prevent sites from tricking users into making an exception or making an exception w/out user consent?

Deliberate choice by user

“Key to that notion of expression is that the signal sent must reflect the user's preference, not the choice of some vendor, institution, site, or network-imposed mechanism outside the user's control; this applies equally to both the general preference and exceptions. The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.”

http://www.w3.org/TR/2014/WD-tracking-dnt-20140424/

CR working draft specifies

- DNT request header field as an HTTP mechanism for expressing the user's preference regarding tracking
- HTML DOM property to make that expression readable by scripts
- APIs that allow scripts to register site-specific exceptions granted by the user
- Mechanisms for sites to communicate whether and how they honor a received preference
  - "Tk" response header field
  - Well-known resources that provide a machine-readable tracking status
- http://www.w3.org/TR/tracking-dnt/

Definition of tracking

Tracking is the collection of data regarding a particular user's activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred. A *context* is a set of resources that are controlled by the same party or jointly controlled by a set of parties.

DNT meaning

- 1
  - This user prefers not to be tracked on the target site.
- 0
  - This user prefers to allow tracking on the target site.

No defaults allowed

- A tracking preference expression is only transmitted when it reflects a deliberate choice by the user.
- In the absence of user choice, there is no tracking preference expressed.
- A user agent must offer users a minimum of two alternative choices: *unset* or *DNT:1*. A user agent may offer a third alternative choice: *DNT:0*.

Tracking status value

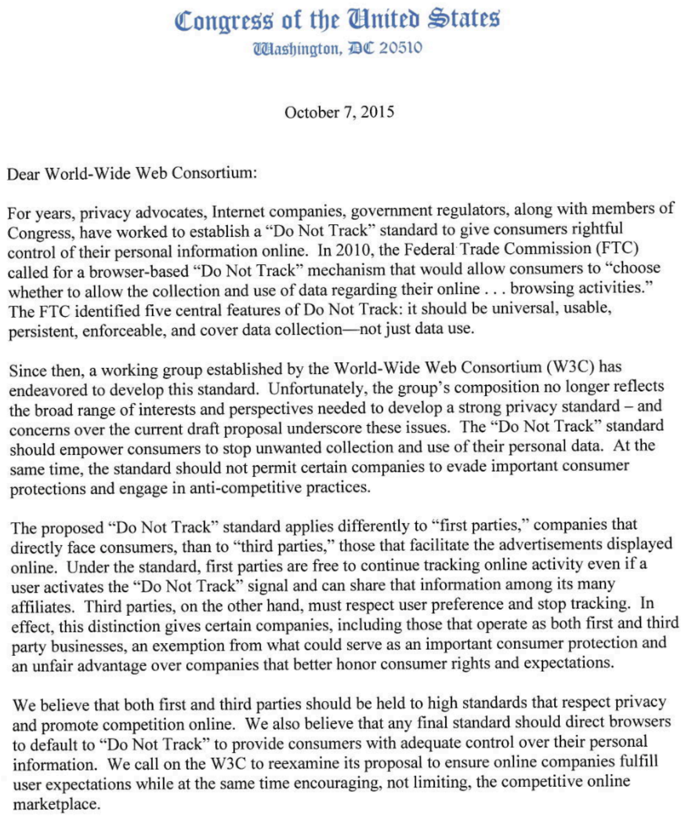
- ! — under construction
- ? — dynamic
- G — gateway to multiple parties
- **N — not tracking**
- **T — tracking**
- **C — tracking with consent**
- P — tracking only if consented
- **D — disregarding DNT**
- U — updated

Tracking compliance

- http://www.w3.org/TR/tracking-compliance/
- First party compliance with DNT:1
  - May collect, retain, and use data, including for customizing content, services, and ads
- Third party compliance with DNT:1
  - May collect data with explicit user consent, data is deidentified, or permitted uses:
    - Frequency capping
    - Financial logging
    - Security
    - Debugging

Congress weighs in

- Lawmakers Call For Stronger Do-Not-Track Standards (October 5, 2015) http://www.mediapost.com/publications/article/259971/senators-call-for-stronger-do-not-track-standards.html
- Senators Markey and Franken, and Congressman Barton complain that DNT has different rules for 1st party and 3rd party



Congress of the United States
Washington, DC 20510

October 7, 2015

Dear World-Wide Web Consortium:

For years, privacy advocates, Internet companies, government regulators, along with members of Congress, have worked to establish a "Do Not Track" standard to give consumers rightful control of their personal information online. In 2010, the Federal Trade Commission (FTC) called for a browser-based "Do Not Track" mechanism that would allow consumers to "choose whether to allow the collection and use of data regarding their online . . . browsing activities." The FTC identified five central features of Do Not Track: it should be universal, usable, persistent, enforceable, and cover data collection—not just data use.

Since then, a working group established by the World-Wide Web Consortium (W3C) has endeavored to develop this standard. Unfortunately, the group's composition no longer reflects the broad range of interests and perspectives needed to develop a strong privacy standard – and concerns over the current draft proposal underscore these issues. The "Do Not Track" standard should empower consumers to stop unwanted collection and use of their personal data. At the same time, the standard should not permit certain companies to evade important consumer protections and engage in anti-competitive practices.

The proposed "Do Not Track" standard applies differently to "first parties," companies that directly face consumers, than to "third parties," those that facilitate the advertisements displayed online. Under the standard, first parties are free to continue tracking online activity even if a user activates the "Do Not Track" signal and can share that information among its many affiliates. Third parties, on the other hand, must respect user preference and stop tracking. In effect, this distinction gives certain companies, including those that operate as both first and third party businesses, an exemption from what could serve as an important consumer protection and an unfair advantage over companies that better honor consumer rights and expectations.

We believe that both first and third parties should be held to high standards that respect privacy and promote competition online. We also believe that any final standard should direct browsers to default to "Do Not Track" to provide consumers with adequate control over their personal information. We call on the W3C to reexamine its proposal to ensure online companies fulfill user expectations while at the same time encouraging, not limiting, the competitive online marketplace.

EFF privacy-friendly Do Not Track (DNT) Policy

- EFF Privacy Badger blocks tracking, but unblocks for companies that comply with their DNT policy
- Does not make distinction between first and third party
- https://www.eff.org/dnt-policy

Privacy Badger 1.0
New Browser Plugin Blocks Spying Ads and Invisible Trackers.

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering &
Public Policy