# Platform for Privacy Preferences (P3P) Project

Week 5/6 - February 10, 12, 17





## 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

- Idea discussed at November 1995 FTC meeting
- Ad Hoc "Internet Privacy Working Group" convened to discuss the idea in Fall 1996
- W3C began working on P3P in Summer 1997
  - Several working groups chartered with dozens of participants from industry, non-profits, academia, government
  - Numerous public working drafts issued, and feedback resulted in 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
- P3P issued as official W3C Recommendation on April 16, 2002
  - `http://www.w3.org/TR/P3P/`





# P3P1.0 - A first step

- Offers an easy way for web sites to communicate about their privacy policies in a standard machine-readable format
  - Can be deployed using existing web servers
- This will enable the development of tools that:
  - Provide snapshots of sites' policies
  - Compare policies with user preferences
  - Alert and advise the user

## P3P is part of the solution

P3P1.0 helps users understand privacy policies but is not a complete solution

- Seal programs and regulations
  - help ensure that sites comply with their policies
- Anonymity tools
  - reduce the amount of information revealed while browsing
- Encryption tools
  - secure data in transit and storage
- Laws and codes of practice
  - provide a base line level for acceptable policies





## The basics

- P3P provides a standard XML format that web sites use to encode their privacy policies
- Sites also provide XML "policy reference files" to indicate which policy applies to which part of the site
- Sites can optionally provide a "compact policy" by configuring their servers to issue a special P3P header when cookies are set
- No special server software required
- User software to read P3P policies called a "P3P user agent"

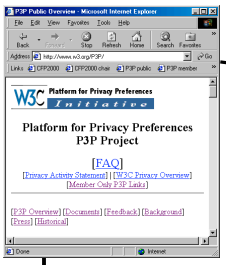
# P3P1.0 Spec Defines

- 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 simple HTTP transaction

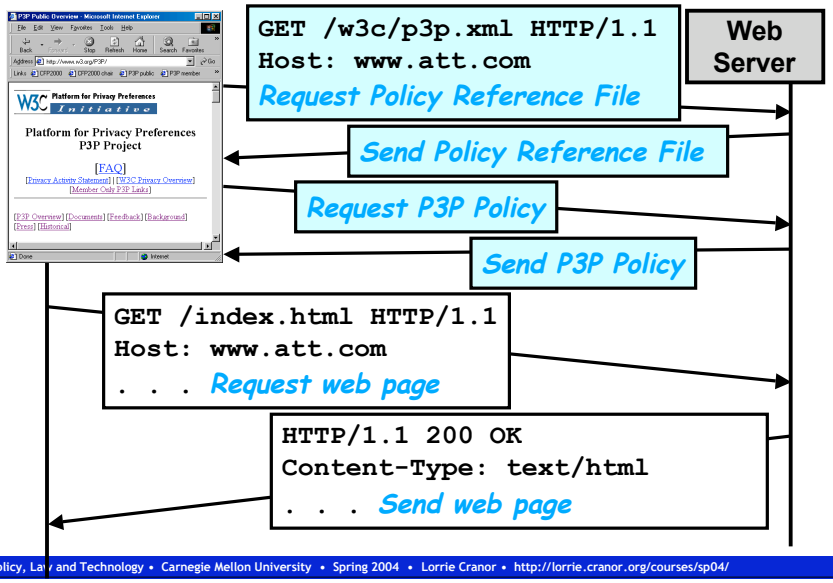



Web Server

```
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



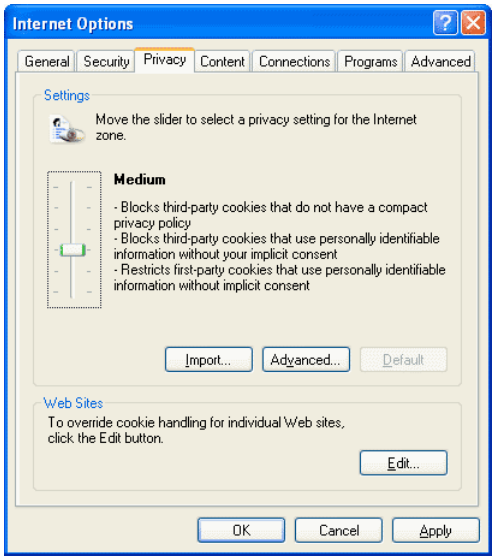




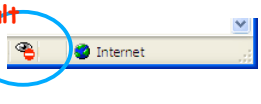

# Transparency

- 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

# P3P in IE6



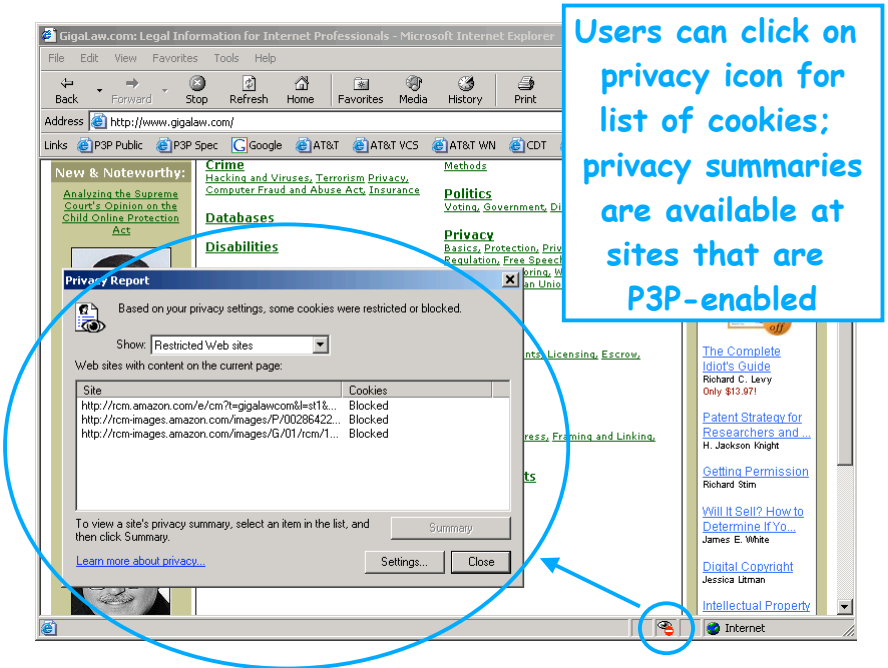

Automatic processing of compact policies only; third-party cookies without compact policies blocked by default



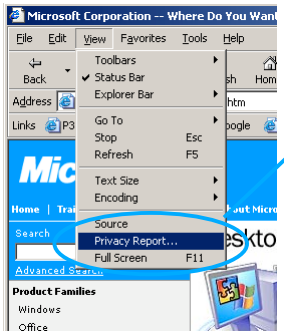

Privacy icon on status bar indicates that a cookie has been blocked – pop-up appears the first time the privacy icon appears






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

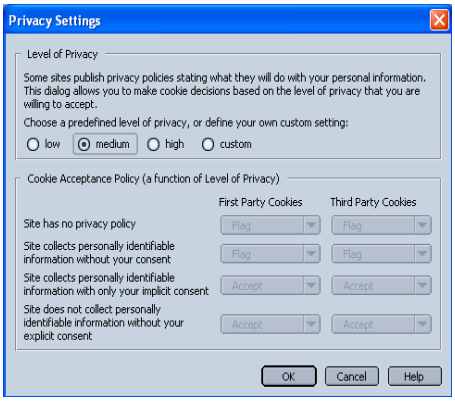



Privacy summary report is generated automatically from full P3P policy

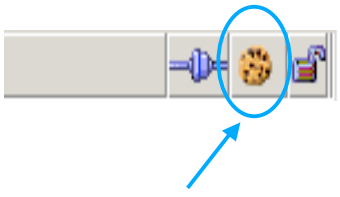





# P3P in Netscape 7

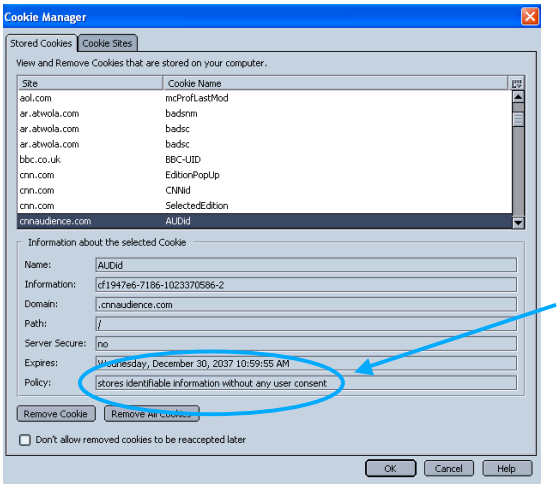



Preview version similar to IE6, focusing, on cookies; cookies without compact policies (both first-party and third-party) are "flagged" rather than blocked by default



Indicates flagged cookie

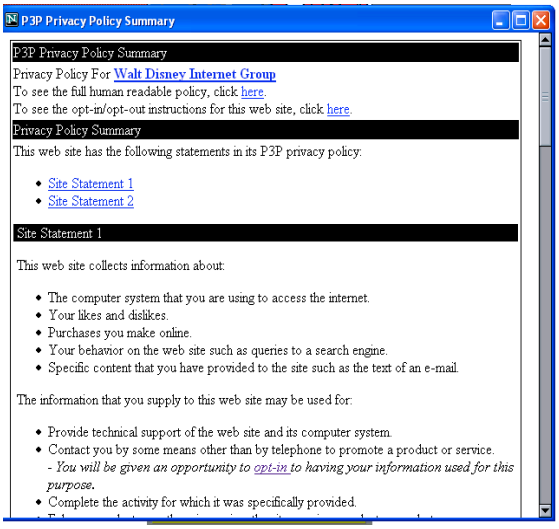
## P3P: Introduction




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



## P3P: Introduction




A policy summary can be generated automatically from full P3P policy

# AT&T Privacy Bird

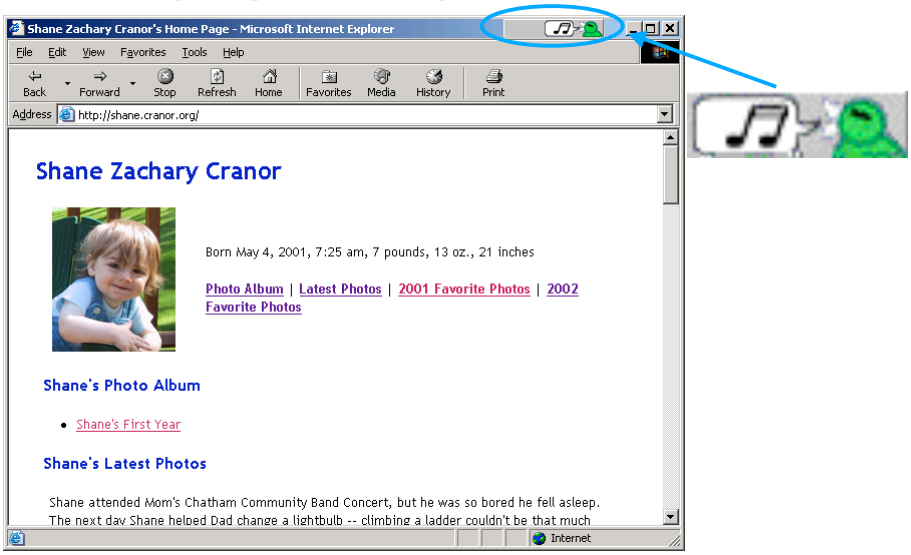
- Free download of beta from http://www.privacybird.com/
- "Browser helper object" for IE 5.01/5.5/6.0
- Reads P3P policies at all P3P-enabled sites automatically

- 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

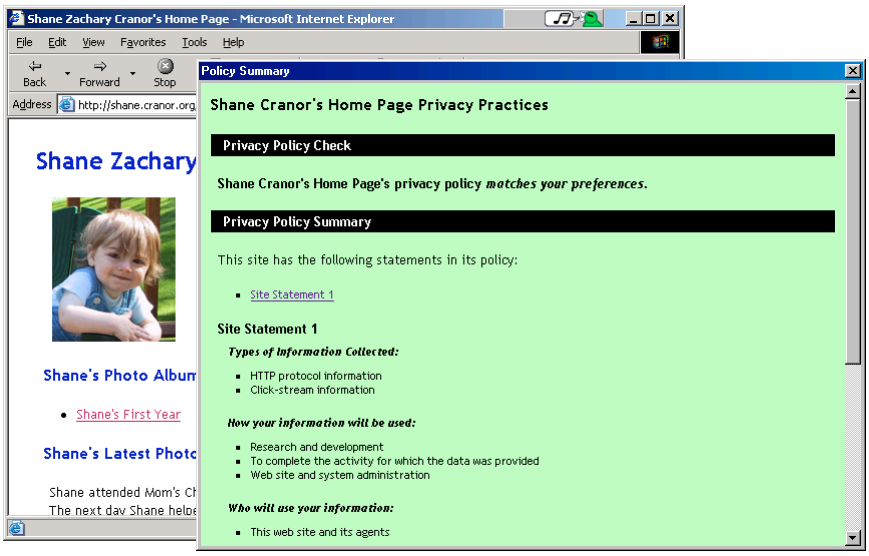




# Chirping bird is privacy indicator



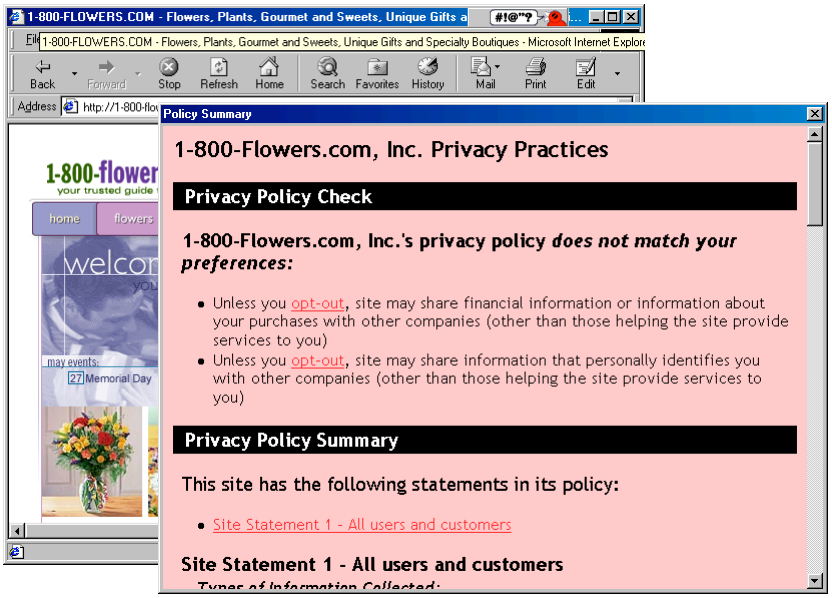
# Click on the bird for more info



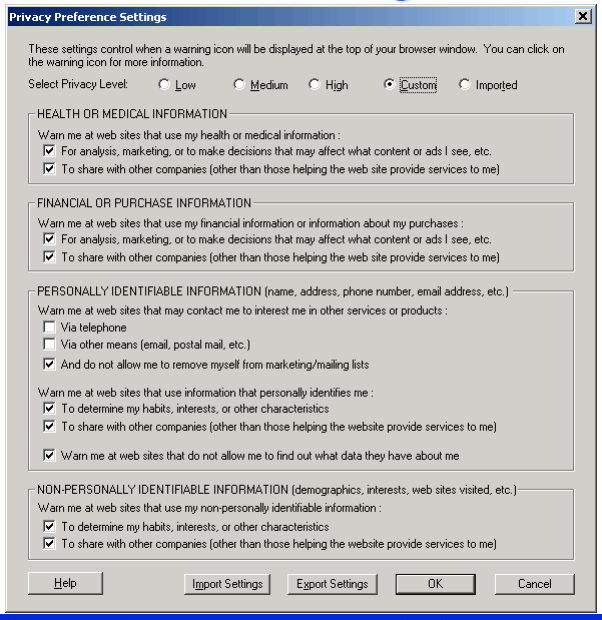





# Privacy policy summary - mismatch



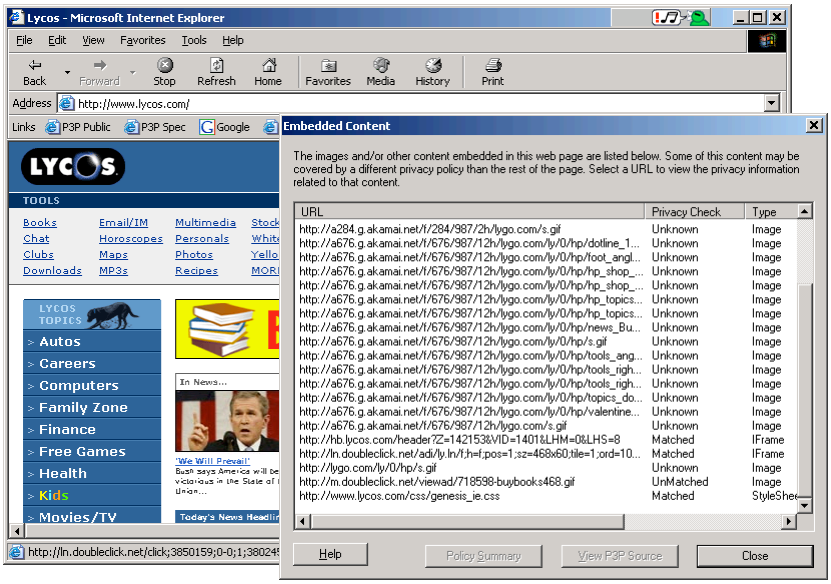
# Users select warning conditions








# Bird checks policies for embedded content



## P3P deployment overview

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





## 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

## One policy or many?

- P3P allows policies to be specified for individual URLs or cookies
- One policy for entire web site (all URLs and cookies) is easiest to manage
- Multiple policies can allow more specific declarations about particular parts of the site
- Multiple policies may be needed if different parts of the site have different owners or responsible parties (universities, CDNs, etc.)





## Third-party content

- Third-party content should be P3P-enabled by the third-party
- If third-party content sets cookies, IE6 will block them by default unless they have P3P compact policy
- Your first-party cookies may become third-party cookies if your site is framed by another site, a page is sent via email, etc.

## Cookies and P3P

- P3P policies must declare all the data *stored* in a cookie as well as any data *linked* via the cookie
- P3P policies must declare all uses of stored and linked cookie data
- Sites should not declare cookie-specific policies unless they are sure they know where their cookies are going!
  - ★ Watch out for domain-level cookies
  - ★ Most sites will declare broad policy that covers both URLs and cookies

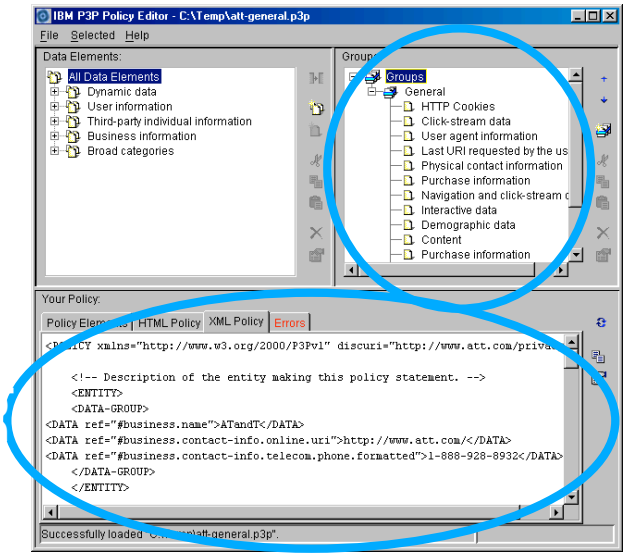




## Generating a P3P policy

- 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




Sites can list the types of data they collect

And view the corresponding P3P policy





# Locating the policy reference file

- Place policy reference file in "well known location" /w3c/p3p.xml
  - ★ Most sites will do this
- Use special P3P HTTP header
  - ★ Recommended only for sites with unusual circumstances, such as those with many P3P policies
- Embed link tags in HTML files
  - ★ Recommended only for sites that exist as a directory on somebody else's server (for example, a personal home page)

## 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
- Procedure depends on server – see *P3P Deployment Guide* appendix `http://www.w3.org/TR/p3pdeployment` or Appendix B of *Web Privacy with P3P*

## Don't forget to test!

- Make sure you use the P3P validator to check for syntax errors and make sure files are in the right place
  http://www.w3.org/P3P/validator/
  - ★ But validator can't tell whether your policy is accurate
- Use P3P user agents to view your policy and read their policy summaries carefully
- Test multiple pages on your site

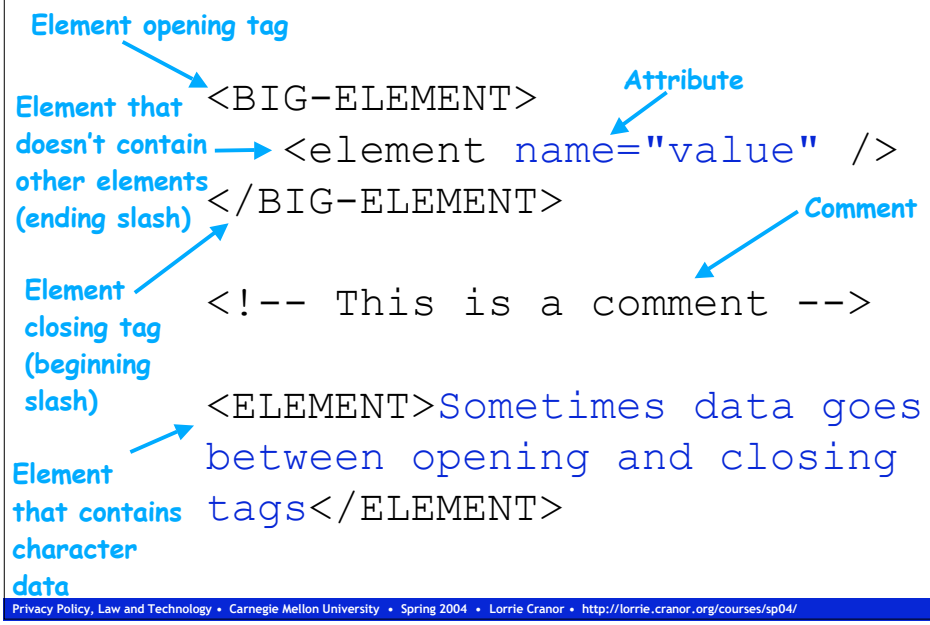




## P3P Policies

- Machine-readable (XML) version of web site privacy policies
- Use P3P Vocabulary to express data practices
- Use P3P Base Data Schema to express type of data collected
- Capture common elements of privacy policies but may not express everything (sites may provide further explanation in human-readable policies)

# XML syntax basics



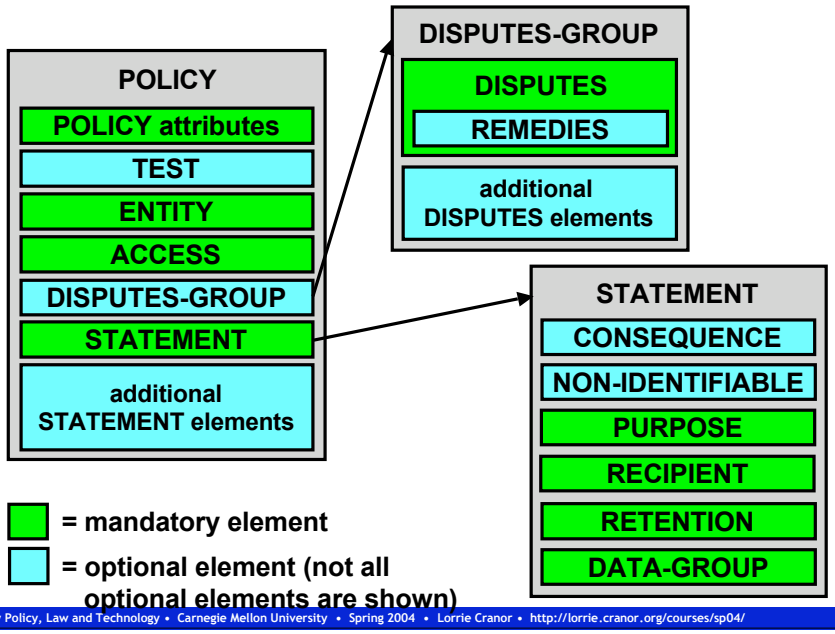





# Assertions in a P3P policy

- 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>`

# Structure of a P3P policy








# Example privacy policy

We do not currently collect any information from visitors to this site except the information contained in standard web server logs (your IP address, referer, information about your web browser, information about your HTTP requests, etc.). The information in these logs will be used only by us and the server administrators for website and system administration, and for improving this site. It will not be disclosed unless required by law. We may retain these log files indefinitely. Please direct questions about this privacy policy to privacy@p3pbook.com.

# 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

Statement

How data may be used

Data recipients

Data retention policy

Types of data collected





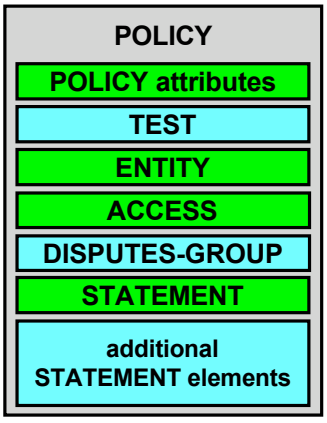
# The POLICY element

- Contains a complete P3P policy
- Takes mandatory `discuri` attribute
  - ★ indicates location of human-readable privacy policy
- Takes `opturi` attribute (mandatory for sites with opt-in or opt-out)
  - ★ Indicates location of opt-in/opt-out policy
- Takes mandatory `name` attribute
- Sub-Elements

```
<EXTENSION>, <TEST>, <EXPIRY>,
  <DATASCHEMA>, <ENTITY>,
  <ACCESS>, <DISPUTES-GROUP>,
  <STATEMENT>, <EXTENSION>
```

- Example

```
<POLICY name="general-p3p-policy"
  discuri="http://www.example.co
  m/privacy.html"
  opturi="http://www.example.com
  /opt-out.html">
```



# The TEST element

- Used for testing purposes
  - ★Presence indicates that policy is for testing purposes and MUST be ignored
- Prevents misunderstandings during initial P3P deployment

```
<TEST/>
```





# The ENTITY element

- Identifies the legal entity making the representation of the privacy practices contained in the policy
- Uses the `business.name` data element and (optionally) other fields in the `business` data set (at least one piece of contact info required)
- Example

```
<ENTITY>
<DATA-GROUP>
  <DATA ref="#business.name">CatalogExample</DATA>
  <DATA ref="#business.contact-info.telecom.telephone.
intcode">1</DATA>
  <DATA ref="#business.contact-info.telecom.telephone.
loccode">248</DATA>
  <DATA ref="#business.contact-info.telecom.telephone.
number">3926753</DATA>
</DATA-GROUP>
</ENTITY>
```

# The ACCESS Element

- Indicates the ability of individuals to access their data
  - **<nonident/>**
  - **<all/>**
  - **<contact-and-other/>**
  - **<ident-contact/>**
  - **<other-ident/>**
  - **<none/>**
- Example

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



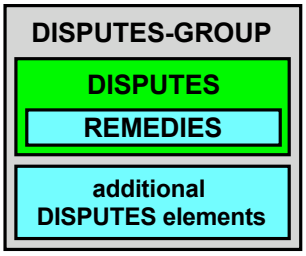


# The DISPUTES Element

- Describes a dispute resolution procedure
  - may be followed for disputes about a service's privacy practices
- Part of a <DISPUTES-GROUP>
  - allows multiple dispute resolution procedures to be listed
- Attributes:
  - **resolution-type**
    - customer service
    - independent organization
    - court
    - applicable law
  - **service**
  - **short-description** (optional)
  - **Verification** (optional)
- Sub-Elements
  - **<IMAGE>** (optional)
  - **<LONG-DESCRIPTION>** (optional)
  - **<REMEDIES>** (optional)

# The REMEDIES element

- Sub element of DISPUTES element
- Specifies possible remedies in case a policy breach occurs
  - **<correct/>**, **<money/>**, **<law/>**
- Example of DISPUTES and REMEDIES



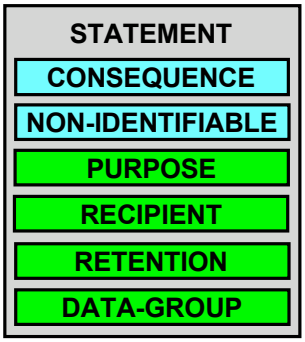

```
<DISPUTES-GROUP>
  <DISPUTES resolution-type="law"
service="http://www.ftc.gov/bcp/conline/edcams/kidzprivac
y/" short-description="Children's Online Privacy
Protection Act of 1998, and Federal Trade Commission
Rule">
    <REMEDIES><law/></REMEDIES>
  </DISPUTES>
</DISPUTES-GROUP>
```





# The STATEMENT element

- Data practices applied to data elements
  - mostly serves as a grouping mechanism
- Contains the following sub-elements
  - **<CONSEQUENCE>** (optional)
  - **<NON-IDENTIFIABLE>** (optional)
  - **<PURPOSE>**
  - **<RECIPIENT>**
  - **<RETENTION>**
  - **<DATA-GROUP>**



## The CONSEQUENCE element

- Consequences that can be shown to a human user to explain why the suggested practice may be valuable in a particular instance, even if the user would not normally allow the practice
- Example

```
<CONSEQUENCE>We offer a 10% discount
to all individuals who join our Cool
Deals Club and allow us to send them
information about cool deals that
they might be interested
in.</CONSEQUENCE>
```





## The NON-IDENTIFIABLE element

- Can optionally be used to declare that no data or no identifiable data is collected
  - *non-identifiable*: there is no reasonable way to attach collected data to identity of a natural person, even with assistance from a third-party
  - Stronger requirements than *non-identified*
- Must have a human readable explanation how this is done at the `discuri`
- Other `STATEMENT` elements are optinal when `NON-IDENTIFIABLE` is present

```
<NON-IDENTIFIABLE/>
```

# The PURPOSE element

- Purposes of data collection, or uses of data
  - `<current/>`
  - `<admin/>`
  - `<develop/>`
  - `<tailoring/>`
  - `<pseudo-analysis/>`
  - `<pseudo-decision/>`
  - `<individual-analysis/>`
  - `<individual-decision/>`
  - `<contact/>`
  - `<historical/>`
  - `<telemarketing/>`
  - `<other-purpose/>`
- Optional attribute:
  - `required`
    - always (default)
    - opt-in
    - opt-out
- Example

```
<PURPOSE>
   <current/><admin/>
   <develop
    required="opt-out"/>
</PURPOSE>
```





# Customization purposes

| Purpose | Does this involve creating a profile of the user? | How is the user identified? | Does this result in a decision that directly affects the user? |
|---|---|---|---|
| Research and development | No | user is not identified | No |
| One-time tailoring | No | user may not be identified at all, or may be identified with a pseudonym or with personally-identifiable information | Yes |
| Pseudonymous analysis | Yes | pseudonym | No |
| Pseudonymous decision | Yes | pseudonym | Yes |
| Individual analysis | Yes | personally-identifiable information | No |
| Individual decision | Yes | personally-identifiable information | Yes |

# The RECIPIENT element

- Recipients of the collected data
  - **<ours>**
  - **<delivery>**
  - **<same>**
  - **<other-recipient>**
  - **<unrelated>**
  - **<public>**
- Optional attribute
  - **required**
    - always (default)
    - opt-in
    - opt-out
- Optional sub-element
  - **<recipient-description>**

Example

```
<RECIPIENT>
 <ours/>
 <same required=
  "opt-out"/>
 <delivery>
  <recipient-description>
   FedEx
  </recipient-description>
 </delivery>
</RECIPIENT>
```





# The RETENTION element

- Indicates the kind or retention policy that applies to the referenced data
  - **<no-retention/>**
  - **<stated-purpose/>**
  - **<legal-requirement/>**
  - **<business-practices/>**
  - **<indefinitely/>**

Requires publishing of **destruction timetable** linked from human-readable privacy policy

- Example

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

# The DATA element

- Describes the data to be transferred or inferred
- Contained in a `DATA-GROUP`
- Attributes:
  - **`ref`**
  - **`optional`** (optional, default is **`no`**, not optional=required)
- Sub-Elements:
  - **`<CATEGORIES>`**
- Example

```
<DATA-GROUP>
  <DATA ref="#dynamic.miscdata">
    <CATEGORIES>
      <preference/><political/>
    </CATEGORIES>
  </DATA>
  <DATA ref="#user.home-info" optional="yes"/>
</DATA-GROUP>
```





# The CATEGORIES element

**Provides hints to user agents as to the intended uses of the data**

- Physical contact information
- Online contact information
- Unique identifiers
- Purchase information
- Financial information
- Computer information
- Navigation and click-stream data
- Interactive data
- Demographic and socio-economic data
- Content
- State management mechanisms
- Political information
- Health information
- Preference data
- Government-issued identifiers
- other

## Base Data Schema

- User data - `user`
  - **`name, bdate, cert, gender, employer, department, jobtitle, home-info, business-info`**
- Third party data - `thirdparty`
  - Same as **`user`**
- Business data - `business`
  - **`name, department, cert, contact-info`**
- Dynamically generated - `Dynamic`
  - **`clickstream, http, clientevents, cookies, miscdata, searchtext, interactionrecord`**





## dynamic.miscdata

- Used to represent data described only by category (without any other specific data element name)
- Must list applicable categories
- Example

```
<DATA ref = "#dynamic.miscdata" >
 <CATEGORIES>
   <online/>
 </CATEGORIES>
</DATA>
```

## Custom data schemas

- You can define your own data elements
- Not required – you can always use categories
- May be useful to make specific disclosures, interface with back-end databases, etc.
- Use the `<DATASCHEMA>` element
  - Embedded in a policy file or in a stand-alone XML file





## Extension mechanism

- `<EXTENSION>` describes extension to P3P syntax
- `optional` attribute indicates whether the extension is mandatory or optional (default is `optional="yes"`)
  - Optional extensions may be safely ignored by user agents that don't understand them
- Only useful if user agents or other P3P tools know what to do with them
- Example (IBM `GROUP-INFO` extension used to add `name` attribute to `STATEMENT` elements)

```
<STATEMENT>
  <EXTENSION optional="yes">
    <GROUP-INFO xmlns=
"http://www.software.ibm.com/P3P/editor/extension-
1.0.html"
      name="Site management"/>
  </EXTENSION>
  . . .
</STATEMENT>
```

# Compact policy syntax

- Part of P3P Header
  - `P3P: CP="NON NID DSP NAV CUR"`
- Represents subset of P3P vocabulary
  - ACCESS (NOI ALL CAO IDC OTI NON)
  - CATEGORIES (PHY ONL UNI PUR ... OTC)
  - DISPUTES (DSP)
  - NON-IDENTIFIABLE (NID)
  - PURPOSE (CUR ADM DEV CUS ... OTP) aio
  - RECIPIENT (OUR DEL SAM UNR PUB OTR) aio
  - REMEDIES (COR MON LAW)
  - RETENTION (NOR STP LEG BUS IND)
  - TEST (TST)





# Policy reference files (PRF)

- Allows web sites to indicate which policy applies to each resource (URL or cookie)
  - Every resource (HTML page, image, sound, form action URL, etc.) can have its own policy
- User agents can cache PRFs (as long as permitted by `EXPIRY`) so they don't have to fetch a new PRF every time a user clicks

# PRF elements

- <EXPIRY>
  - Determines how long PRF is valid – default is 24 hours
- <POLICY-REF>
  - Provides URL of policy in **about** attribute
- <INCLUDE>, <EXCLUDE>
  - URL prefixes (local) to which policy applies/doesn't apply
- <COOKIE-INCLUDE>, <COOKIE-EXCLUDE>
  - Associates / disassociates cookies with policy – if you want a policy to apply to a cookie, you must use **<COOKIE-INCLUDE>**!
- <METHOD>
  - HTTP methods to which policy applies
- <HINT>
  - Provides URLs of PRFs for third-party content





# PRF example

```
<META xmlns="http://www.w3.org/2002/01/P3Pv1" xml:lang="en">
  <POLICY-REFERENCES>
    <EXPIRY max-age="172800"/>
    <POLICY-REF about="http://www.example.com#policy1">
      <INCLUDE>/</INCLUDE>
      <INCLUDE>/news/*</INCLUDE>
      <EXCLUDE>/news/top/*</EXCLUDE>
    </POLICY-REF>
    <POLICY-REF about="http://www.example.net#policy2">
      <INCLUDE>/news/top/*</INCLUDE>
    </POLICY-REF>
    <POLICY-REF about="/P3P/policies.xml#policy3">
      <INCLUDE>/photos/*</INCLUDE>
      <INCLUDE>/ads/*</INCLUDE>
      <COOKIE-INCLUDE/>
    </POLICY-REF>
    <HINT scope="http://www.example.org"
      path="/mypolicy/p3.xml"/>
  </POLICY-REFERENCES>
</META>
```

## Policy updates

- Changing your P3P policy is difficult, but possible
- New policy applies only to new data (old policy applies to old data unless you have informed consent to apply new policy)
- Technically you can indicate exact moment when old policy will cease to apply and new policy will apply
- But, generally it's easiest to have a policy phase-in period where your practices are consistent with both policies





## 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





# 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 the same level of detail
  - ★ Typically natural-language policies contain more detailed explanations of specific practices
- In some jurisdictions, regulators and courts may treat P3P policies equivalently to natural language privacy policies
- The same corporate attorneys and policy makers involved in drafting natural-language privacy policy should be involved in creating 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 |





# Types of P3P user agent tools

- On-demand or continuous
  - Some tools only check for P3P policies when the user requests, others check automatically at every site
- Generic or customized
  - Some tools simply describe a site's policy in some user friendly format – others are customizable and can compare the policy with a user's preferences
- Information-only or automatic action
  - Some tools simply inform users about site policies, while others may actively block cookies, referrers, etc. or take other actions at sites that don't match user's preferences
- Built-in, add-on, or service
  - Some tools may be built into web browsers or other software, others are designed as plug-ins or other add-ons, and others may be provided as part of an ISP or other service

# User privacy preferences

- P3P 1.0 agents may (optionally) take action based on user preferences
  - ★ Users should not have to trust privacy defaults set by software vendors
  - ★ User agents that can read APPEL (A P3P Preference Exchange Language) files can offer users a number of canned choices developed by trusted organizations
  - ★ Preference editors allow users to adapt existing preferences to suit own tastes, or create new preferences from scratch
  - ★ For more info on APPEL see **http://www.w3.org/TR/WD-P3P-preferences** or Chapter 13 in *Web Privacy with P3P*





# APPEL rule

```
<appel:RULE behavior="limited" prompt="yes"
     description="Warning! Data may be shared.">
  <p3p:POLICY>
    <p3p:STATEMENT>
      <p3p:RECIPIENT appel:connective="or" >
        <p3p:same/>
        <p3p:other-recipient/>
        <p3p:public/>
        <p3p:unrelated/>
      </p3p:RECIPIENT>
    </p3p:STATEMENT>
  </p3p:POLICY>
</appel:RULE>
```

description

pattern

connective
- or
- and
- non-or
- non-and
- and-exact
- or-exact

Behavior
- request
- block
- limited

# EPAL

- Enterprise Privacy Authorization Language
- Developed by IBM, submitted to W3C
- Allows enterprises to develop granular rules to check whether data access is authorized
- Similar to P3P syntax but not identical
- Includes
  - Data-categories
  - User-categories - administrators, doctors, etc.
  - Purposes
  - Actions - disclose, read, etc.
  - Obligations - delete after 30 days, get consent, etc.
  - Conditions - user category = doctor
- Allow and deny rules

http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/





# P3P tools beyond user agents

- P3P validators
  - Check a site's P3P policy for valid syntax
- Policy generators
  - Generate P3P policies and policy reference files for web sites
- Web site management tools
  - Assist sites in deploying P3P across the site, making sure forms are consistent with P3P policy, etc.
- Search and comparison tools
  - Compare privacy policies across multiple web sites – perhaps built into search engines

# Available tools

- P3P user agents
  - IE6
  - AT&T Privacy Bird
  - JRC P3P Proxy
- P3P Editors, Generators, and Validators
  - IBM P3P Editor
  - W3C P3P Validator
  - Privacy Council Compact Policy Generator
  - … and many more …

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





# Many possibilities for P3P tools

- P3P user agent integrated into anonymity tool
- P3P user agent integrated into electronic wallet or form filler
- P3P user agent that can automatically generate standard privacy policy "food label" reports
- P3P user agent that can validate seals
- Search engines that weight results according to P3P policy
- Comparison shopping services that include privacy policy as one factor in comparison
- Tools that provide feedback to web sites on whether their policies match user preferences
  - Aggregate feedback
  - Feedback in header extension
- Server-side tools to tag collected data with P3P policy information
- Tools to automatically generate compliance reports based on P3P policy

# Impacts

- Somewhat early to evaluate P3P
- Some companies that P3P-enable think about privacy in new ways and change their practices
  - ★ Systematic assessment of privacy practices
  - ★ Concrete disclosures – less wiggle room
  - ★ Disclosures about areas previously not discussed in privacy policy
- Hopefully we will see greater transparency, more informed consumers, and ultimately better privacy policies





# Evaluating privacy technology

**As opportunities emerge for individuals to customize privacy preferences, research should be conducted to evaluate alternative arrangements. These evaluations should employ a broad range of criteria including ease of understanding, adequacy of notification, compliance with standards, contractual fairness and enforceability, appropriate choice of defaults, efficiency relative to the potential benefits, and integration with other means of privacy protection.**

**— Phil Agre, in *Technology and Privacy: The New Landscape* (MIT Press, 1997), p. 24.**