17 – Usability of privacy policies and the dimensions of privacy notice

Lujo Bauer, Nicolas Christin, and Abby Marsh
March 16, 2016

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security
Notice and choice

Protect privacy by giving people control over their information

**Notice** about data collection and use

**Choices** about allowing their data to be collected and used in that way
Nobody wants to read privacy policies

“the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand”

Nobody wants to read privacy policies

• Research needed to develop:
  – concise formats for showing policies
  – tools for alerting users of policy mismatches
    • integrated with normal functionality (e.g., web search)
  – tools to extract information from human-readable policy
Towards a privacy “nutrition label”

• Standardized format
  – People learn where to find answers
  – Facilitates policy comparisons

• Standardized language
  – People learn terminology

• Brief
  – People find info quickly

• Linked to extended view
  – Get more details if needed
Iterative design process

- Series of studies
  - Focus groups
  - Lab studies
  - Online studies
- Metrics
  - Reading-comprehension (accuracy)
  - Time to find information
  - Ease of policy comparison
  - Subjective opinions, ease, fun, trust


• rate website on scale
• give specific alternatives
• inspired by energy labels

From CMU’s Usable Privacy Policies Project. N. Sadeh, A. Acquisti, T. Breaux, L. Cranor, …
visual ranking of alternatives

visualize average
Privacy label for Android

**Description**
Like word games? Like weasels? This is the game for you. Word Weasel is a fast word game where you find as many words as you can from 9 letters in 50 seconds. Compete with everyone else playing at the same time, a new game starts every minute!

"The most fun you can have on your own with 9 random letters. Brilliantly simple, devilishly addictive." –Kim, Android Market

**Privacy score**
10,000+ downloads
1.9MB

**Privacy Facts**
- Personal information
- Location
- Credit card / financial
- Health / medical

**Reviews**
- Average 4.6
- 5 stars 534
- 4 stars 210
- 3 stars 37
- 2 stars 5
- 1 star 7
PrivacyGrade: Grading The Privacy Of Smartphone Apps

We're a team of researchers from Carnegie Mellon University. We have assigned privacy grades to Android apps based on some techniques we have developed to analyze their privacy-related behaviors. Learn more here or browse our analyzed apps.

How Are Privacy Grades Assigned?

Grades are assigned using a privacy model that we built. This privacy model measures the gap between people's expectations.

Our Work in the News

Protect Your Privacy & Security on the Internet With These Tools
TechCrunch, 02/02/15
Smartphone App Privacy Icon Study Conducted for LifeLock, Inc. by Cranor et al., 2013
Let your computer read for you

- Platform for Privacy Preferences (P3P)
- W3C specification for XML privacy policies
  - Proposed 1996
  - Adopted 2002
- Optional P3P compact policy HTTP headers to accompany cookies
- Lacks incentives for adoption
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
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.
Users can view English translation of (part of) compact policy in Cookie Manager.
A policy summary can be generated automatically from full P3P policy.
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
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 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)

Help  Import Settings  Export Settings  OK  Cancel
Privacy policy summary - mismatch

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:
Expand/collapse added in beta 1.2

---

**Policy Summary**

- **Federal Trade Commission**
  - Privacy Policy Check
  - Federal Trade Commission's privacy policy matches your preference

**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.

---

**Privacy Policy Summary**

- + Policy Statement 1 - Basic Information
- - Access to your information
  - This site allows you to access your data and information about you from its records

**More Information**

- + Policy Statement 2 - Data Collection
- - Access to your information
  - This site allows you to access your data and information about you from its records

- + How to reach this site
- + How to resolve privacy-related issues
Bird checks policies for embedded content
Privacy Bird icons
Example:
Sending flowers
FTD.COM - Send flowers and gifts delivered fresh from florists - Microsoft Internet Explorer

Customer Service
Shopping Cart
My Account

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

Mixed Tulips
Starting at $29.99

Order Now
More like this
Shop Now
Click Here

Order Now
More like this

FTD's Guarantee

FTD's 'Good as Gold' Guarantee – Fresh, beautiful flowers and plants that will last at least 7 days.
PHILLIP'S
1-800-FLORALS
1-800-356-7257


PICKS OF THE WEEK

FTD® Star Gazer™ Bouquet #3064 $109.95
Multicolor Roses Bowl #0083 $59.95
Pastel Basket Planter #1112 $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
Condition 3: Privacy Information

Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players.
www.cvssoftware.com/c/product.htm?recordID56119
$14.45 (w/shipping)

Duracell AA8 DURACELL - Alkaline Batteries Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs...
discountofficeitems.zoovv.com/product/DURMN15RT12Z - Privacy Policy
$14.60 (w/shipping)

Duracell Alkaline Battery Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs DURACELL AA ALKALINE BATTERY - 8 PACK
Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...
www.instorewares.com/Coppertop-Alkaline-Lithium-Bat... - Privacy Policy
$14.80 (w/shipping)

Duracell Coppertop Alkaline AA Batteries
Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.
www.officequarters.com/product.php/item/DUR-MN150388... - Privacy Policy
$15.14 (w/shipping)
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

Done
No P3P syntax checking in IE

• IE accepts P3P policies containing bogus tokens or missing required tokens

• Example of valid compact policy:

• Examples of invalid policies accepted by IE:

Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p

Microsoft uses a “self-declaration” protocol (known as “P3P”) dating from 2002 …. It is well known – including by Microsoft – that it is impractical to comply with Microsoft’s request while providing modern web functionality.
Alternatives to machine-readable policies...

- Extract information from human-readable policies through:
  - Natural language processing
  - Crowdsourcing
Crowdsourcing privacy policy extractions

• Not your typical crowdsourcing task
• Challenges
  • obtain high quality annotations
  • with manageable cost
  • from non-expert crowd workers
  • from complex policy documents
Privacy policy annotation tool

Answer the following questions

Question:
Does the policy state that the website might collect contact information about its users?

Select sentence from policy and click
Remove last selection

Your personally identifiable information may be required to engage in these activities as well as to receive products and services that you may have requested.

- No - the policy explicitly states that the website will not collect contact information.
- Yes - the policy explicitly states that the website might collect contact information.
- Unclear - the policy does not explicitly state whether the website might collect contact information or not, but the selected sentences could mean that contact information might be collected.
- Not applicable - this question is not addressed by this policy.

Your Progress

Jump directly to question ->

Search this policy
Interpretation of privacy policies

• Comparative annotation study with privacy policy experts, skilled annotators, AMT Crowdworkers on 6 privacy policies

• Result Highlights
  • Data collection relatively easy to identify
  • Data sharing practices more difficult
  • Even experts do not always agree
  • Finer nuances difficult to extract
  • Policy language too ambiguous

Nobody wants to read privacy policies

- Research needed to develop:
  - concise formats for showing policies
  - tools for alerting users of policy mismatches
    - integrated with normal functionality (e.g., web search)
  - tools to extract information from human-readable policy