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

Lorrie Cranor, Blase Ur, and Rich Shay w/ special guest Florian Schaub

March 17, 2015

05-436 / 05-836 / 08-534 / 08-734
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”

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


Privacy label for Android

Privacy score
10,000+ downloads
1.9MB

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 comment

comment
Ad supported, with ability to upgrade to ad-free full version in game.

Uses the SOWPODS word list containing 100,000+ words. They may be obscure, but yes those are words!

Privacy Facts
THIS APP COLLECTS YOUR
✔ Personal information
✔ Contacts
✔ Location
☐ Calendars
☐ Photos

THIS APP USES
☐ Advertising
✔ Analytics

REVIEWS
Average
4.6
5 stars
793
4 stars
534
3 stars
210
2 stars
37
1 star
5
http://www.azarask.in/blog/post/privacy-icons/ 2010

Privacy Icons

Your Data is Used Only for the Intended Use

Your Data May be Used for Purposes You Do Not Intend

Your data is never given to advertisers.

Site gives your data to advertisers.

Your data is never bartered or sold.

Your data may be bartered or sold.

Data is given to law enforcement only when legal process is followed.

Data may be given to law enforcement even when legal process is not followed.

Your data is kept for less than 1 month.

Your data may be kept indefinitely.
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
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.
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
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

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

Policy Summary

Shane Cranor’s Home Page Privacy Practices

Privacy Policy Check

Shane Cranor’s Home Page’s privacy policy matches your preferences.

Privacy Policy Summary

This site has the following statements in its policy:

- Site Statement 1

Site Statement 1

Types of Information Collected:

- HTTP protocol information
- Click-stream information

How your information will be used:

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

Who will use your information:

- This web site and its agents
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.
Privacy Policy Summary
- Policy Statement 1 - Basic Information
  Data collected from all Web users: access logs, and search strings (if entered).
- Policy Statement 2 - Data Collection
  - Access to your information
    This site allows you to access your data about you from its records
  - How to reach this site
  - How to resolve privacy-related issues

More Information

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
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)
Example:
Sending flowers

PICKS OF THE WEEK:

- FTD® Star Gazer™ Bouquet #3064X $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
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:

  CAO DSP COR CURa ADMa DEVa OUR IND PHY ONL UNI COM NAV INT DEM PRE

- Examples of invalid policies accepted by IE:

  AMZN

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.
Towards Usable Privacy Policies:
The Usable Privacy Policies Project

Florian Schaub
March 17, 2015
Why privacy policies?

• Transparency about a service provider’s data practices
• Notice & Choice framework in the US
• Informed(?) user consent

• Goal: Reduce power asymmetry between provider and user
Proposals to improve notices

- Summary interfaces and layered privacy policies
  - e.g. privacy nutrition labels, short notices, privacy icons
- Machine-readable privacy policies (e.g. P3P, DNT)

Proposals to improve notices

- Summary interfaces and layered privacy policies
  - e.g. privacy nutrition labels, short notices, privacy icons
- Machine-readable privacy policies (e.g. P3P, DNT)
- Lack of industry support & adoption incentives

The Usable Privacy Policies Project

- NSF SaTC Frontier project (3.5 years)
- Principal investigators:
  - Norman Sadeh (Lead PI, CMU)
  - Alessandro Acquisti (CMU)
  - Travis Breaux (CMU)
  - Lorrie Cranor (CMU)
  - Aleecia McDonald (Stanford)
  - Joel Reidenberg (Fordham)
  - Noah A. Smith (CMU)

www.usableprivacy.org
Our approach

• Semi-automatically extract data practices from privacy policies by combining crowdsourcing, machine learning & natural language processing

• Understanding and modeling user’s privacy preferences to focus on data practices users care about

• Provide effective user interfaces for privacy notices

• Large-scale analysis of website privacy policies
General idea

A website’s privacy policy

Crowd sourcing

Natural language processing

Machine learning

More effective privacy notices for users

Website’s extracted data practices
Overall Approach

Natural Language Privacy Policies of Websites

Semi-Automated Extraction of Privacy Policy Features

Extracted Data Practices

Policy Analysis

Inform Public Policy

Understand Users’ Privacy Preferences & Needs

Identification and generation

Effective User Interfaces for Privacy Notices

Inform Internet Users

Relevant Features of Privacy Policies

User Privacy Profiles

Support personalization

user-centered design process

Inform Internet Users

Extracted Data Practices

privacy practices to be presented to user

Policy Analysis

features for which to elicit user preferences

Natural Language Privacy Policies of Websites

features for which to elicit user preferences

Semi-Automated Extraction of Privacy Policy Features

policy features to be extracted

Extracted Data Practices

formal models

inform internet users

Inform Public Policy

inform public policy

Extracted Data Practices

privacy practices to be presented to user

Effective User Interfaces for Privacy Notices

user-centered design process

relevant features of privacy policies

Semi-Automated Extraction of Privacy Policy Features

inform internet users

Inform Internet Users

Support personalization

formal models

Semantic features

Florian Schaub
Usability Aspects

Design usable crowd-sourcing tasks

Natural Language Privacy Policies of Websites

Semi-Automated Extraction of Privacy Policy Features

Extracted Data Practices

Policy Analysis

Inform Public Policy

Understand what data practices are relevant

Understand Users’ Privacy Preferences & Needs

Identification and generation

Relevant Features of Privacy Policies

User Privacy Profiles

Effective User Interfaces for Privacy Notices

Inform Internet Users

Design usable notices

florian.schaub@cmu.edu

Inform Public Policy

Semi-Automated Extraction of Privacy Policy Features

Extracted Data Practices

Policy Analysis

Effective User Interfaces for Privacy Notices

Inform Internet Users
Usability Aspects

Design usable crowd-sourcing tasks

Natural Language Privacy Policies of Websites

Semi-Automated Extraction of Privacy Policy Features

Extracted Data Practices

Policy Analysis

Inform Public Policy

Understand Users’ Privacy Preferences & Needs

identification and generation

relevant features of privacy policies

User Privacy Profiles

Effective User Interfaces for Privacy Notices

Inform Internet Users

extracted data practices

privacy practices to be presented to user

policy analysis

features for which to elicit user preferences

inform public policy

relevant features of privacy policies

effective user interfaces for privacy notices

inform internet users

semi-automated extraction of privacy policy features

formal models

semantic features

inform public policy
Relevant data practices

- Analysis of 165 US federal class action cases
- Analysis of 116 FTC enforcement complaints
  - Unauthorized disclosure of personal information
  - Surreptitious collection of personal information
  - Unlawful retention of personal information
  - Failure to secure personal information

- Prior studies on privacy preferences & concerns
  - information types: contact, location, financial health

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

The image shows a user interface for a privacy policy annotation tool. The tool allows users to search for specific policies and answer questions about the policies. The example policy shown is from time.com and includes a question about whether the website might collect contact information about its users.
Privacy policy annotation tool

• Iterative design
• Goals & insights
  • policy and questions visible at same time
  • clear & accessible instructions
  • sequential and go-to navigation
  • sentence selection with undo
  • concise questions & response options, yet understandable
  • keyword definitions
  • unclear is a valid answer
Annotation results

collection of contact information

2x Yes: The policy explicitly states that the website might collect contact information

6x Unclear: The policy does not explicitly state whether the website might collect contact information or not

The Information We Collect

At some Turner Network sites, you can order products, enter contests, vote in polls or otherwise express an opinion, subscribe to one of our services such as our online newsletters, or participate in one of our online forums or communities. In the course of these various offerings, we often seek to collect from you various forms of personal information. Examples of the types of personally identifiable information that may be collected at these pages include: name, address, e-mail address, telephone number, fax number, credit card information, and information about your interests in and use of various products, programs, and services.

At some Turner Network sites, you may also be able to submit information about other people. For example, you might submit a person's name and e-mail address to send an electronic greeting card from our site.
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

How good are crowdworkers?

- Only considering answers where 8 of 10 crowdworkers agree:
  - 76% of cases: they agree on *same answer as experts*
  - 2% of cases: they agree on different answer than experts*
  - 22% of cases: crowdworkers do not reach agreement

Crowdworkers agree with experts or not at all

*3 of 4 experts agree on same answer in 90.1% of cases

Predicting & highlighting relevant paragraphs

This Privacy Statement describes the types of personal information we collect on the Site, how we may use that information and with whom we may share it. The Privacy Statement also describes the measures we take to protect the security of the personal information. We also tell you how you can reach us to ask us to update your preferences regarding how we communicate with you or answer any questions you may have about our privacy practices.

Information We Collect

You may choose to provide us with personal information (such as name, contact details and payment information), such as:

- Contact information, such as your name, address, telephone number, and email address, and your title or occupation.
- Login and access credentials (such as username and password) for Lowe's accounts.
- Payment information, such as your payment card number and expiration date.
- Date of birth.
- The geolocation of your device (such as if you opt to use the “Find Near Me” feature of the mobile-optimized portion of our websites or our Mobile Applications).
- The unique ID number associated with certain Lowe's accounts.

Answer the following questions

Question 2:
Does the policy state that the website might collect financial information about its users?

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

- Analysis of sentences selected by experts and skilled annotators
  - 110 data practice specific regular expressions
  - Logistic regression to rank paragraphs based on probability of containing the answer to question x
  - Regression features: regex matches, n-grams

- Evaluation study with crowdworkers
  - between subjects crowdworkers (no, 5 or 10 highlights)
  - compared to skilled annotator gold standard data
Highlighting experiment results

- 10 highlights increase accuracy
- 5 highlights significantly faster, but less accurate
- Workers still select text from non-highlighted parts
- Self-reported understanding of legal text increases

<table>
<thead>
<tr>
<th>Condition</th>
<th>Correct</th>
<th>Wrong</th>
<th>No Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOHIGH</td>
<td>76 (84.4%)</td>
<td>4 (4.4%)</td>
<td>10 (11.1%)</td>
</tr>
<tr>
<td>TOP05</td>
<td>74 (82.2%)</td>
<td>9 (10 %)</td>
<td>7 (7.8 %)</td>
</tr>
<tr>
<td>TOP10</td>
<td>81 (90.0%)</td>
<td>3 (3.3%)</td>
<td>6 (6.7 %)</td>
</tr>
</tbody>
</table>
Challenges

- Long completion times
- Adapt number of workers to question difficulty
- Interpretative ambiguity
Annotation task workflow
Annotation task workflow

segment policy into paragraphs

categorize content of paragraphs

category-specific follow-up tasks & questions
Categorize paragraphs

This is a paragraph from the privacy policy of nytimes.com
Select all categories that fit.

To enable payment and donations via the NYT Services, we collect and store name, address, telephone number, email address, credit card information and other billing information. This information will only be shared with third parties who help to complete the purchase transaction. Examples of this include fulfilling orders and processing credit card payments.

- [ ] collection: information is collected by the main website or provided by the user
- [ ] sharing: information is collected by or shared with a third party
- [ ] purpose: why information is being collected, shared, etc. or what it is used for
- [ ] consent: any choices or privacy controls offered to users (opt-in, opt-out, etc.)
- [ ] other: the paragraph talks about other topics or aspects

submit
This is a paragraph from the privacy policy of nytimes.com.
Select all categories that fit.

To enable payment and donations via the NYT Services, we collect and store name, address, telephone number, email address, credit card information and other billing information. This information will only be shared with third parties who help to complete the purchase transaction. Examples of this include fulfilling orders and processing credit card payments.

- collection: information is collected by the main website or provided by the user
- sharing: information is collected by or shared with a third party
- purpose: why information is being collected, shared, etc. or what it is used for
- consent: any choices or privacy controls offered to users (opt-in, opt-out, etc.)
- other: the paragraph talks about other topics or aspects

Submit
Category-specific follow-up tasks

• For each label ask label-specific follow-up questions
• Worker selects answer option and marks respective text.
  • Example: collection
    • What information collected?
    • For what purpose?
  • Example: third party sharing
    • Shared with whom?
    • For what purpose?
    • Use limitations?
Category-specific follow-up tasks

Response options for categorization

Select relevant words and press button

Advantages & Challenges

• Fine-granular annotation rather than holistic interpretation

• Recombination of results
• Disambiguating scope
• Determining the required number of annotators
Effective Privacy Notices

- Natural Language Privacy Policies of Websites
- Understand Users’ Privacy Preferences & Needs
- Semi-Automated Extraction of Privacy Policy Features
- Relevant Features of Privacy Policies
- Extracted Data Practices
- User Privacy Profiles
- Policy Analysis
- Support personalization
- Iterative design
- Effective User Interfaces for Privacy Notices
- Inform Public Policy
- Design usable notices
- Inform Internet Users
Existing Privacy Notices & Browser Extensions

Florian Schaub

Access to your information
This site gives you access to your contact data and some of its other data identified with you.

How to resolve privacy-related disputes with this site
Please email our customer service department: bellgroup.com 5000 Forbes Avenue Pittsburgh, PA 15213 United States Phone: 800-555-BELL help@bellgroup.com

we will collect and use your information in this way by default, we will not collect and use your information in this way unless you allow us to by opting in

For our everyday business purposes such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus
For our marketing purposes to offer our products and services to you
For joint marketing with other financial companies
For our affiliates’ everyday business purposes information about your transactions and experiences
For our affiliates’ everyday business purposes information about your creditworthiness
For our affiliates to market to you
For nonaffiliates to market to you

We believe a precise balance between the competing pressures of privacy, the security of our systems, and the need for innovation. We believe accepting IP addresses after 8 months and cookies in our search engine logs after 18 months preserves the privacy balance. Today, these intervals of time were gone from the Privacy Policy, although some pages still acknowledge this. So we must conclude that Google has decided to stop trying to find the right balance between privacy of users and our own needs.

Limited copyright license to operate and improve all Google Services

Terms of Service
Don’t Trust
The terms of service are only but some issues need your consideration.

Google collects a lot of information about the services you use and how you use them, including when you visit a website using Google’s search service for advertising. Google stores data in their Privacy Policy. We strive for a reasonable balance between the competing pressures of privacy, the security of our systems, and the need for innovation. In particular, we believe accepting IP addresses after 8 months and cookies in our search engine logs after 18 months preserves the privacy balance. Today, these intervals of time were gone from the Privacy Policy, although some pages still acknowledge this. So we must conclude that Google has decided to stop trying to find the right balance between privacy of users and our own needs.
### Version 0

<table>
<thead>
<tr>
<th></th>
<th>Collection</th>
<th>Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact</strong></td>
<td>Yes 90%</td>
<td>No agreement reached</td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td>Yes 80%</td>
<td>Not applicable 60%</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Yes 60%</td>
<td>No agreement reached</td>
</tr>
<tr>
<td><strong>Health</strong></td>
<td>Not applicable 70%</td>
<td>Not applicable 90%</td>
</tr>
<tr>
<td><strong>Deletion</strong></td>
<td>Unclear 80%</td>
<td></td>
</tr>
</tbody>
</table>
Goals

• Browser extension showing extracted data practices
  • Provide relevant information to users
  • Easy to understand
  • Make information actionable
  • Enable meaningful comparisons

• Collect users’ needs
• Encourage users to contribute annotations
• Enable website operators to clarify practices
Design considerations

• Emphasize unexpected data practices
• Provide assessment of data practices
• Provide alternatives
• Avoid jargon and use simplified non-technical wording
• Leverage interactions (e.g., expandable menus, details on demand)
• Encourage users to contribute to annotations
Mockup 1

- Overall assessment & relative comparison
- summary of user choices
- summary of data practices
- summary rating per category
- user feedback & contribution

**Your Choices:**

- Find a privacy-respectful website: [Find site]
- Block Third-party Trackers: Block Trackers
- Limit Third-party Sharing: [URL/email/unavailable]
- Limit unrequested Marketing: [URL/email/unavailable]
- Limit Profiling: [URL/email/unavailable]

**What this website does?**

- **Third-parties:** Low Protection Learn more
  - Website shares your information with third-parties, you can't limit it
  - Third-parties collect your information on this website, you can limit it
  - Trackers detected on this website
- **Secondary Uses:** Low Protection Learn more
  - Website will send you marketing propaganda, you can't limit it
  - Website may treat you different based on what it learns about you, you can't limit it
  - Website may use your information for other unspecified purposes
- **Profile Management:** Low Protection Learn more
  - You can't delete your user account
  - You can't delete information that the website has collected from you
- **Data Collection:** Low Protection Learn more
  - Website collects your location
  - Website logs more than what is minimally needed to provide service
- **Policy Changes:** Low Protection Learn more
  - Website may change its data practices at any time without providing adequate notice and choices to you
  - Your information may be sold or transferred if the company is acquired by another company without providing adequate choices to you

Dislike anything or want to learn more about this website? Click Here

The Usable Privacy Project

Florian Schaub

Carnegie Mellon University
Mockup 2

- highlight some practices
- choices and practices integrated
- slider interface to expand practices
- reduced text

NYTimes may treat your data badly
based on current privacy policy from Jan 15, 2015
most news sites do better!

why?

- **No limits on data use**
The website may use your data for any purpose.
Risk: they could sell your data to advertisers

- **Sharing with third parties**
The website shares your data with others, namely advertisers and law enforcement.
Risk: you can’t control who gets your data

- **Few trackers**
Some other websites and companies can track you on this website.
Risk: you may not know these trackers, but they learn a lot about you

---

Concerned? Tell us!
We will contact the website for you anonymously
Mockup 3

- sorted by good, bad, unclear data practices

NYTimes may treat your data badly
based on current privacy policy from Jan 15, 2015
most news sites do better!

Click to see & control what NYTimes
can do with your data

<table>
<thead>
<tr>
<th>good privacy practices</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>the website informs users about policy changes.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>unexpected privacy practices</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>no limits on how data can be used. data sharing with advertisers.</td>
<td></td>
</tr>
</tbody>
</table>

- **No limits on data use**
The website may use your data for any purpose.
Risk: they could sell your data to advertisers

- **Sharing with third parties**
The website shares your data with others, namely advertisers and law enforcement.
Risk: you can’t control who gets your data

<table>
<thead>
<tr>
<th>unclear &amp; unknown practices</th>
<th>1</th>
</tr>
</thead>
</table>

Concerned? Tell us!
We will contact the website for you anonymously
Mockup 4

- emphasize comparison

<table>
<thead>
<tr>
<th>Website's Data Practices:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-parties: <strong>Worse than similar sites</strong> [Compare]</td>
</tr>
<tr>
<td>Secondary Uses: <strong>Worse than similar sites</strong> [Compare]</td>
</tr>
<tr>
<td>Profile: <strong>Worse than similar sites</strong> [Compare]</td>
</tr>
<tr>
<td>Data Collection: <strong>Same as similar sites</strong> [Compare]</td>
</tr>
<tr>
<td>Policy Changes: <strong>Same as similar sites</strong> [Compare]</td>
</tr>
</tbody>
</table>
Mockup 5

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

NYTimes’ privacy rating

based on current privacy policy, last updated on Jan 15, 2015

most news sites do better!
here are some privacy-friendly alternatives:
– WashingtonPost.com (A++)
– The Guardian (A+)
– HuffingtonPost.com (A)

NYTimes Privacy Practices in Detail
Click a category to see & control what NYTimes can do with your data

<table>
<thead>
<tr>
<th>Category</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>data collection</td>
<td>A</td>
</tr>
<tr>
<td>third parties</td>
<td>D</td>
</tr>
<tr>
<td>choices &amp; control</td>
<td>B</td>
</tr>
</tbody>
</table>

Concerned? Tell us!
We will contact the website for you anonymously
Mockup 6

visual ranking of alternatives

visualize average

overall ranking and for data practices

average comparisons

Florian Schaub

Carnegie Mellon University
Next steps

- Refine plugin design and build functional prototypes
- 2-4 focus groups
  - test and refine terminology and main UI elements
  - participatory design
- Lab study
  - within subjects study to assess usability of few different variants
- Online or field study
  - evaluate final extension at large scale and in different website contexts
Take-aways

• Semi-automatic extraction of data practices from privacy policies with crowdsourcing and NLP/ML

• Provide notices that are relevant, understandable, and actionable

• Truly interdisciplinary effort

Norman Sadeh et al., The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About, Tech. report CMU-ISR-13-119, CMU, December 2013
http://reports-archive.adm.cs.cmu.edu/anon/isr2013/abstracts/13-119.html