11. Privacy Notice and Choice

Blase Ur and Mainack Mondal
April 30th, 2018
CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO

Security, Usability, & Privacy
Education & Research
Today’s class

• Discuss projects
• Privacy notice and choice
Project suggested paper structure

- Abstract
- Introduction
- Related work
- Methodology
- Pilot results
- Lessons learned (for moving forward)
- Discussion / limitations / conclusion
Privacy notice & choice
Fair Information Practice Principles

(US Federal Trade Commission)

1. Notice / awareness
2. Choice / consent
3. Access / participation
4. Integrity / security
5. Enforcement / redress
About Our Privacy Policy

Wherever you do something like buy one of our products, watch a video, or make a call, your personal information is created. Because we know your privacy is important to you, we want to explain how we collect, use and protect that information. The policy is written in an easy to understand format. We want to simplify our language to make informed choices about your privacy, and then spend the right amount of time on products and services.

Effective July 24, 2015

A Quick Summary of Our Policy

Our Privacy Policy applies to your use of all products, services, and our AT&T affiliated sites, such as DIRECTV, unless they have a separate privacy policy. Because some apps, including some AT&T and DIRECTV branded apps, use information in different ways, they may have their own terms and conditions. These apps may also offer you additional privacy controls.

Back to Top

Our privacy commitments:

- We don't sell your personal information to anyone for any purpose. Period.
- We keep your personal information in our business records while you're a customer, or until it is no longer needed for business, tax or legal purposes.
- We will keep your information safe using encryption or other appropriate security controls.
Learn at inappropriate times
Misconceptions
Lack of understanding
Lack of choices
Habituation
Time to read policies of websites you visit: 244 hours/year.

“Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent”
Tools of FTC in US

• Unfair practices
  – Injure consumer
  – Violate established policy
  – Unethical

• Deceptive practices
  – Mislead consumer
  – Differ from reasonable consumer expectations
Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices

Settlement ensures consumers can control targeted ads

FOR RELEASE
December 20, 2016
Choice/Opt Out

Opting out of email communications (promotional, free email newsletters, and Ratings alerts)

If you subscribe to any of our paid products or services (for example, Consumer Reports magazine or ConsumerReports.org), our free email newsletters (for example, those about cars, finance, drugs or safety issues) or our Ratings alerts, we may send you promotional emails about our other products and services or to ask you about your experience.

Opting out online
You can opt out of receiving these email communications from us by following the instructions provided at the bottom of each email. If you use this method, you will stop receiving only that particular type of email message.

If you are a subscriber to one of our paid products or services, you can manage your email communication preferences on your "My Account" page by clicking here (or by going to www.consumerreports.org/myaccount).
Evernote's new not-so-privacy policy will let employees read your notes

The note-taking app will let humans (and not just machines) sift through your private data.

It’s getting worse
Simplified notice and choice

“the question is not whether consumers should be given a say over unexpected uses of their data; rather, the question is how to provide simplified notice and choice.”

Edith Ramirez
Former FTC Chairwoman
January 2015
Speaking about IoT privacy
EU General Data Protection Regulation (effective 5/25/18)

• “have transparent and easily accessible policies”

• “provide any information… in an intelligible form, using clear and plain language, adapted to the data subject”

• Request consent in a way that is “clear, concise, and not unnecessarily disruptive”
How can we put people in control over their personal information?
Privacy Notice Design Space
Privacy notice design space

F. Schaub, R. Balebako, A. Durity, L.F. Cranor, A Design Space for Effective Privacy Notices, SOUPS’15
privacy notice

- timing
  - at setup
  - just in time
  - context-dependent
  - periodic
  - persistent
  - on demand

- channel
- modality
- control
privacy notice

**timing**
- at setup
- just in time
- context-dependent
- periodic
- persistent
- on demand

**channel**

**modality**

**control**

---

“Cluster” Would Like to Access Your Contacts
This allows Cluster to let you choose which friends to invite to shared photo albums.

Don’t Allow  OK

Cookies on the BBC website
We use cookies to ensure that we give you the best experience on our website. If you continue without changing your settings, we’ll assume that you are happy to receive all cookies on the BBC website. However, if you would like to, you can change your cookie settings at any time.

Continue  Find out more
privacy notice

timing
- at setup
- just in time
- context-dependent
- periodic
- persistent
- on demand

channel

modality

control

Privacy Checkup

Hi Charlie — Sorry to interrupt. You haven’t changed who can see your posts lately, so we just wanted to make sure you’re sharing this post with the right audience. (Your current setting is Public, though you can change this whenever you post.) Learn more.

Who do you want to share this post with?

Friends  Public  More Options
privacy notice

**Timing**
- at setup
- just in time
- context-dependent
- periodic
- persistent
- on demand

**Channel**

**Modality**
- periodic
- persistent
- on demand

**Control**
privacy notice

**timing**
- at setup
- just in time
- context-dependent
- periodic
- persistent
- on demand

**channel**

**modality**

**control**
privacy notice

- timing
  - at setup
  - just in time
  - context-dependent
  - periodic
  - persistent
  - on demand

- channel

- modality

- control
privacy notice

- timing
- channel
  - primary
  - secondary
  - public
- modality
- control
privacy notice

- timing
- channel
  - primary
  - secondary
  - public
- modality
- control

The WP Company LLC ("The Washington Post") recognizes the importance of protecting the privacy of your personal information, and we have developed this Privacy Policy to provide you with important information about our privacy practices. This Privacy Policy applies when you use a website, mobile application, or other online service (collectively, the "Services") unless otherwise restricted by the terms of use or privacy settings. If the Services link to or otherwise refers to another website or application, this Privacy Policy does not govern or apply to information collected or processed by such websites or applications. For more information, please refer to our terms of use and privacy settings.
privacy notice

- timing
- channel
  - primary
  - secondary
- modality
  - public
- control

Diagram showing various devices and icons related to privacy notice, timing, channel, modality, and control.
privacy notice

- timing
- channel
  - primary
  - secondary
- modality
  - public
- control

http://www.offlinetags.net/
privacy notice

- timing
- channel
- modality
  - visual
  - auditory
  - haptic
  - machine-readable
- control
privacy notice

- timing
- channel
- modality
  - visual
  - auditory
  - haptic
  - machine-readable
- control

"this call will be recorded for training purposes"
The Platform for Privacy Preferences 1.1 (P3P1.1) Specification
W3C Working Group Note 13 November 2006
privacy notice

- timing
- channel
- modality

control
- blocking
- non-blocking
- decoupled
privacy notice

- timing
- channel
- modality
- control
  - blocking
  - non-blocking
  - decoupled
privacy notice

- timing
- channel
- modality

control
- blocking
- non-blocking
- decoupled
Layered examples from iOS

just-in-time, primary visual, blocking

persistent, primary visual, non-blocking

at setup, primary visual, blocking

on demand, primary visual, decoupled

on demand, secondary visual, decoupled
Attempts at improving notice & choice
Attempt: Machine-readable privacy policies
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 Internet Explorer

• P3P implemented in IE 6, 7, 8, 9, 10 …

• Default privacy setting
  – Rejects third-party cookies without a CP
  – Rejects unsatisfactory third-party cookies
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

Merrell Primo Chill Slide - Men's Tan: Merrell Shoes
Buy Merrell Primo Chill Slide - Men's Tan and find Spring trends at Onlineshoes. Free Shipping and Exchanges on all Merrel!...
http://yhs.trafficdashboard.com/track.htm?id=1031... - Privacy Policy - Similar Pages

$89.95

merrell® Primo Chill Slide Shoes, Chocolate, Women's
Italian styled winter slide for convenience and warmth. Easy-on and water resistant, the Primo Chill gives your feet after-sport comfort in casual style. Water-resistant pigskin leather upper with sheepskin lining. Removable wool fleece footbed. Injection-molded nylon shank for increased arch support. Air Cushion EVA midsole for softer flex and increased comfort. Merrell Pilot sole with sticky rubber sports a weight-saving design that is siped and barred for traction....
http://clickserve.cc-dt.com/link/ddiprod?id=41000... - Privacy Policy - Similar Pages

$90.00

Merrell Primo Chill Slide
http://shopping.yahoo.com/p:Merrell%20Primo%20Chill... - Privacy Policy - Similar Pages

$89.95 - $89.95

Merrell Primo Chill Slide (Men's)
We heated up our stylish Italian standout slide with a sheepskin lining with removable footbed and a water resistant pigskin upper. Merrell Pilot Sole has a weight-saving cutaway configuration but is boldly siped and barred for wet and dry surface traction. FEATURES: Slip Lasted Construction, Water Resistant Pigskin Upper, Sheepskin Lining, Wool Fleece Foot-Bed, Nylon 6.6 Injection Molded Arch Shank, Compression Molded EVA Foot-Frame, Air Cushion Mid-Sole, Merrell Pilot Sole/Sticky Rubber. Available Colors: Black, Chocolate, Natural, Tan. J63253....
http://www.shoebuy.com/cgi-bin/abref.cgi?link=yps&... - Privacy Policy - Similar Pages

$99.95

Merrell Shoes Primo Chill Slide - Men’s
Why limit your casual winter footwear wardrobe to unimaginative, straight-laced shoes? Merrell's Primo Chill Slides offer the slip-in convenience of traditional post-sport footwear.
Impact of privacy information on decision making

- Online shopping study conducted at CMU lab
- Paid participants to make online purchases with their own credit cards, exposing their own personal information
- Participants paid fixed amount and told to keep the change – real tradeoff between money and privacy
- Studies demonstrate that when readily accessible and comparable privacy information is presented in search results, many people will pay more for better privacy


http://privacyfinder.org/
Attempt: Personalized privacy assistants
Personal privacy assistants
Attempt: Make your own machine-readable privacy policies
Use NLP to read policies

• Usableprivacy.org

• It’s a hard problem

• Annotated corpus → machine learning
Attempt: Crowdsourcing
Terms of Service; Didn’t Read

**SoundCloud (Class B)**

- You stay in control of your copyright
- Collected personal data used for limited purposes
- 6 weeks to review changes
- Indemnification from claims related to your content or your account
- Personal information can be disclosed in case of business transfer or insolvency

[More details](#)

**GitHub (Class D)**

- You don’t grant any copyright license to GitHub
- Changes can happen any time, sometimes without notice
- You shall defend and indemnify GitHub
- Your personal information is used for limited purposes
- Your account can be suspended and your data deleted any time for any reason

[More details](#)

**Twitpic (Class E)**

- Twitpic takes credit for your content
- Your content is for Twitpic and their partners
- Reduction of legal period for cause of action
- You indemnify Twitpic from any claim related to your content
- Deleted images are not really deleted

[More details](#)

**Delicious (Class D)**

- Very broad copyright license on your content, includes right for Delicious to distribute through any media
- No Right to leave the service
- Only for personal and non-commercial use
- [bad] delicious new terms 5. third party services get access to personal information
- Your personal information are an asset for business transfers

[More details](#)
Attempt: Standardized notices
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


Standardized financial notices

- Gramm-Leach-Bliley Act mandated annual disclosures
- In 2009, regulators created a recommended form
  - High adoption because of safe harbor
### Standardized financial notices

**Facts**

**What does [Name of Financial Institution] do with your personal information?**

**Why?**
Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

**What?**
The types of personal information we collect and share depend on the product or service you have with us. This information can include:
- Social Security number and [income]
- [account balances] and [payment history]
- [credit history] and [credit scores]

When you are *no longer* our customer, we continue to share your information as described in this notice.

**How?**
All financial companies need to share customers’ personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers’ personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.
# Standardized financial notices

<table>
<thead>
<tr>
<th>Reasons we can share your personal information</th>
<th>Does [name of financial institution] share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For our marketing purposes—to offer our products and services to you</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For joint marketing with other financial companies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes—information about your transactions and experiences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes—information about your creditworthiness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For our affiliates to market to you</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For nonaffiliates to market to you</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Questions?** Call [phone number] or go to [website]
# Standardized financial notices

## Who we are

**Who is providing this notice?** [insert]

## What we do

**How does [name of financial institution] protect my personal information?**

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.

[insert]

**How does [name of financial institution] collect my personal information?**

We collect your personal information, for example, when you

- [open an account] or [deposit money]
- [pay your bills] or [apply for a loan]
- [use your credit or debit card]

[We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]

**Why can’t I limit all sharing?**

Federal law gives you the right to limit only

- sharing for affiliates’ everyday business purposes—information about your creditworthiness
- affiliates from using your information to market to you
- sharing for nonaffiliates to market to you

State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
### Standardized financial notices

**Definitions**

<table>
<thead>
<tr>
<th><strong>Affiliates</strong></th>
<th>Companies related by common ownership or control. They can be financial and nonfinancial companies.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="affiliate information" /></td>
</tr>
<tr>
<td><strong>Nonaffiliates</strong></td>
<td>Companies not related by common ownership or control. They can be financial and nonfinancial companies.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="nonaffiliate information" /></td>
</tr>
<tr>
<td><strong>Joint marketing</strong></td>
<td>A formal agreement between nonaffiliated financial companies that together market financial products or services to you.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="joint marketing information" /></td>
</tr>
</tbody>
</table>

**Other important information**

![insert other important information](image)
Standardized financial notices

• Built a parser and built an online database
• Lets people compare practices
• https://cups.cs.cmu.edu/bankprivacy
Messing up standardized notices

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and Payment history
- Income and Credit history
- Account balances and Checking account information

When you are no longer our customer, we continue to share your information as described in this notice.

All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Geneva State Bank chooses to share; and whether you can limit this sharing.

<table>
<thead>
<tr>
<th>Reasons we can share your personal information</th>
<th>Does Geneva State Bank share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For our everyday business purposes</strong> - such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For our marketing purposes</strong> - to offer our products and services to you</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For joint marketing with other financial companies</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Attempt: Improve timing
Privacy label for Android

**Word Weasel**

**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

**Privacy score**
793
10,000+ downloads
1.9MB

**Privacy Facts**

- THIS APP COLLECTS YOUR
  - Personal information
  - Location

- THIS APP USES
  - Advertising
  - Analytics

**Reviews**

<table>
<thead>
<tr>
<th>Average</th>
<th>5 stars</th>
<th>4 stars</th>
<th>3 stars</th>
<th>2 stars</th>
<th>1 star</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.6</td>
<td>534</td>
<td>210</td>
<td>37</td>
<td>5</td>
<td>7</td>
</tr>
</tbody>
</table>

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!
Attempt: Icons
Attempt: Standardized disclosure icons
What Do Online Behavioral Advertising Disclosures Communicate to Users?

Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guizi Xu. WPES 2012
The industry claims total success

“The DAA has revolutionized consumer education and choice by delivering a real-time, in-ad notice more than 10 billion times every day through the increasingly ubiquitous DAA Advertising Option Icon (also known as the ‘Ad Choices’ Icon)”

Objectives

• Evaluate the effectiveness of different OBA disclosures at communicating notice and choice about OBA

• Find ways to improve effectiveness of OBA disclosures
Methodology

• Large scale between-subjects online study
  – 1,505 participants
  – Over 100 participants per treatment

• Participants recruited through Amazon Mechanical Turk

• Guided browsing scenario

• Online survey
First exposure to OBA disclosures
Second exposure to OBA disclosures

- Why did I get this ad?
- Interest based ads
- AdChoices
- Sponsor ads
- Learn about your ad choices
- Configure ad preferences
- ‘No tagline’
Do icons and taglines suggest tailored ads?

• To what extent, if any, does this combination of the symbol and phrase, placed on the top right corner of the above ad suggest the following?
  – This ad has been tailored based on websites you have visited in the past. [true]
This ad has been tailored based on websites you have visited in the past

- Why did I get this ad? 80%
- Interest based ads 68%
- Learn about your ad choices 66%
- Configure ad preferences 58%
- AdChoices 58%
- Blank 34%
- Sponsor Ads 26%

Colors:
- Definitely not
- Probably not
- Not sure
- Probably
- Definitely
Takeaways

• OBA icons and taglines are not noticed
• “AdChoices” was outperformed by other tagline treatments at communicating notice and choice about OBA
• Users are afraid to click on icon