

# Privacy Notice and Choice in Practice

Lorrie Faith Cranor  
July 2013



# CyLab Usable Privacy and Security Laboratory



# Carnegie Mellon University

Master of Science in Information Technology

---



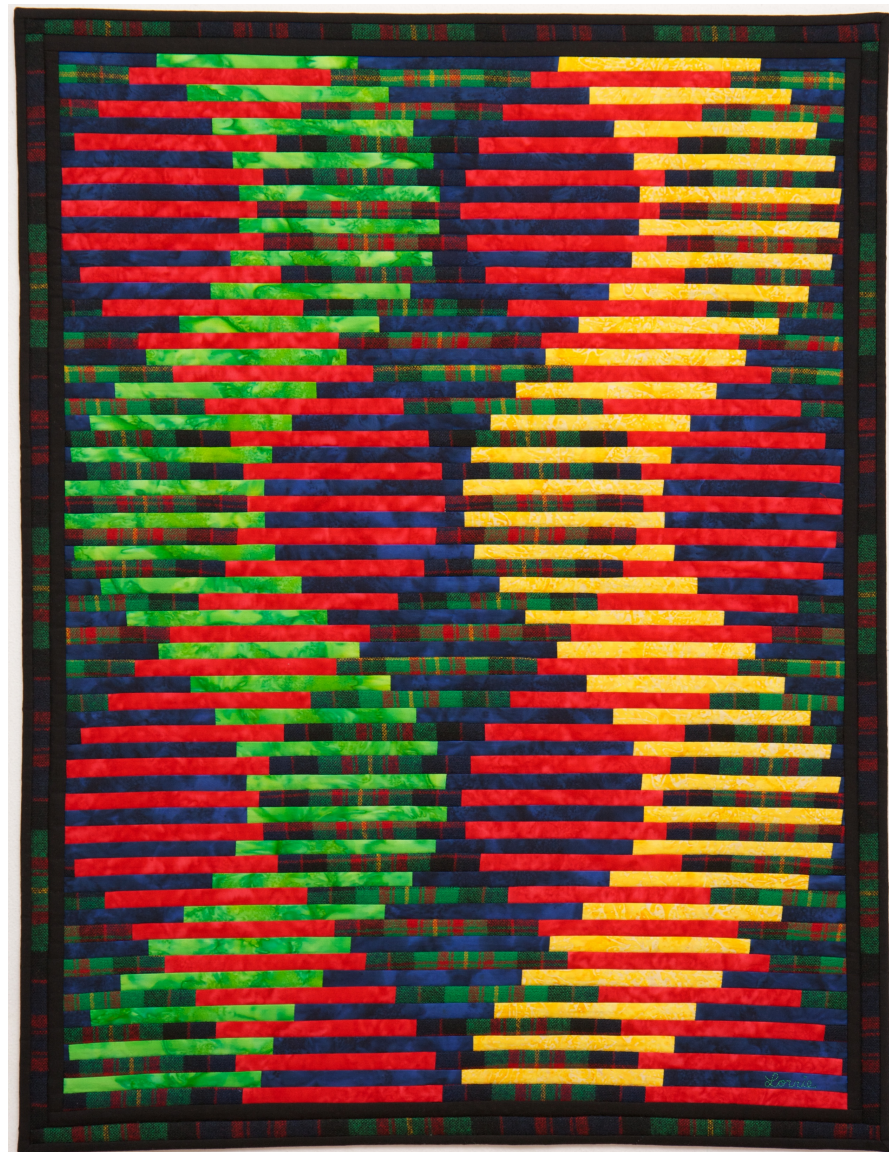
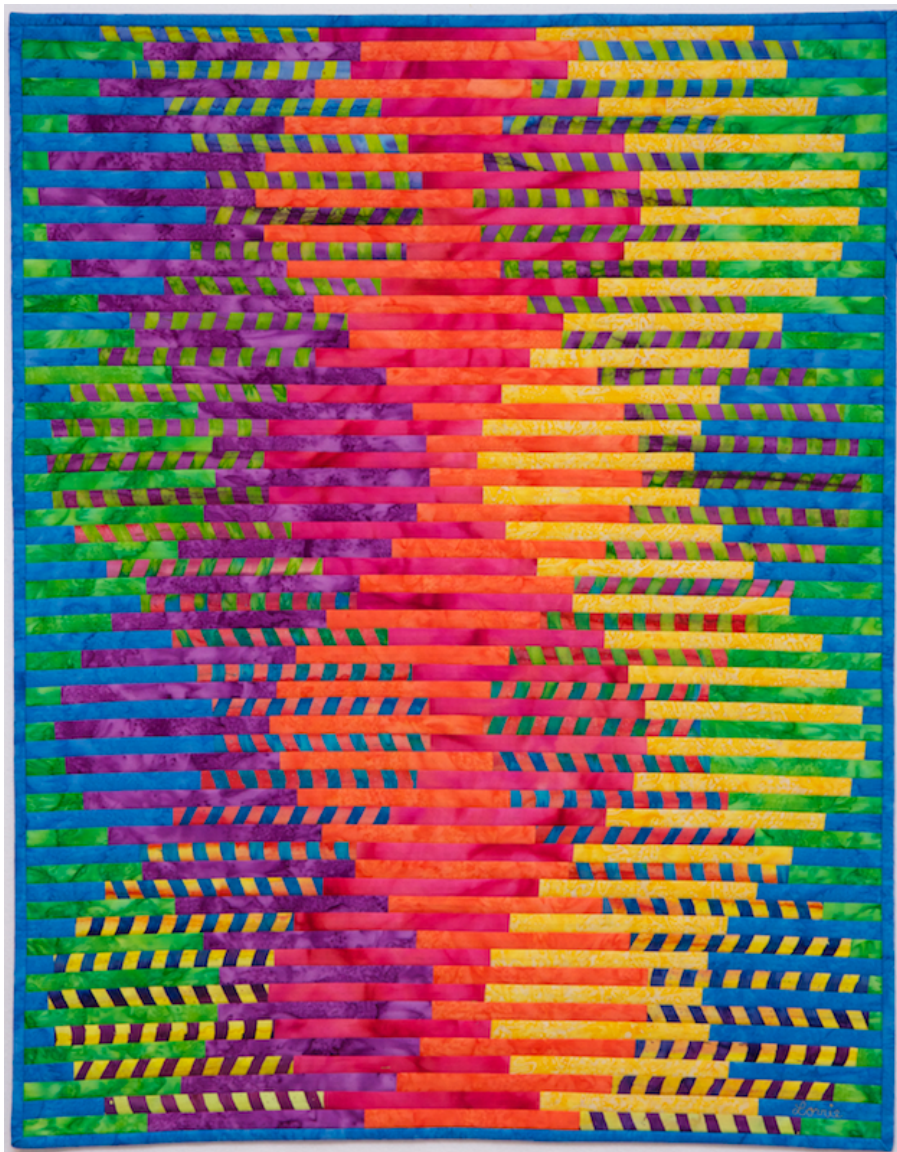
privacy  
ENGINEERING

[privacy.cs.cmu.edu](http://privacy.cs.cmu.edu)

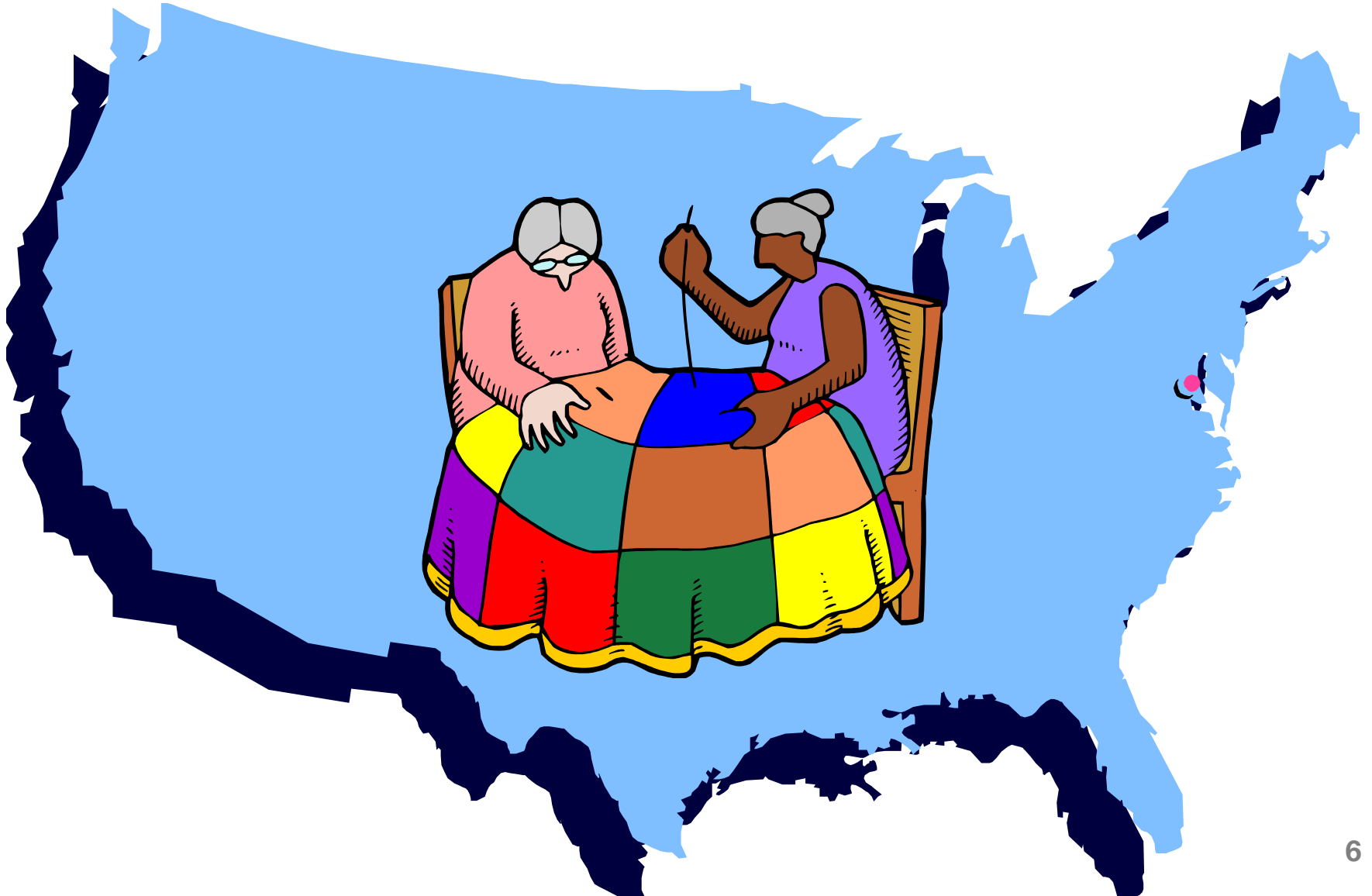








# Patchwork quilt of privacy laws



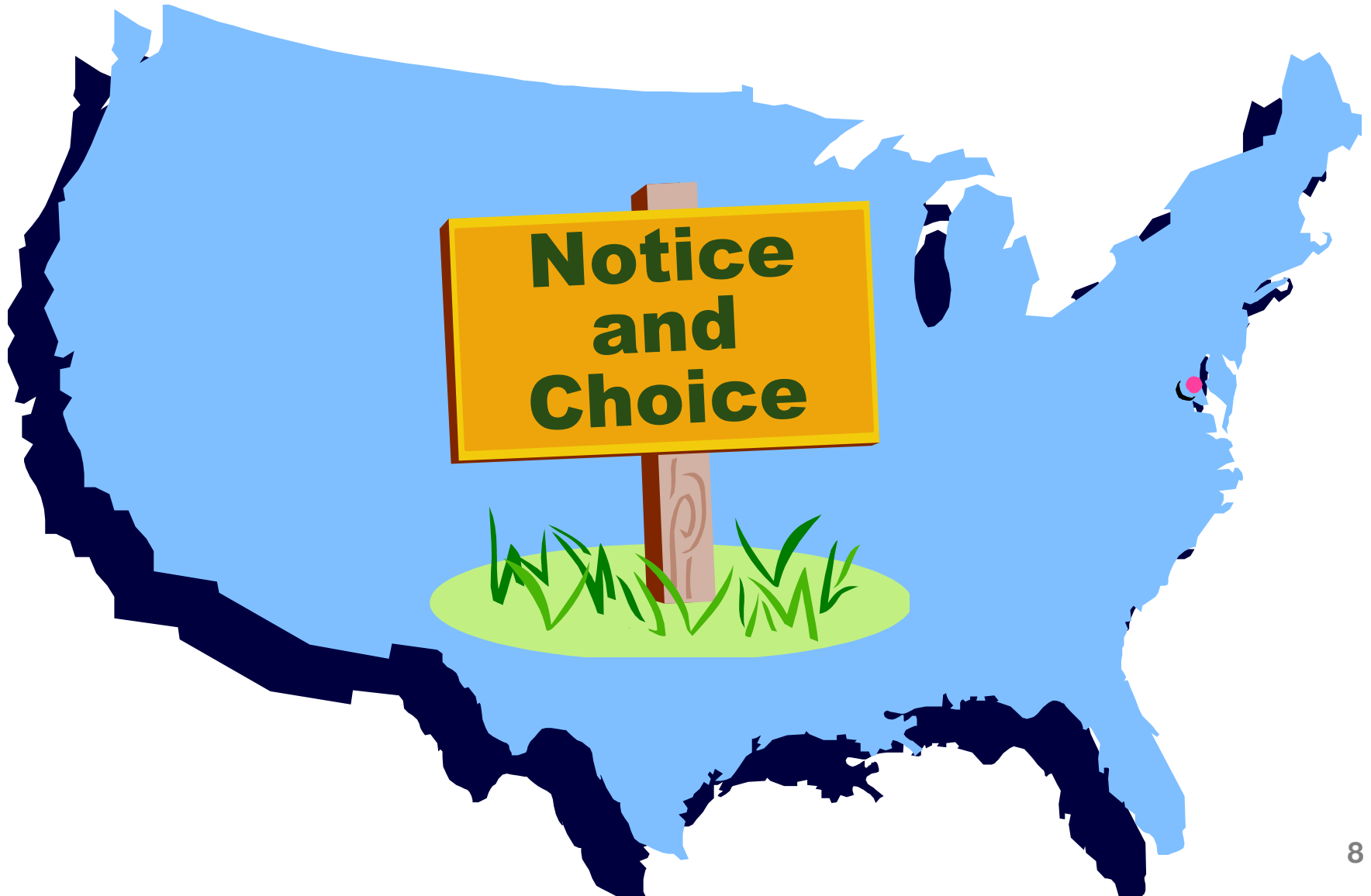
# US government privacy reports

- U.S. FTC and White House reports released in 2012
- U.S. Department of Commerce multi-stakeholder process to develop enforceable codes of conduct





# Privacy self regulation

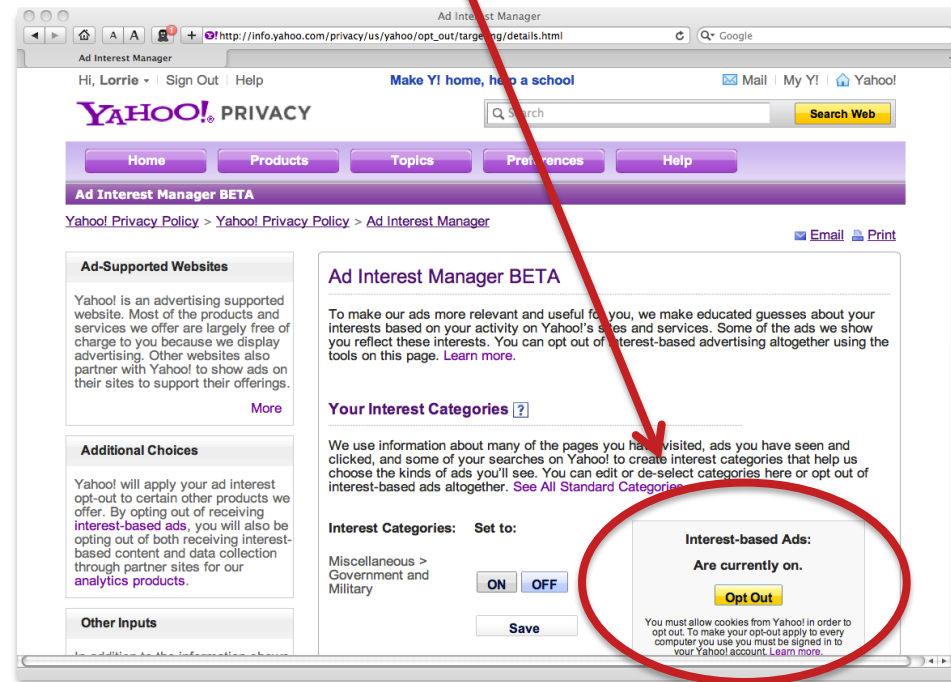
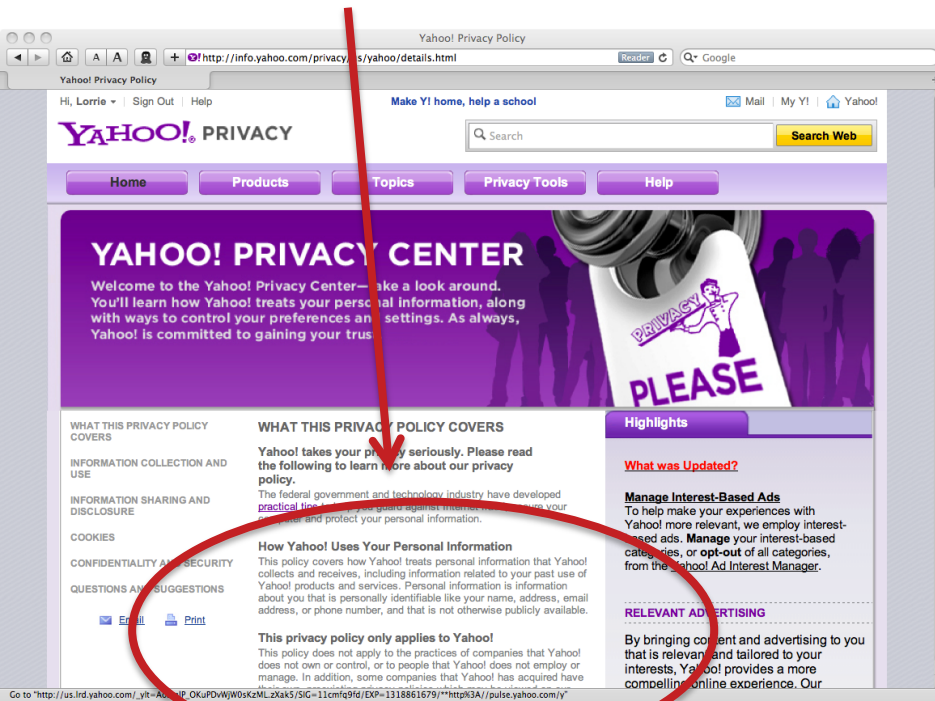


# Notice and choice

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



RECORDING OF CONTENTS MAY  
OCCUR DURING SHIPPING.



[illegible][illegible]

# **Privacy Facts**

[illegible]

“In theory there is no  
difference between theory and  
practice. In practice there is.”

—Yogi Berra

How effective is privacy  
notice and choice **in practice**?





Français

Home

Contact Us

Help

Search

canada.gc.ca

[Home](#) ► [News Room](#)

## Search

Search

Advanced search

## Sections

[About Us](#)[Legal Corner](#)[Commissioner's Findings](#)[Parliamentary Activities](#)[Resources](#)[News Room](#)[Frequently Asked Questions](#)[A-Z Index](#)

## Transparency

[Completed Access to Information Requests](#)[Proactive Disclosure](#)

## HOW TO FILE

[A privacy complaint](#)

## SECURING PERSONAL INFORMATION

## News

## Global Privacy Enforcement Network Internet Privacy Sweep Questions and Answers

May 6, 2013

### *What will happen during the Internet Privacy Sweep? What is the goal?*

Privacy enforcement authorities participating in the Sweep will designate individuals within their organizations to search the Internet in a coordinated effort to assess privacy practices related to a predetermined theme – this year the theme is Privacy Practice Transparency.

The Sweep will provide flexibility for privacy enforcement authorities to tailor their search within this common theme to focus on issues that are relevant in the context of domestic legislation, market factors and strategic priorities.

The purpose of the Sweep is *not* to conduct an in-depth analysis of the privacy practice transparency of each website, but to replicate the consumer experience by spending a few minutes per site checking for performance against set common indicators.

The Sweep is not an investigation, nor is it intended to conclusively identify

## News

Year  

## Speeches

Year  

## UPCOMING EVENTS

GO

## Media Relations

## Contact:

[Anne-Marie Hayden](#)

Non-journalists are invited to contact our Information Centre. Please call 1-800-282-1376 (toll free) or (613) 947-1698 and ask to speak with an Information Officer.

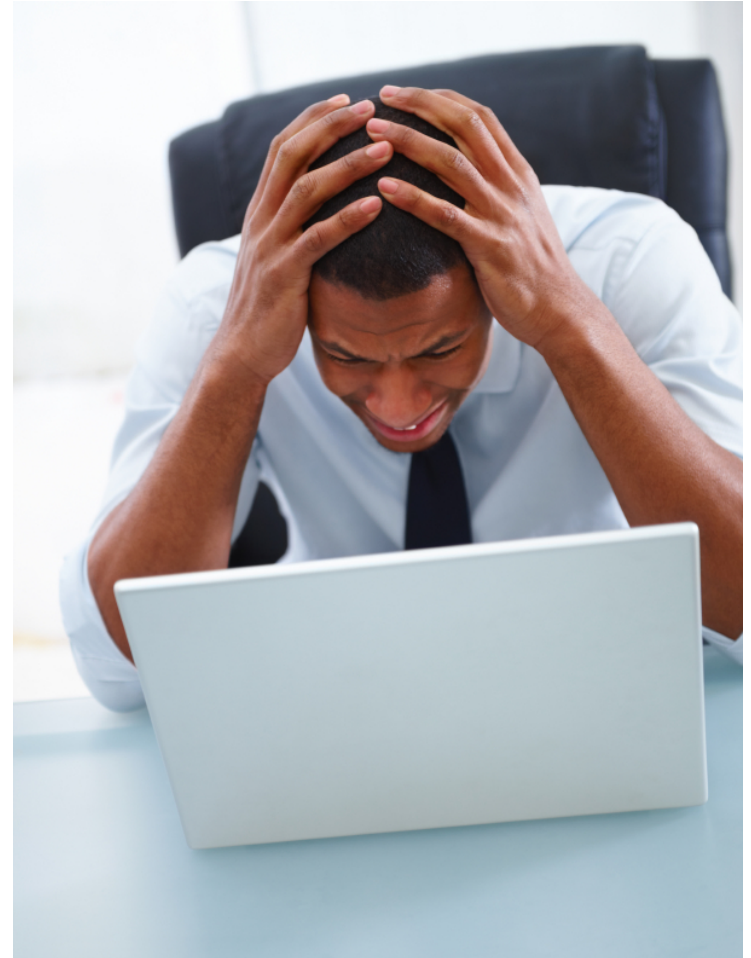
## Address:

112 Kent Street  
Ottawa, ON  
K1A 1H3  
Fax: (613) 995-1139

# 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”

- *Protecting Consumer Privacy in an Era of Rapid Change*. Preliminary FTC Staff Report. December 2010.



# Cost of reading privacy policies

- What would happen if everyone read the privacy policy for each site they visited once each month?
- Time = 244/hours year
- Cost = \$3,534/year
- National opportunity cost for time to read policies: \$781 billion



A. McDonald and L. Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review Issue. <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>





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.



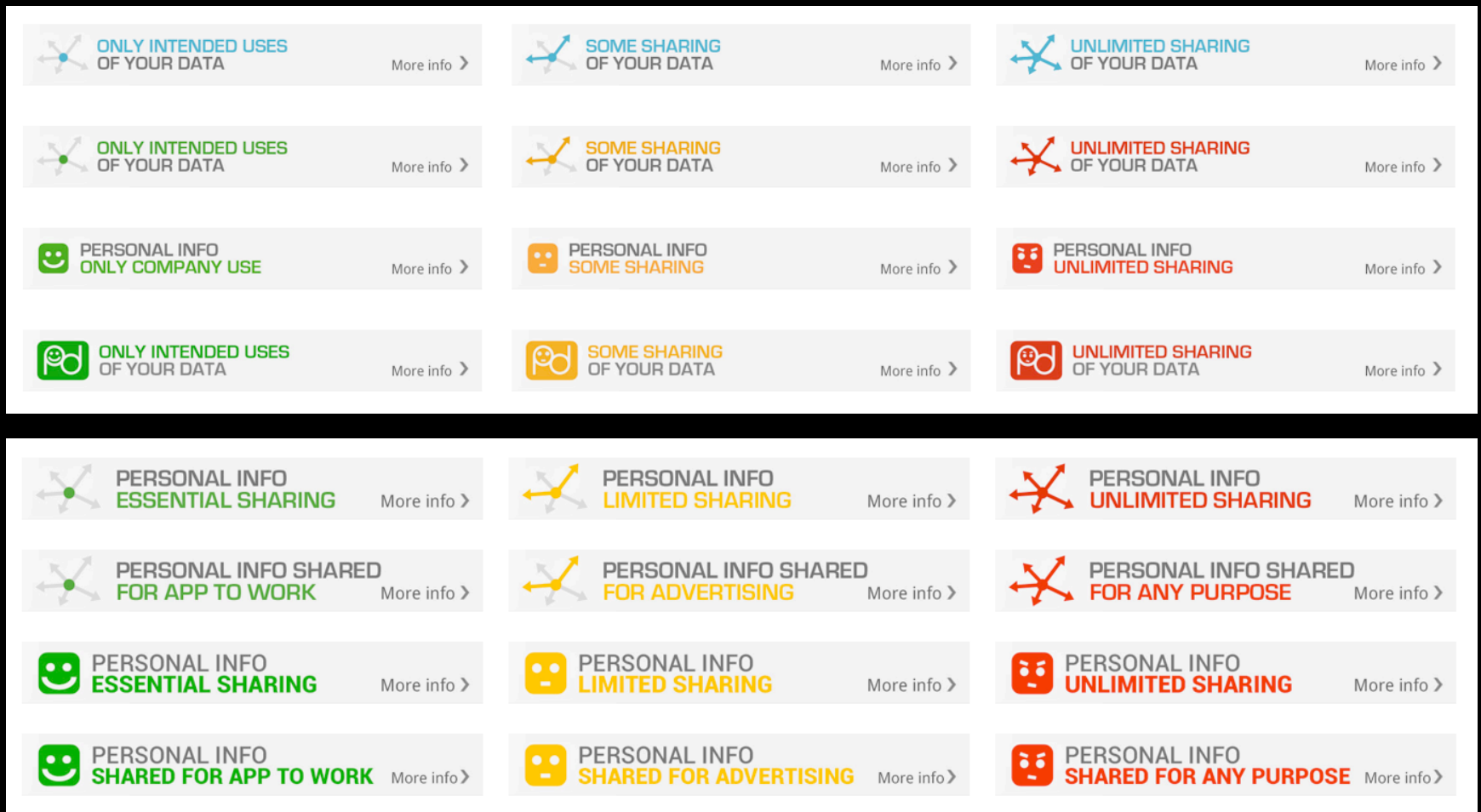
Data may be given to law enforcement even when legal process is not followed.



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

# 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

**Shredded Oats™**  
Original

## Nutrition Facts

Serving Size 1-1/4 Cup (2 oz/55g)  
Servings Per Container About 12

Amount Per Serving	Cereal	With 1/2 Cup Vit. A & D Fortified Skim Milk
<b>Calories</b>	220	260
Calories from Fat	25	25

	% Daily Value**	
<b>Total Fat</b> 2.5g*	4%	4%
Saturated Fat 0.5g	2%	2%
Trans Fat 0g		

<b>Cholesterol</b> 0mg	0%	1%
<b>Sodium</b> 250mg	10%	12%
<b>Potassium</b> 180mg	5%	11%

<b>Total Carbohydrate</b> 42g	14%	16%
Dietary Fiber 5g	20%	20%
Soluble Fiber 2g		
Insoluble Fiber 3g		
Sugars 11g		

## Protein 6g

Vitamin A	0%	6%
Vitamin C	35%	35%
Calcium	2%	15%
Iron	10%	10%
Vitamin E	8%	8%
Thiamin	10%	15%
Riboflavin	4%	10%
Niacin	6%	6%
Phosphorus	15%	30%
Magnesium	15%	20%
Zinc	10%	15%
Copper	10%	10%

\* Amount in cereal. One half cup skim milk contributes an additional 40 calories, 65mg sodium, 200mg potassium, 6g carbohydrate (6g sugars), and 4g protein.

\*\* Percent daily values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs:

	Calories	2,000	2,500
Total Fat	Less Than	65g	80g
Sat Fat	Less Than	20g	25g
Cholesterol	Less Than	300mg	300mg
Sodium	Less Than	2,400mg	2,400mg
Potassium	Less Than	3,500mg	3,500mg
Total Carbohydrate	Less Than	300g	375g
Dietary Fiber	Less Than	25g	30g

Calories per gram:  
Fat 9 • Carbohydrate 4 • Protein 4

**Ingredients:** Whole Oat Flour, Whole Wheat Flour, Unsulphured Molasses, Malted Barley Extract, Baking Soda, Salt, Natural Vitamin E (Mixed Tocopherols [Soy]), Vitamin C.

Contains wheat and soy. Made on equipment that also processes milk, almonds and hazelnuts.

Distributed by: **Barbara's Bakery, Inc.®**, a Weetabix North America Company  
20 Cameron Street, Clinton, MA 01510  
www.BarbarasBakery.com

Product of Canada

**TRADER JOE'S®**  
**Organic HIGH FIBER O's**

## Nutrition Facts

Serving Size 1 1/4 cup (55g)  
Servings per Container 8

**Amount per Serving**

**Calories** 190 Calories from Fat 10

% Daily Value\*

<b>Total Fat</b> 1g	2%
Saturated Fat 0g	0%
Trans Fat 0g	

<b>Cholesterol</b> 0mg	0%
<b>Sodium</b> 115mg	5%

<b>Total Carbohydrate</b> 44g	15%
Dietary Fiber 9g	36%

Soluble Fiber less than 1g	
Insoluble Fiber 8g	

Sugars 9g	
<b>Protein</b> 6g	12%

Vitamin A 0% • Vitamin C 130%

Calcium 4% • Iron 30%

Thiamin 25% • Riboflavin 25%

Niacin 25% • Vitamin B6 25%

Folate 25% • Vitamin B12 25%

Zinc 15%

\* Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs:

	Calories	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
Cholesterol	Less than	300mg	300mg
Sodium	Less than	2,400mg	2,400mg
Total Carbohydrate	Less than	300g	375g
Dietary Fiber	Less than	25g	30g
Protein	Less than	50g	65g

**INGREDIENTS:** Organic Whole Grain Wheat Flour, Organic Wheat Bran, Organic Evaporated Cane Juice, Organic Oat Fiber, Sea Salt, Organic Caramel Color, Natural Vitamin E. **NUTRITION BLEND:** Nicotinamide, Vitamin C, Niacin, Iron, Zinc, Vitamin B6, Riboflavin, Thiamin, Folate, Vitamin B12.

Our vendors follow Good Manufacturing Practices to segregate ingredients to avoid cross contact with allergens. Made on shared equipment with milk, tree nuts & soy. Facility processes eggs & peanuts.

Dist. & Sold Exclusively By:  
Trader Joe's, Monrovia, CA 91016

Certified Organic by  
Quality Assurance International (QAI).



# 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

P.G. Kelley, J. Bresee, L.F. Cranor, and R.W. Reeder.  
A “Nutrition Label” for Privacy. SOUPS 2009.





P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor.  
Standardizing Privacy Notices: An Online Study  
of the Nutrition Label Approach. CHI2010.

Acme						
information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						

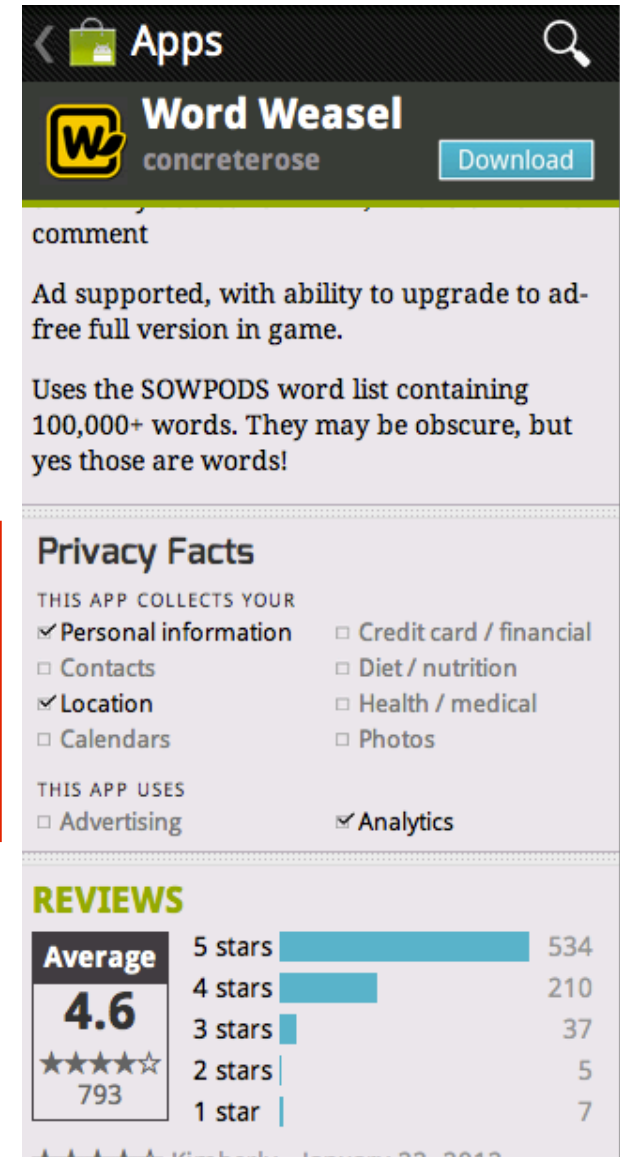
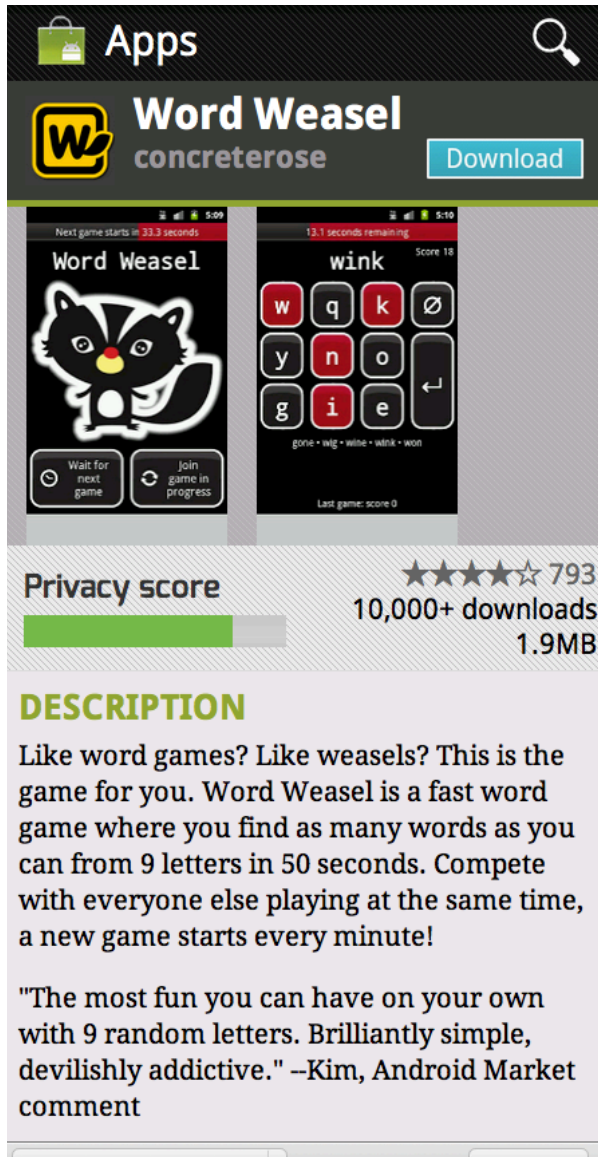
<p><b>Access to your information</b> This site gives you access to your contact data and some of its other data identified with you</p> <p><b>How to resolve privacy-related disputes with this site</b> Please email our customer service department</p>	<p>acme.com 5000 Forbes Avenue Pittsburgh, PA 15213 United States Phone: 800-555-5555 help@acme.com</p>
---	---

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



# Privacy label for Android



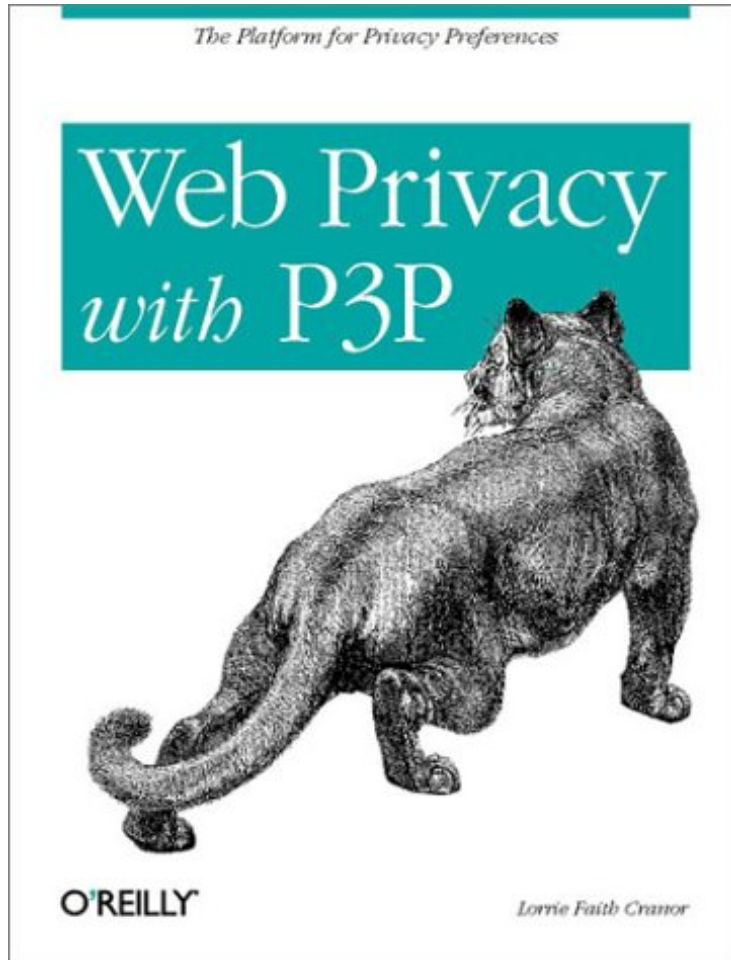


# Role play studies

- Task for participants in lab or online
  - Select apps for friend with new Android phone
  - Choose from 2 similar apps w/ different permission requests in each of 6 categories
  - Click on app name to visit download screens
- Post-task questionnaire
- Participants who saw Privacy Facts more likely to select apps that requested fewer permissions
  - Other factors such as brand and rating reduce effect

P.G. Kelley, L.F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. CHI 2013.

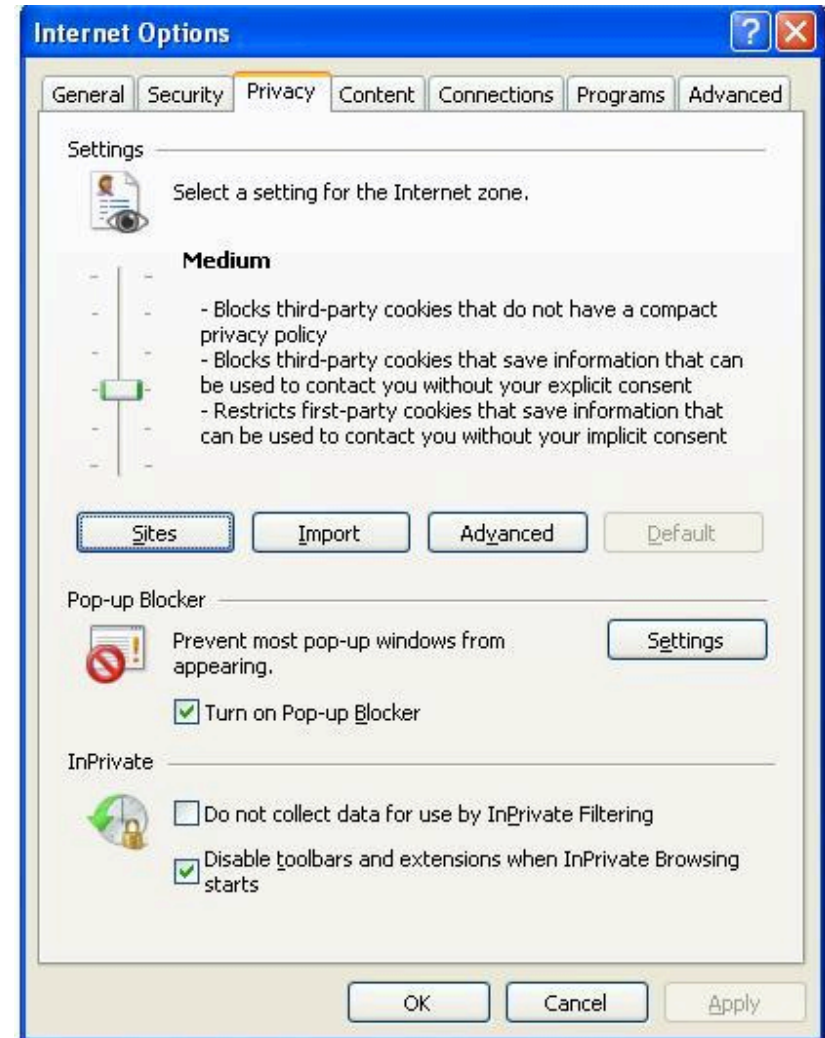
# Let your computer read for you



- 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 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>**

P. Leon, L. Cranor, A. McDonald, and R. McGuire. Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens. WPES 2010.



[MSDN Blogs](#) > [IEBlog](#) > [Google Bypassing User Privacy Settings](#)

## Google Bypassing User Privacy Settings

Published Monday, February 20, 2012 1:31 PM

 152 comments

When the IE team heard that Google had bypassed user privacy settings on Safari, we asked ourselves a simple question: is Google circumventing the privacy preferences of Internet Explorer users too? We've discovered the answer is yes: Google is employing similar methods to get around the default privacy

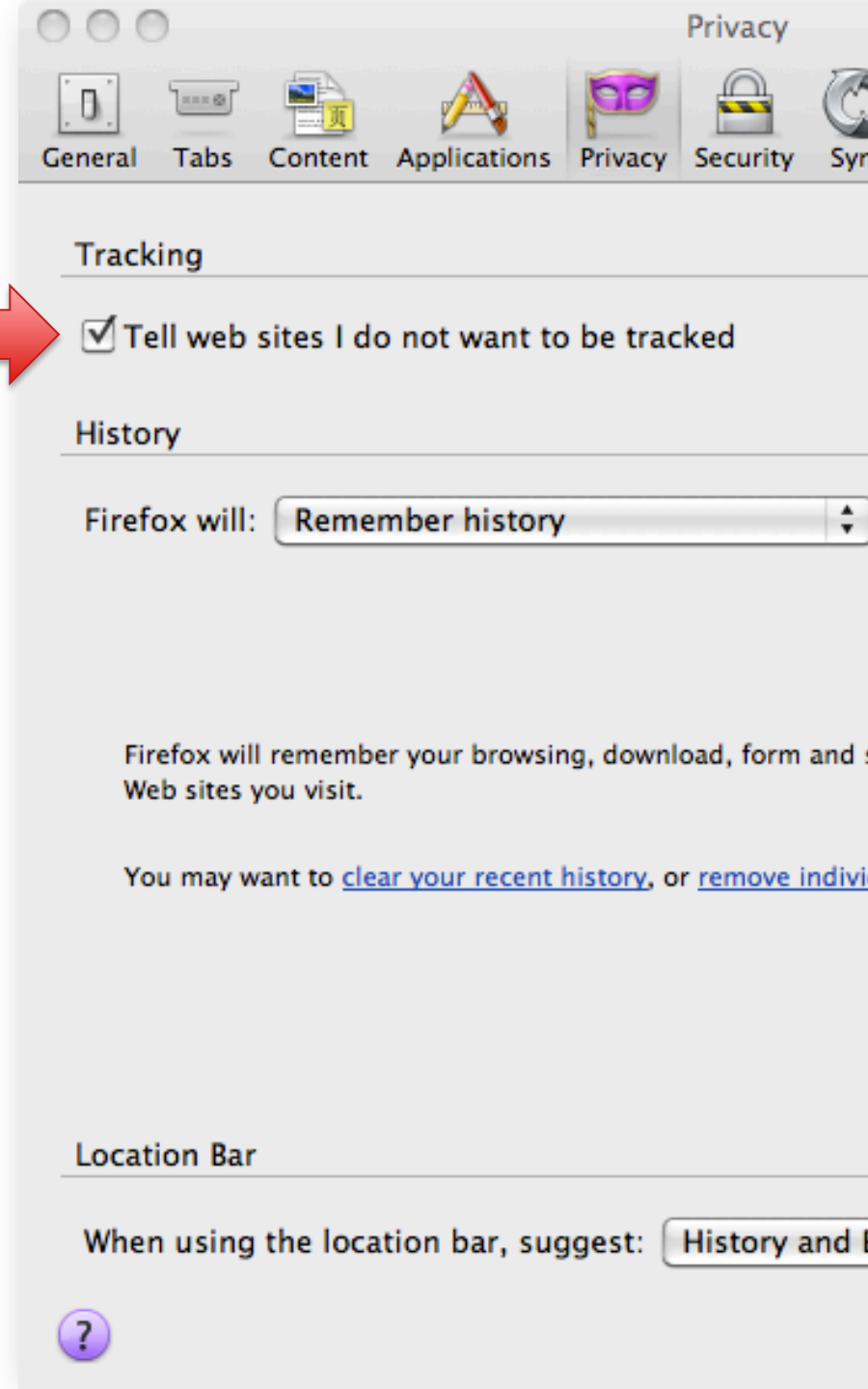
### Languages

[English](#)[Français](#)[Deutsch](#)[Português \(Brasil\)](#)[한국어](#)[日本語](#)[简体中文](#)[Русский](#)

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.

# Do not track

- Proposed W3C standard
- User checks a box
- Browser sends “do not track” header to website
- Website stops “tracking”
- W3C working group trying to define what that means



# Lots of tools to stop tracking

- Browser privacy settings
  - Cookie blocking
  - P3P
  - Tracking Protection Lists
  - Do Not Track
- Browser add-ons
- Opt-out cookies
- Digital Advertising Alliance (DAA) AdChoices icon and associated opt-out pages



# Are any of these tools effective?

- Do the tools work?
  - Does technology do what it is supposed to do?
  - Do companies respect user choices?
- Can consumers use them?
  - Do users understand tracking?
  - Do users understand what tools do?
  - Can users make tools do what they want?



# Smart, Useful, Scary, Creepy: Perceptions of Behavioral Advertising

Blase Ur, Pedro G. Leon,  
Lorrie Faith Cranor, Richard Shay,  
and Yang Wang  
*SOUPS 2012*

# Research goals

- Gain insight into what users think about online behavioral advertising (OBA)
- Identify how participants' mental models correspond with notice and choice mechanisms

# Methodology

- 48 participants
- Recruited from the Pittsburgh, PA region
  - Non-technologists
  - Interested in testing privacy tools
- Combination semi-structured interview and usability study
- Part way through interview showed WSJ video to inform participants about OBA

# Participants unaware of OBA


- Participants believed ads were tailored, but only based on context or on a single site

**amazon** Blase's Amazon.com | Today's Deals | Gift Cards | Help


Shop by Department ▾ Search All ▾ Go

Your Amazon.com | Your Browsing History | Recommended For You | Amazon Betterizer | Improve Your Recommendations | Your Profile | Learn More


## Your Amazon.com




**New Release**  
Elixir Strings Acoust...  
\$31.98 **\$12.67**  
Why recommended?



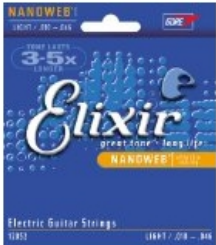
**New Release**  
Kyser 6 String Capo,...  
\$24.95 **\$15.16**  
Why recommended?




Planet Waves Pro Wind...  
★★★★☆ (153)  
\$13.99 **\$6.99**  
Why recommended?



Elixir Strings Acoust...  
★★★★☆ (39)  
\$30.00 **\$12.12**  
Why recommended?



Elixir Strings Electr...  
★★★★☆ (34)  
\$22.00 **\$8.64**  
Why recommended?



Snark SN-2 All Instru...  
★★★★☆ (546)  
\$39.00 **\$11.20**  
Why recommended?

> See all recommendations in Musical Instruments



# Participants unaware of OBA

- Participants believed ads were tailored, but only based on context or on a single site
- Thought it was only hypothetical
  - “I guess if they were monitoring what I did on the Internet...But I’d hope they weren’t...”

# Didn't recognize OBA icon

- Not sure what would happen if they clicked on icon
  - Express interest in product
  - Purchase your own ads
  - Go to product's website
  - See related ads



# Mixed opinion about OBA

- Recognized benefits
  - Advertisers can reach consumers interested in their products
  - Consumers find things they're interested in and don't get ads for things they're not interested in
- Concerned about privacy

# Beliefs about OBA

- Advertisers collect information including name, financial information, and address
- This information, along with browsing history, is stored in cookies

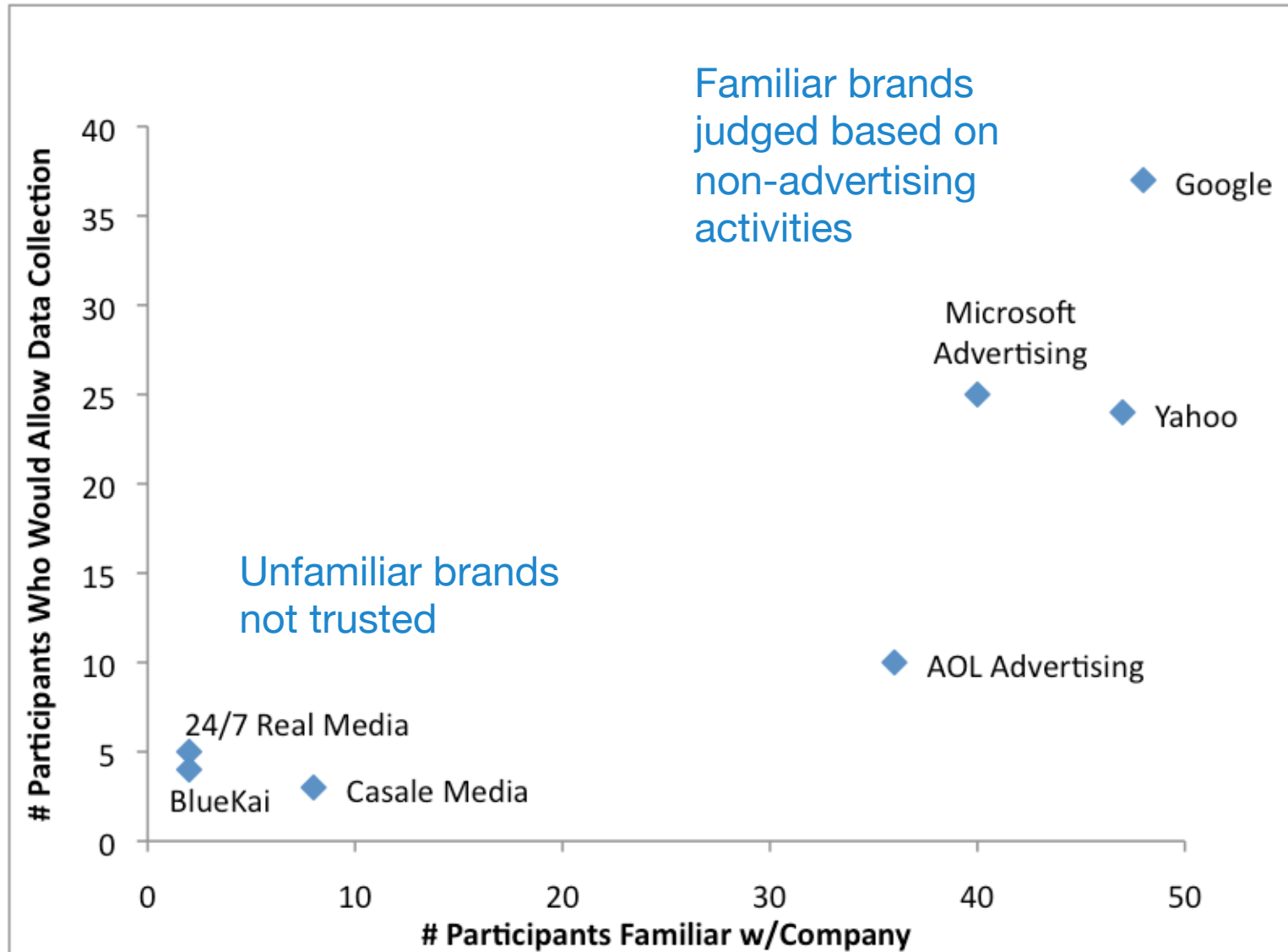


# Participants' impressions: available choice mechanisms

- Deleting cookies
- No options
- Antivirus software suites
- Web browser



# Familiarity and trust are important



# Takeaways

- Opinions about OBA mixed – both useful and creepy
- Participants did not understand OBA technologies
- Some of the worst fears based on misconceptions
- Participants did not know how to effectively exercise choice

# Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising

Pedro G. Leon, Blase Ur, Rebecca  
Balebako, Lorrie Faith Cranor,  
Richard Shay, and Yang Wang  
*CHI 2012*

# Three types of tools tested

## Blocking Tools



## Opt-out Tools



## Privacy built in browser





# Methodology

- Part of previous interview study
- 45 participants evaluated 9 tools
  - Between subjects study
  - Random assignment, controlled for preferred web browser and operating system

# Testing protocol

- Semi-structured interview
- Usability testing
  - Task 1: Learn about and install the tool
  - Task 2: Change tool settings
  - Task 3: Browsing scenarios
- Exit questionnaire


# DAA website

Firefox THE SELF-REGULATORY PROGRAM FOR... +

http://www.aboutads.info/ Google

## THE SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING

Home The Principles For Consumers For Companies List of Participants Resources News Enforcement Contact



TM

*Advertising Option Icon*

### Welcome to the online home of the Self-Regulatory Program for Online Behavioral Advertising.

Building on the [Self-Regulatory Principles for Online Behavioral Advertising](#) (Principles) released in July 2009, the nation's largest media and marketing associations have come together to launch this Program, which gives consumers a better understanding of and greater control over ads that are customized based on their online behavior (also called "interest-based" advertising).

Our participating companies share a commitment to delivering consumers a robust and credible Program of notice and choice for online behavioral advertising, and to enhancing consumer confidence in the online medium.

**For Consumers**

**Learn about Online Behavioral Advertising:** If you're an online user, you can [find out more](#) about online behavioral advertising and how it helps provide you with more relevant advertising on the websites you visit. You'll learn how online advertising supports the free content, products and services you use online; what choices you have; and how to use browser controls to enhance your privacy.

**Exercise Your Choice:** You can now [visit](#) the beta version of the Program's Consumer Opt Out Page, which allows users to

**Participating Associations**

- A-s LEADERSHIP COMMUNITY ADVOCACY GUIDANCE
- AAF
- ANA Leading the Marketing Community
- BBB Start With Trust
- DMA Direct Marketing Association
- iab.
- NAI

CONSUMER CHOICE PAGE

Make choices about interest-based ads from participating companies

http://www.aboutads.info/home

5:03 PM 9/29/2011

# Opting out can be challenging



Translate

From: Japanese - detected ▼



To: English ▼

Translate

すでにターゲティング広告が配信されている場合、すべての配信停止処理にはお時間かかる場合があります。  
この処理は、ユーザー情報を参考にしたターゲティング広告を配信停止しただけになっていますので、それ以外の広告配信については停止処理を行っていませんこと、ご了承下さい。

Ä

If you have already targeted ads are delivered, all unsubscribe process may take your time.  
This process has not only stop targeting ads that reference the user information for ad serving, otherwise it does not stop in the process, please understand.



**New!** Click the words above to view alternate translations. [Dismiss](#)

# Ghostery configuration interface

The screenshot shows the Ghostery Options configuration interface in a web browser. The browser's address bar displays "ghostery/content/options.html". The interface is divided into two main sections: "Performance Options" and "Blocking Options".

**Performance Options**

- ☒ Scan and block images served off the matched tracker domain
- ☒ Scan and block iframes served off the matched tracker domain
- ☒ Scan and block embed and object tags served off the matched tracker domain
- ☒ Look for and prevent redirection from known trackers
- ☒ Scan for dynamically inserted page elements

**Blocking Options**

- ☒ Enable web bug blocking
- ☐ Enable cookie protection [experimental]

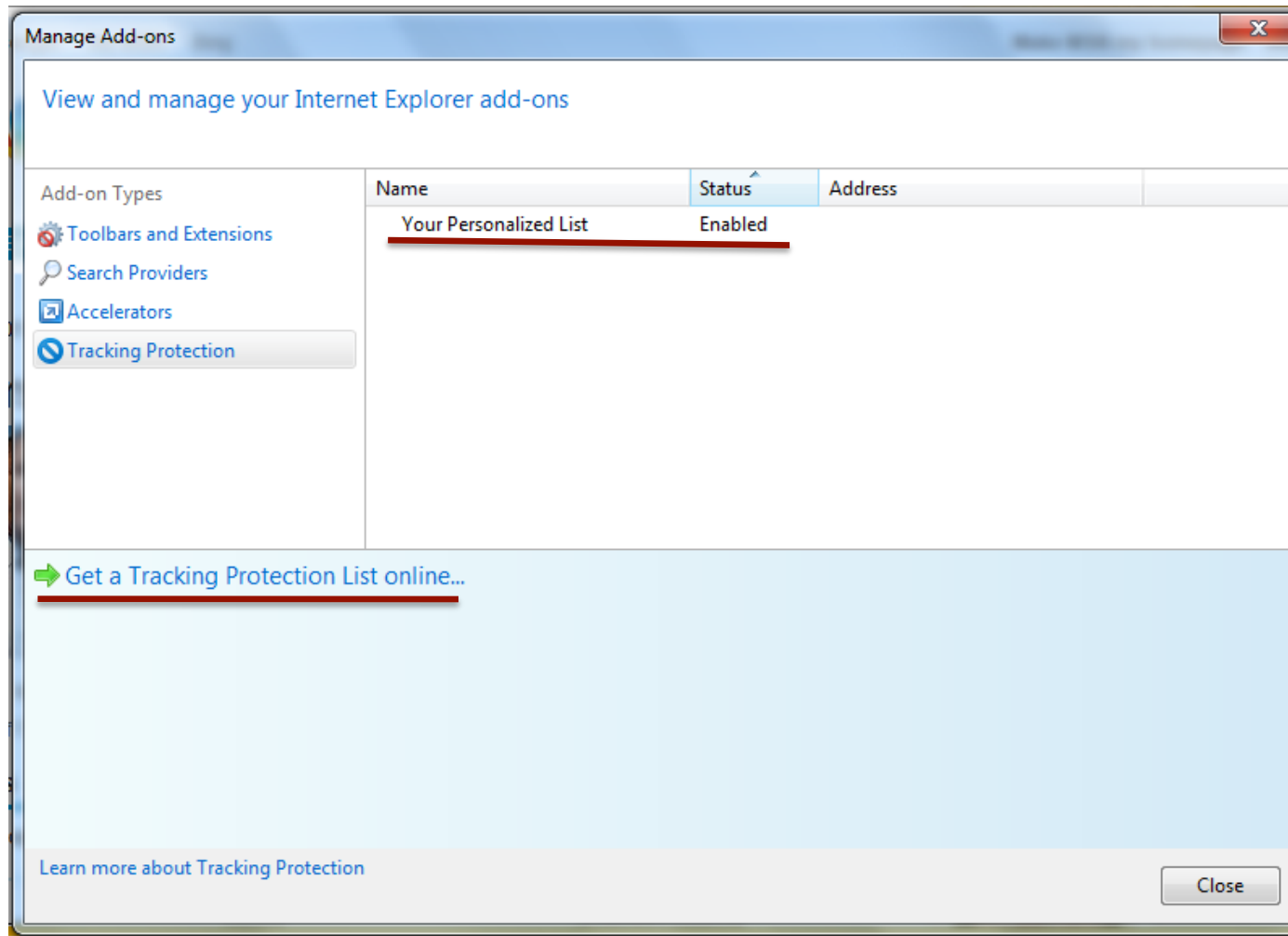
Below the Blocking Options, there is a summary and a list of blocked items:

659 bugs & 396 cookies (click for more info)

24/7 Real Media	iab. NAI	▶
2leep		
33Across	iab. NAI	▶
3DStats		
5min Media	iab.	
[x+1]	NAI	▶
Accelerator Media		



# IE-TPL configuration interface



# Takeaways

- Problematic defaults
- Poorly designed interfaces and jargon
- Feedback
- Misconceptions about opt-out tools
- Users unable to make meaningful decisions on a per-company basis

# What Do Online Behavioral Advertising Disclosures Communicate to Users?

Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. WPES 2012



AdChoices



Pop in. Stand out.

Buy Now!

TARGET P&G eStore by eStore Retail Services amazon.com

AT&T.

The nation's **largest** 4G network.



LEARN MORE

Rethink Possible®

4G speeds not available everywhere.

It's 1702, a decade after  
The Crucible's infamous seductress  
danced with the devil in Salem.

MAY 4-26, 2013

*Abigail*  
1702

BY ROBERTO AGUIRRE-SACASA  
DIRECTED BY TRACY BRIDGEN

CITY THEATRE

BUY TICKETS >

YAHOO!  
--- ON THE ---  
ROAD

Don't miss a beat

Ad Feedback

AdChoices

# 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)”*



Peter Kosmala, Former Managing Director of The Digital Advertising Alliance. *Yes, Johnny Can Benefit From Transparency and Control.* November 3, 2011.



# 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

HOME PAGE TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS

Subscribe: Home Delivery / Digital Log In Register Now

Why did I get this ad? 

# The New York Times

Tuesday, October 25, 2011 Last Update: 11:21 PM ET

CLICK HERE

Follow Us    Subscribe to Home Delivery Personalize Your Weather

Switch to Global Edition ▶

**JOBS**  
REAL ESTATE  
AUTOS  
ALL CLASSIFIEDS

**WORLD**  
U.S.  
POLITICS  
NEW YORK  
BUSINESS  
DEALBOOK  
TECHNOLOGY  
SPORTS  
SCIENCE  
HEALTH  
OPINION  
ARTS  
Books  
Movies  
Music  
Television  
Theater  
STYLE  
Dining & Wine  
Fashion & Style  
Home & Garden  
Weddings/

## Europe Faces New Hurdles in Crisis Over Debt

By STEVEN ERLANGER and RACHEL DONADIO 20 minutes ago

On the eve of a European Union summit meeting, crucial financial measures were still unresolved.

- Tempers Flare as European Meeting Nears

## I.B.M. Names Virginia Rometty as New Chief Executive

By STEVE LOHR 22 minutes ago

The selection of Ms. Rometty, a senior vice president at I.B.M., will make her one of the highest-profile women executives in corporate America.



## Baseball's Game of Telephone

By PAT BORZI 3 minutes ago

Monday night's bullpen debacle by the Cardinals has put a new spotlight on baseball's reliance on landlines.

## New Poll Finds a Deep Distrust of Government

By JEFF ZELENY and MEGAN THEE-BRENAN 3 minutes ago

With Election Day just over a year away, a deep

## OPINION »

OP-ED | CLIFFORD WINSTON

### Are Law Schools and Bar Exams Necessary?

The barriers to entry for the legal industry exist to protect lawyers from competition with non-lawyers.

- Brooks: The Fighter Fallacy | Comments
- Nocera: Jobs's Biographer
- Cohen: Defending the E.U.
- Bruni: Have Glock
- Editorial: Refinancing
- Room for Debate: Will Amazon Kill Off Publishers?

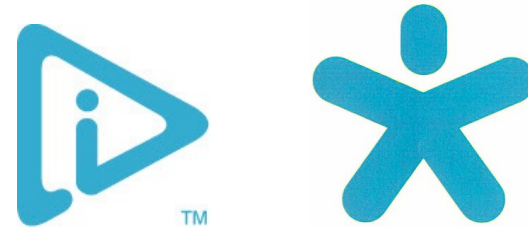
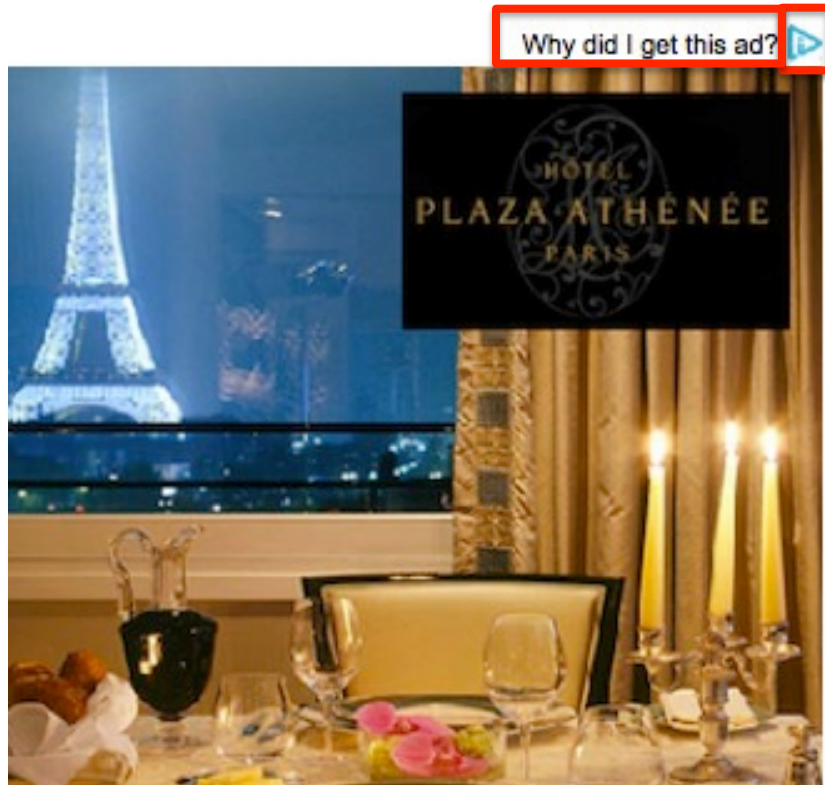
THE WORLD SERIES 



Dilip Vishwanat for The New York Times



# 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'

# Exposure to landing pages



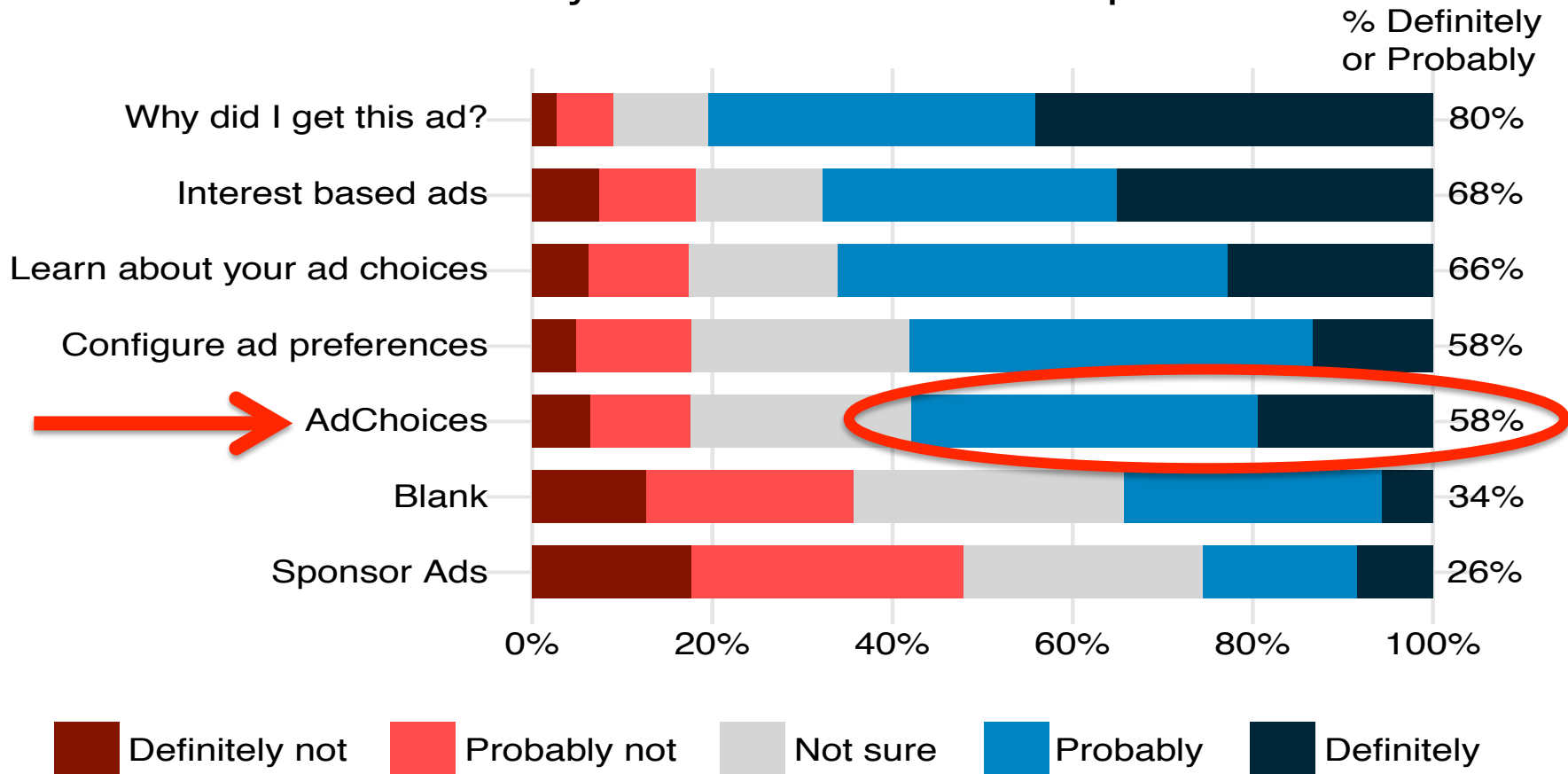
- AOL
- Yahoo!
- Microsoft
- Google
- Monster

# 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]



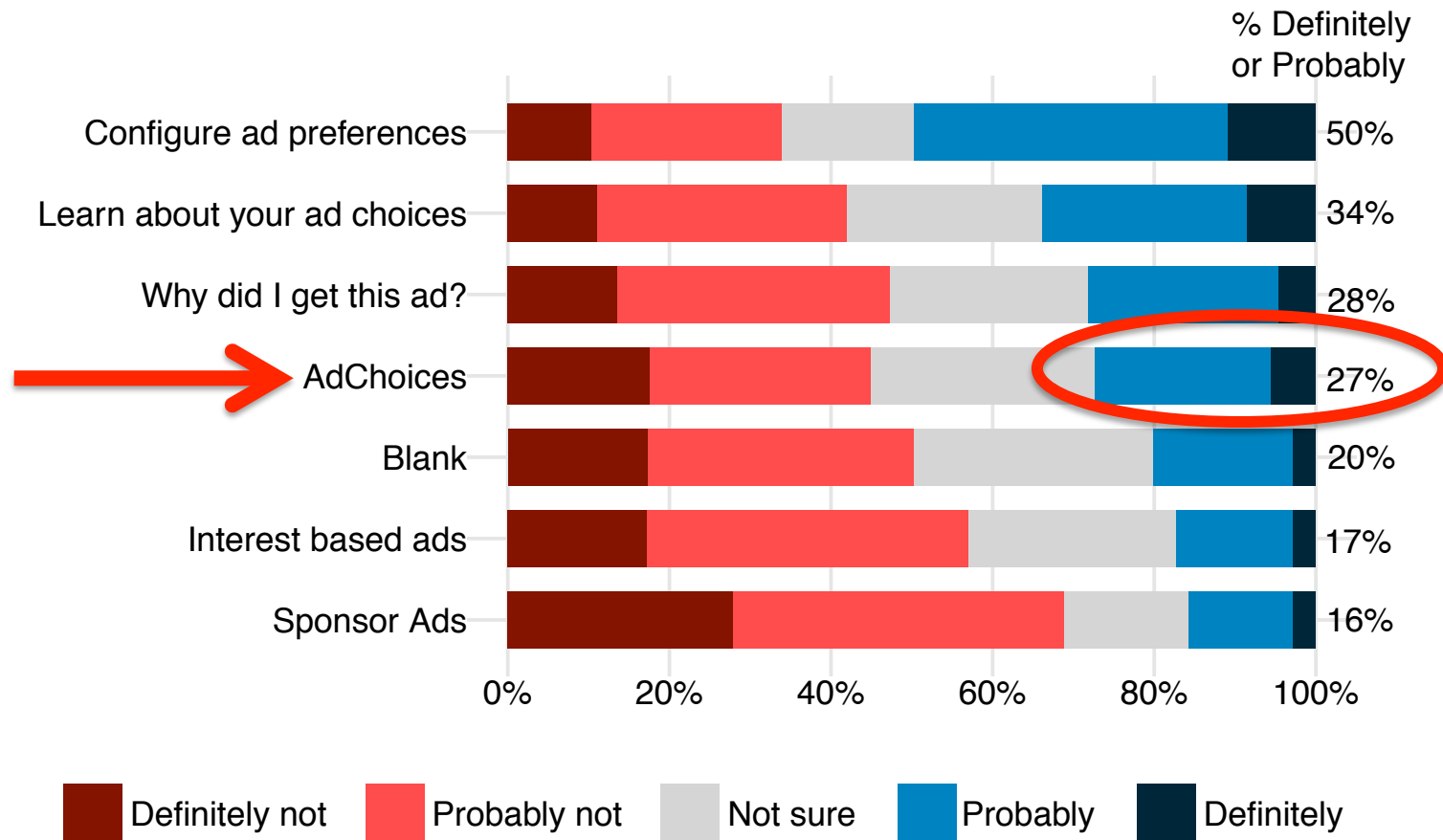
This ad has been tailored based on websites you have visited in the past



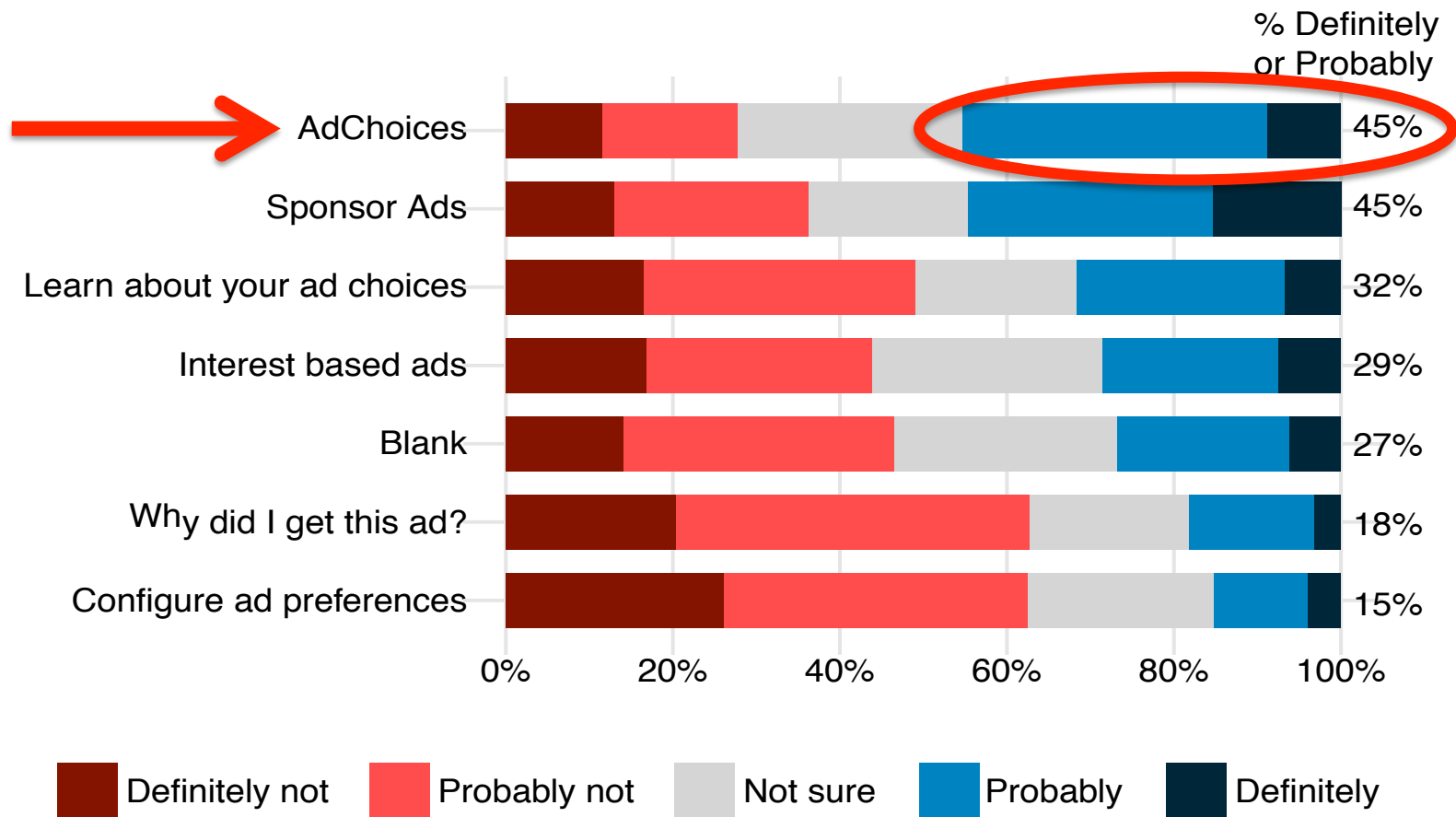
# Willingness to click

- What do you think would happen if you click on that symbol or that phrase?
  - It will take you to a page where you can tell the advertising company that you do not want to receive tailored ads. [true]
  - More ads will pop up. [false]
  - It will take you to a page where you can buy advertisements on this website. [false]

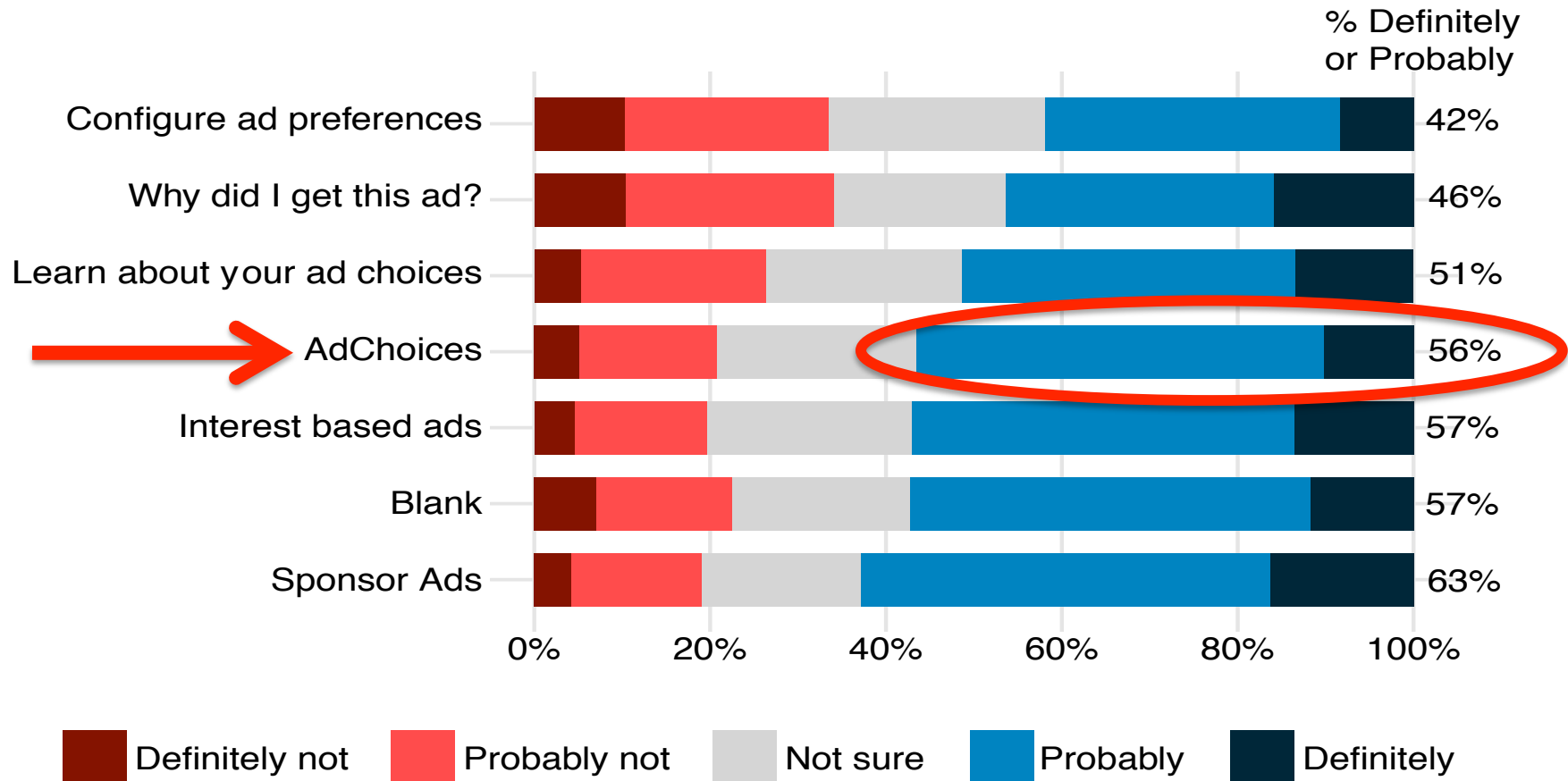
Will take you to a page where you can tell the advertising company that you do not want to receive tailored ads



Will take you to a page where you can  
buy advertisements on this website



## More ads will pop up



# 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

How effective is privacy  
notice and choice in practice?



**Notice and Choice  
Mechanism**

**Effectiveness in  
Practice**

<b>Notice and Choice Mechanism</b>	<b>Effectiveness in Practice</b>
<b>Privacy policies</b>	Nobody reads
<b>Privacy nutrition labels</b>	Promising research, not used
<b>Privacy Facts for Android</b>	Promising research, not used
<b>P3P</b>	Used to circumvent browser privacy settings
<b>Do Not Track</b>	No agreement on what it means
<b>Tools to opt-out of tracking</b>	Difficult to use
<b>AdChoices icon</b>	Nobody knows what it means and people are afraid to click on it

# Are They Actually Any Different? Comparing Thousands of Financial Institutions' Privacy Practices

Lorrie Faith Cranor, Kelly Idouchi,  
Pedro Giovanni Leon, Manya  
Sleeper, Blase Ur, WEIS 2013

FACTS	WHAT DOES PNC 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: <ul style="list-style-type: none"> <li>• Social Security number and income</li> <li>• Account balances and account transactions</li> <li>• Credit scores and payment history</li> </ul>
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 PNC chooses to share, and whether you can limit this sharing.

Reasons we can share your personal information	Does PNC share?	Can you limit this sharing?
<b>For our everyday business purposes</b> — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
<b>For our marketing purposes</b> — to offer our products and services to you	Yes	No
<b>For joint marketing with other financial companies</b>	Yes	Yes
<b>For our affiliates' everyday business purposes</b> — information about your transactions and experiences	Yes	No
<b>For our affiliates' everyday business purposes</b> — information about your creditworthiness	Yes	Yes
<b>For our affiliates to market to you</b>	Yes	Yes
<b>For nonaffiliates to market to you</b>	No	We don't share

<b>To limit our sharing</b>	<ul style="list-style-type: none"> <li>• Call 1-800-762-2118 — our menu will prompt you through your choice(s)</li> <li>• Visit us online: <a href="http://www.PNC.com/privacy">www.PNC.com/privacy</a> (Online Banking customers only.)</li> </ul> <p><b>Please note:</b> If you are a <i>new</i> customer, we can begin sharing your information 30 days from the date we sent this notice. When you are <i>no longer</i> our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.</p>
<b>Questions?</b>	Call 1-800-762-2118

FACTS	WHAT DOES CIT Group Inc. ("CIT") 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?	<p>The types of personal information we collect and share depends on the product or service you have with us. This information can include:</p> <ul style="list-style-type: none"> <li>• Social Security Number and income</li> <li>• account balances and transaction history</li> <li>• credit history and credit scores</li> </ul> <p>When you are no longer our customer, we continue to share your information as described in this notice.</p>
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 CIT chooses to share; and whether you can limit this sharing.

#### Reasons we can share your personal information

	Does CIT share?	Can you limit this sharing?
<b>For our everyday business purposes</b> — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
<b>For our marketing purposes</b> — to offer our products and services to you	Yes	No
<b>For joint marketing with other financial companies</b>	No	We don't share
<b>For our affiliates' everyday business purposes</b> — information about your transaction	Yes	No
<b>For our affiliates' everyday business purposes</b> — information about your creditworthiness	No	No
<b>For nonaffiliates to market to you</b>	No	No

Questions? Call: 1-800-681-  
policy/index.h

FACTS	WHAT DOES BANK OF AMERICA DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Under federal law, that means personally identifiable 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?	<p>The types of personal information we collect and share depend on the product or service you have with us.</p> <p>This information can include:</p> <ul style="list-style-type: none"> <li>• Social Security number and employment information</li> <li>• account balances, transaction history and credit information</li> <li>• assets and investment experience</li> </ul>
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 Bank of America chooses to share; and whether you can limit this sharing.

#### Reasons we can share your personal information

	Does Bank of America share?	Can you limit this sharing?
<b>For our everyday business purposes</b> — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
<b>For our marketing purposes</b> — with service providers we use to offer our products and services to you (Please see below to limit the ways we contact you)	Yes	No
<b>For joint marketing with other financial companies</b>	Yes	No
<b>For our affiliates' everyday business purposes</b> — information about your transactions and experiences	Yes	No
<b>For our affiliates' everyday business purposes</b> — information about your creditworthiness	Yes	No
<b>For nonaffiliates to market to you</b> — for all credit card accounts	Yes	Yes
<b>For nonaffiliates to market to you</b> — for accounts and services endorsed by another organization (e.g., debit card co-branded with a baseball team) "Sponsored Accounts"	Yes	Yes
<b>For nonaffiliates to market to you</b> — for accounts other than credit card accounts and Sponsored Accounts, such as insurance, investments, deposit and lending	No	We don't share

69

# Gramm-Leach Bliley Act (1999)

- Mandated annual privacy disclosures
- Disclosures were full of fine print, difficult to read and compare



# Standardized notice

- Eight federal agencies jointly released a model privacy form (2009)
  - Two pages
  - Optional, but widely adopted
  - Safe harbor

# Model Privacy Form

Rev. (insert date)

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: <ul style="list-style-type: none"><li>■ Social Security number and [income]</li><li>■ [account balances] and [payment history]</li><li>■ [credit history] and [credit scores]</li></ul>		
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.		
Reasons we can share your personal information		Does [name of financial institution] share?	Can you limit this sharing?
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			
To limit our sharing	<ul style="list-style-type: none"><li>■ Call [phone number]—our menu will prompt you through your choice(s)</li><li>■ Visit us online: [website] or</li><li>■ Mail the form below</li></ul> <p>Please note:</p> <p>If you are a new customer, we can begin sharing your information [30] days from the date we sent this notice. When you are no longer our customer, we continue to share your information as described in this notice.</p> <p>However, you can contact us at any time to limit our sharing.</p>		
Questions?	Call [phone number] or go to [website]		


2

Mail-in Form			
<b>Leave Blank</b> OR (If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.) <input type="checkbox"/> Apply my choices only to me)	Mark any/all you want to limit:		
	<input type="checkbox"/> Do not share information about my creditworthiness with your affiliates for their everyday business purposes.		
	<input type="checkbox"/> Do not allow your affiliates to use my personal information to market to me.		
	<input type="checkbox"/> Do not share my personal information with nonaffiliates to market their products and services to me.		
	Name	Mail to:	
Address	[Name of Financial Institution]		
City, State, Zip	[Address 1]		
[Account #]	[Address 2]		
	[City], [ST] [ZIP]		

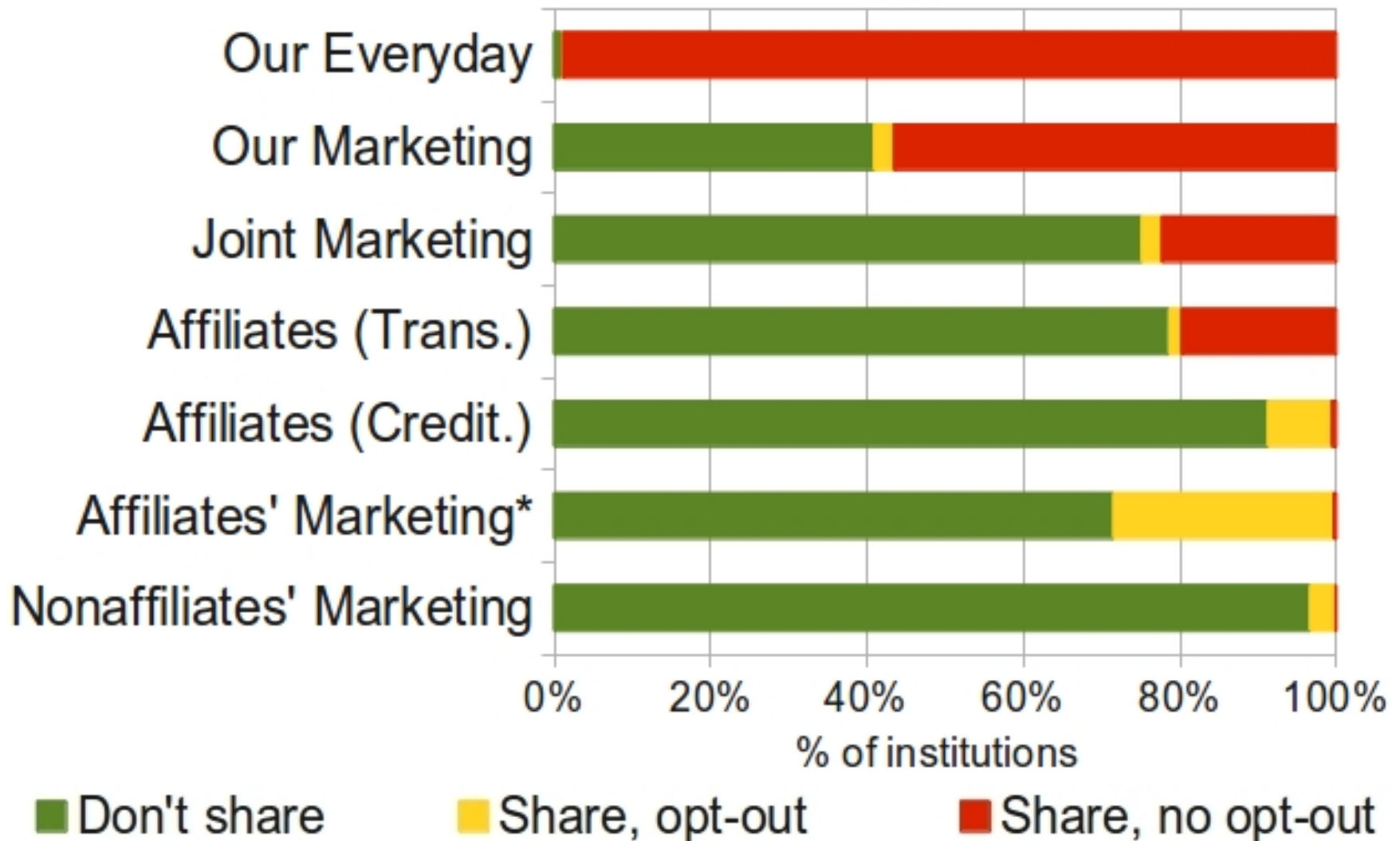
Page 2	
Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of financial institution] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer 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 <ul style="list-style-type: none"><li>■ [open an account] or [deposit money]</li><li>■ [pay your bills] or [apply for a loan]</li><li>■ [use your credit or debit card]</li></ul> <p>[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.]</p>
Why can't I limit all sharing?	Federal law gives you the right to limit only <ul style="list-style-type: none"><li>■ sharing for affiliates' everyday business purposes—information about your creditworthiness</li><li>■ affiliates from using your information to market to you</li><li>■ sharing for nonaffiliates to market to you</li></ul> <p>State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]</p>
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account—unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. <ul style="list-style-type: none"><li>■ [affiliate information]</li></ul>
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. <ul style="list-style-type: none"><li>■ [nonaffiliate information]</li></ul>
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. <ul style="list-style-type: none"><li>■ [joint marketing information]</li></ul>
Other important information	
[insert other important information]	



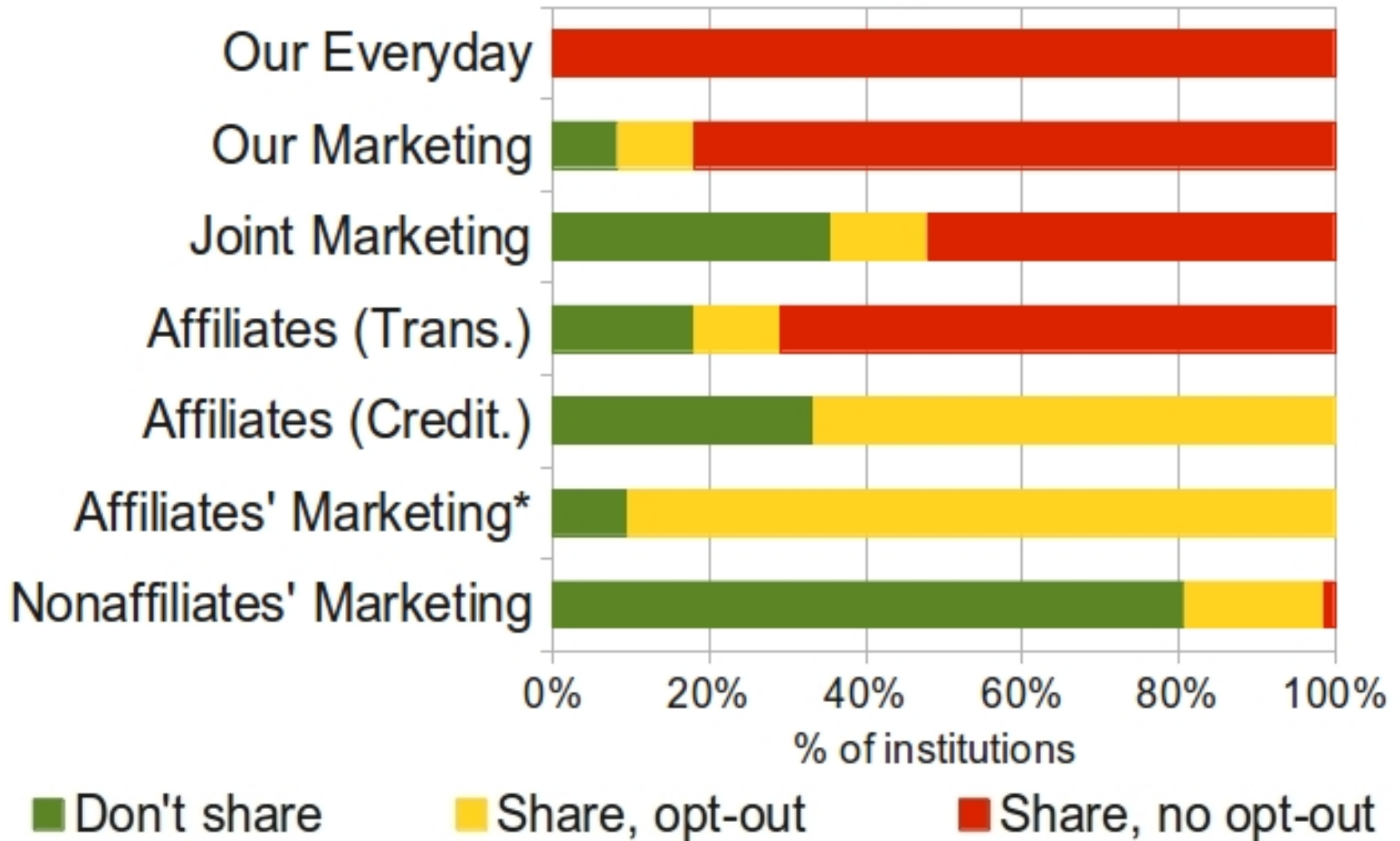
# Data collection and extraction

- FDIC directory of 7,072 institutions
- Download top 10 results for Google query:  

- Restrict to institution's web domain
- Convert HTML or PDF to text
- Regular expressions (pattern matching)
  - Structure of document
- Manual verification: 90%+ accurate per section on a random sample of 50 policies

# Reasons for sharing



# 100 largest banks



# Comparing Credit Cards

Institution	Our everyday	Our marketing	Joint marketing	Affiliates-Trans.	Affiliates-Credit.	Affiliates' Marketing	Non-affiliates' marketing
<b>Capital One, Chase, Discover, HSBC</b>	■	■	■	■	■	■	■
<b>Bank of America, Citi</b>	■	■	■	■	■	□	■
<b>Am. Ex.</b>	■	■	■	■	■	■	■
<b>Barclays</b>	■	■	■	■	■	□	■
<b>GE Capital</b>	■	■	■	■	■	□	■
<b>U.S. Bank</b>	■	■	■	■	■	□	■
<b>Wells Fargo</b>	■	■	■	■	■	■	■

■ Don't share

■ Share, opt-out

■ Share, no opt-out

# Logistic Regressions

- Dependent variable: {Share, Do not share}
- Independent variables: assets, state, specialization, regulator, etc.
- Significant factors included:
  - OCC district (geographic location)
  - Number of offices
  - Member or not of a bank holding company

# Banks are not all the same

- Banks have different privacy policies
- Many banks do little sharing of customer data
- No easy way for consumers to find banks with good privacy policies

[Win prizes and help our research](#)
[Login here](#) if you already signed up


shoes

Search

Search Engine:

- ☐ Google  
☒ Yahoo!  
☐ Shopping

Preference Level:

Medium



### [Dress, Casual & Athletic Shoes | Zappos.com](#)

[Privacy Report](#)

Online shoe store selling a variety of brand name men's and women's footwear.

<http://www.zappos.com/> - No Cache - [Privacy Policy](#) - [Similar Pages](#)


### [Nike.com - Shop the Official NikeStore](#)

[Privacy Report](#)

Designs, develops, and markets footwear, apparel, equipment, and accessory products. Explore Nike's site to shop online, customize products, and find a local store.

<http://www.nike.com/> - No Cache - [Privacy Policy](#) - [Similar Pages](#)


### [Onlineshoes.com - official site](#)

[Privacy Report](#)

Shop online for name brand shoes at Onlineshoes.com. Choose from over 170 brands. Enjoy free shipping and exchanges, plus 110% price guarantee on all shoes.

<http://www.onlineshoes.com/> - No Cache - [Privacy Policy](#) - [Similar Pages](#)


### [Shoes from Shoebuy.com - Free Shipping & Return Shipping](#)

[Privacy Report](#)

Sells mens' and womens' shoes, sandals, boots, and sneakers.

<http://www.shoebuy.com/> - [Cached](#) - [Privacy Policy](#) - [Similar Pages](#)


### [Footwear Shopping in the Yahoo! Directory](#)

[Privacy Report](#)

Browse through footwear shops and official company sites in the Yahoo! Directory. Find retailers selling shoes, boots, and accessories from Nike, adidas, Puma, Timberland, Converse, Reebok, Skechers, and others.

[http://dir.yahoo.com/Business\\_and\\_Economy/Shopping...](http://dir.yahoo.com/Business_and_Economy/Shopping...) - [Cached](#) - [Privacy Policy](#) - [Similar Pages](#)
[Shoes.com - Womens. Mens. and Childrens Shoes](#)



# What Info is Collected, and How

- What: 24 options, SSN + choose exactly 5

## 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]

- How: 34 options, choose exactly 5

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]

- The most commonly used terms were the examples listed in the model

# Curiosities Encountered

- Self-contradictory statements (15)

Does Geneva State  
Bank share?

Yes

Yes

Yes

# Curiosities Encountered

- Self-contradictory statements (15)

Does Geneva State Bank share?	Can you limit this sharing?
Yes	We don't share
Yes	We don't share
Yes	We don't share

# Curiosities Encountered

- Self-contradictory statements (15)

Does Geneva State Bank share?	Can you limit this sharing?
Yes	We don't share
Yes	We don't share
Yes	We don't share

- 24 institutions appear to be violating the Fair Credit Reporting Act (FCRA)
  - Not providing required opt-outs

# Takeaways

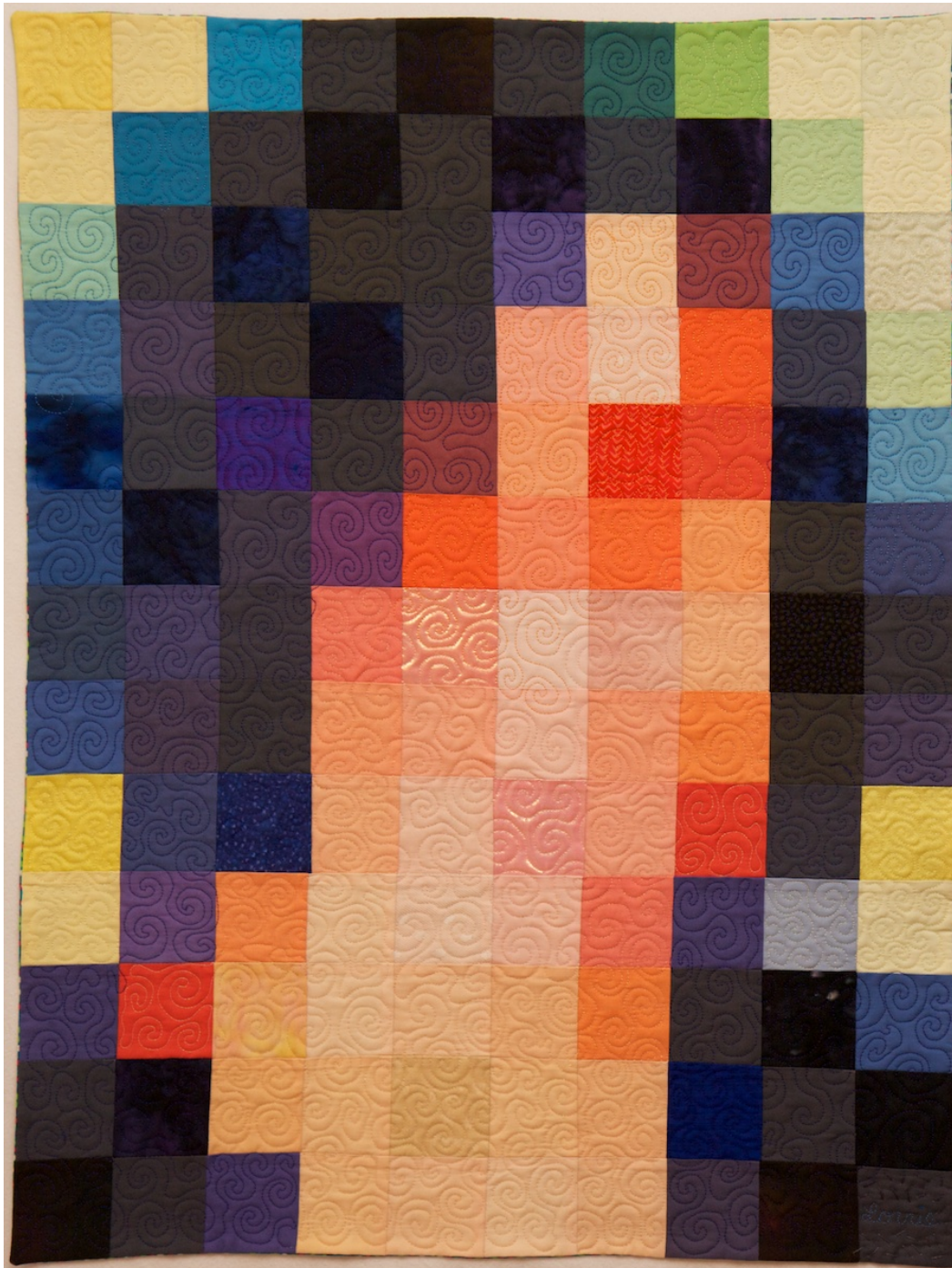
- Adoption happens when there are incentives
- Institutions **are** actually different!
  - Largest institutions have the worst practices
  - Opportunity for consumer privacy choice
- But we need to help consumers find the banks with good privacy
- Model form needs some improvement

How effective is privacy  
notice and choice in practice?

# How to make notice and choice more effective

- Incentives for adoption
- Enforcement (legal and technical)
- Baseline requirements
- Standardized notice formats
- Machine-readable notice formats
- Reduce ambiguity
- Link to full disclosure
- Comparison tools
- More research





**Carnegie  
Mellon  
University**

CyLab



Engineering &  
Public Policy

