Expecting the Unexpected

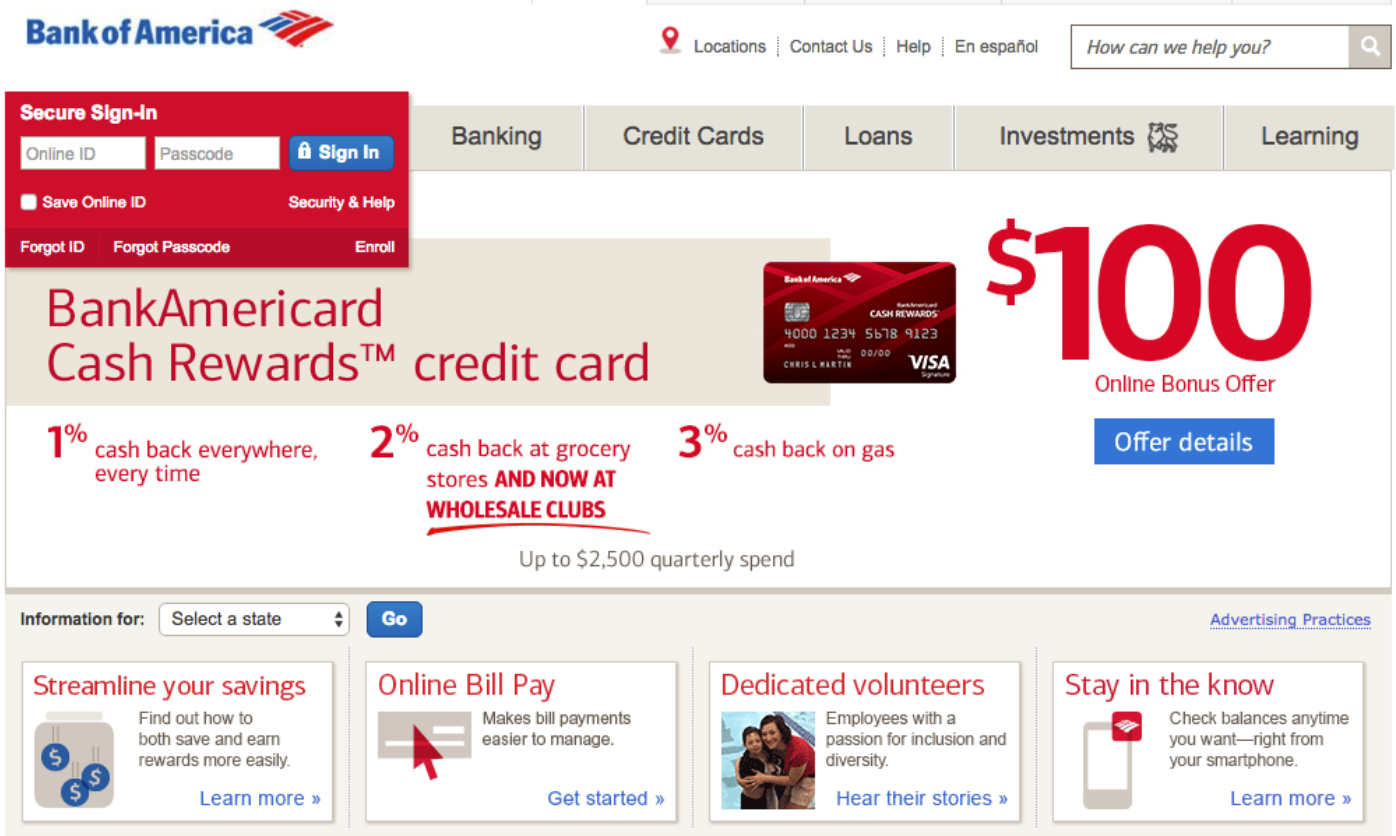
Understanding Mismatched Privacy Expectations Online

Ashwini Rao, Florian Schaub, Norman Sadeh,
Alessandro Acquisti, Ruogu Kang

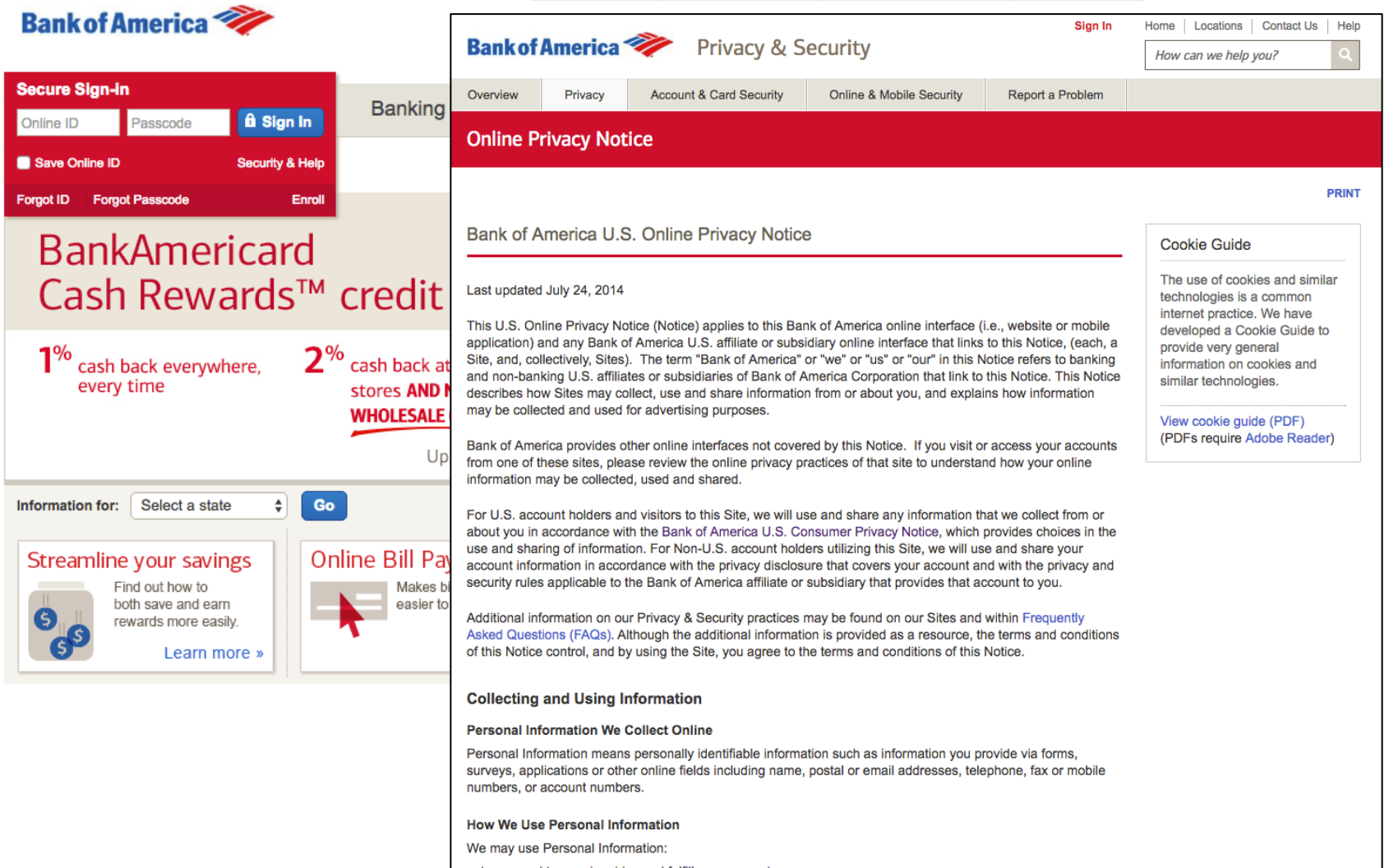
Carnegie Mellon University

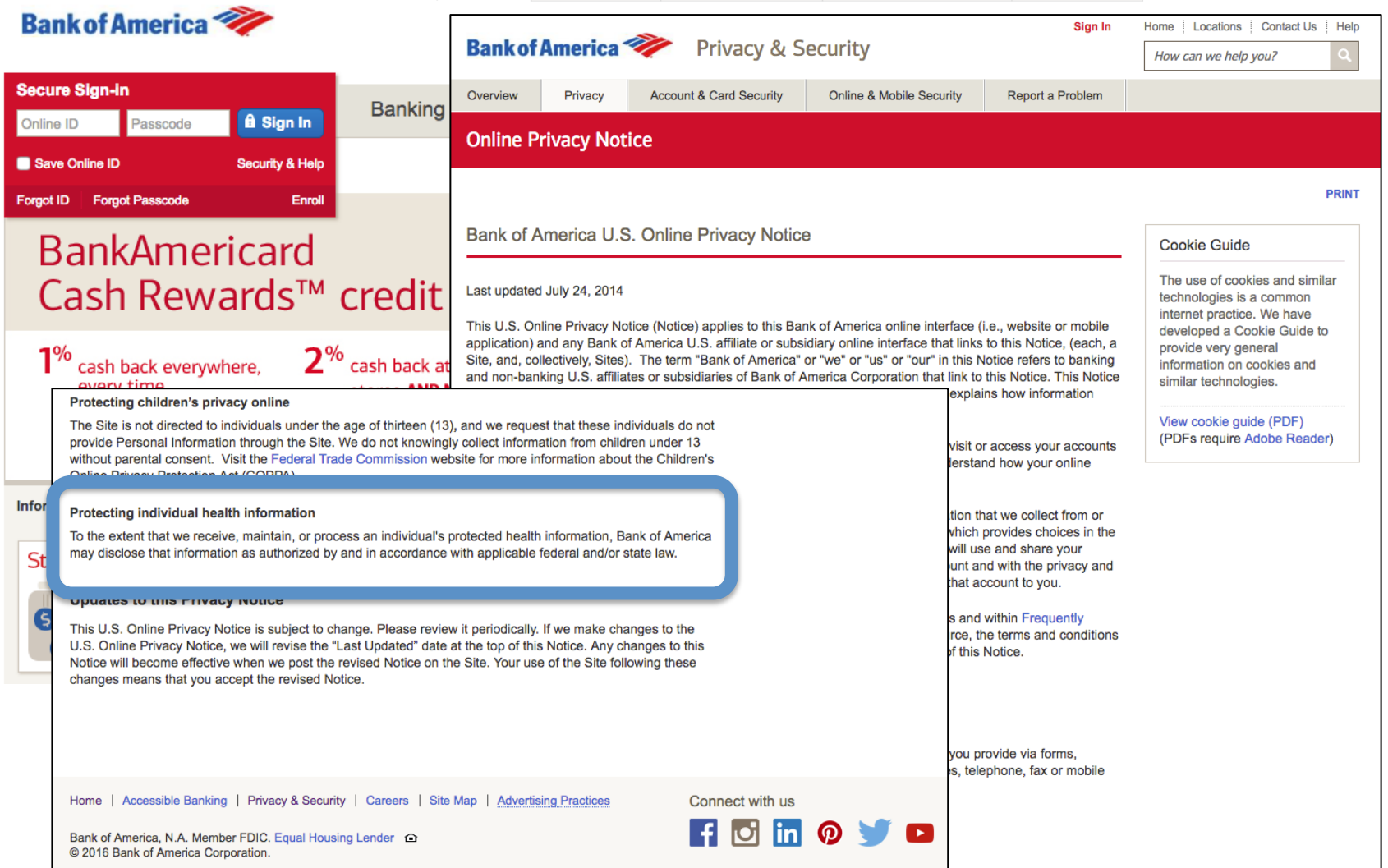
SOUPS 2016 | June 22, 2016

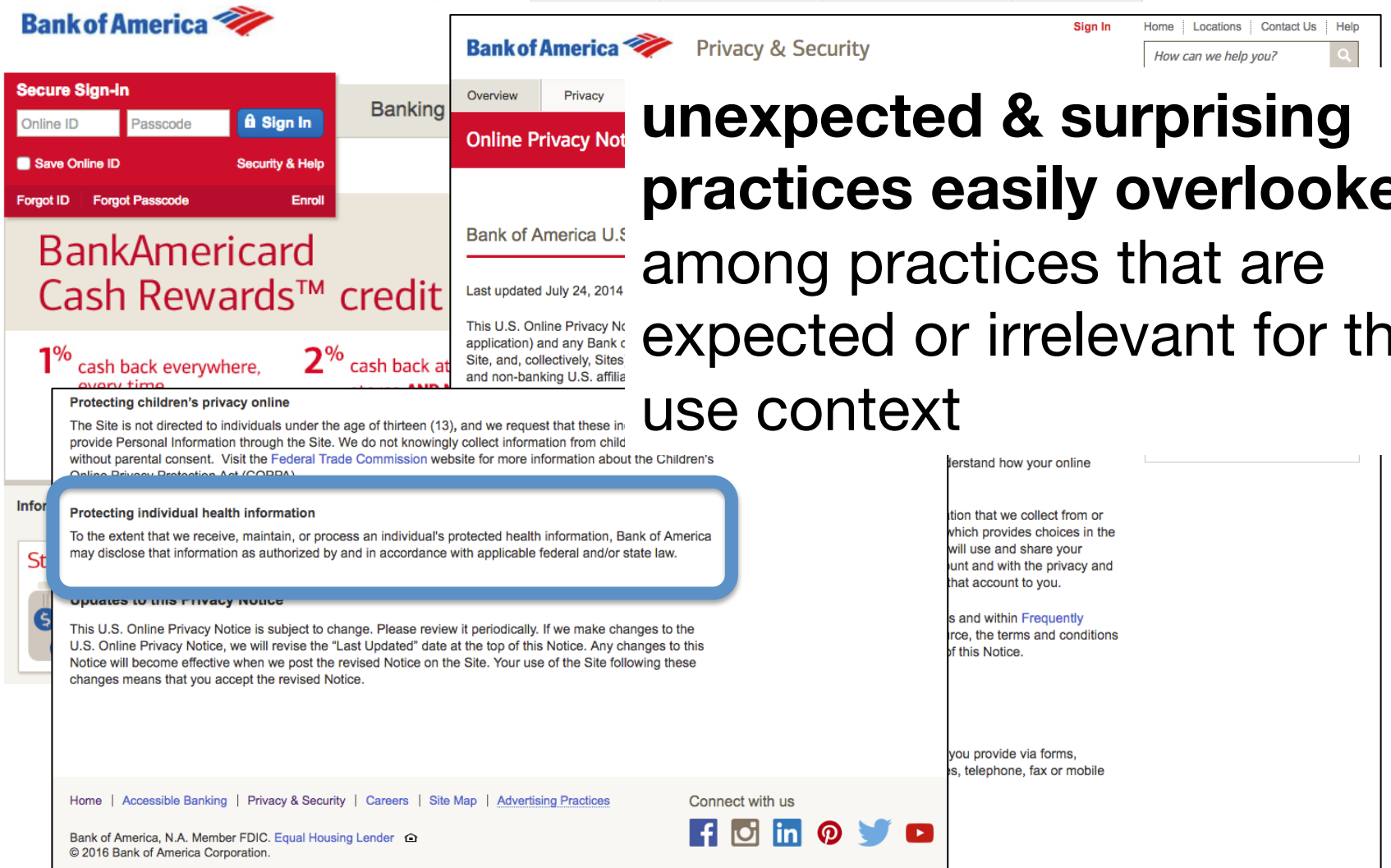
Carnegie Mellon University



What information does this website collect?


Bank of America
Secure Sign-In
Online ID
Passcode
Sign In
Save Online ID
Security & Help
Forgot ID
Forgot Passcode
Enroll
Banking
BankAmericard Cash Rewards™ credit
1% cash back everywhere, every time
2% cash back at
stores AND
WHOLESALE
Information for:
Select a state
Go
Streamline your savings
Find out how to both save and earn rewards more easily.
Learn more »
Online Bill Pay
Bank of America
Privacy & Security
Sign In
Home
Locations
Contact Us
Help
How can we help you?
Overview
Privacy
Account & Card Security
Online & Mobile Security
Report a Problem
Online Privacy Notice
PRINT
Bank of America U.S. Online Privacy Notice
Last updated July 24, 2014
This U.S. Online Privacy Notice (Notice) applies to this Bank of America online interface (i.e., website or mobile application) and any Bank of America U.S. affiliate or subsidiary online interface that links to this Notice, (each, a Site, and, collectively, Sites). The term "Bank of America" or "we" or "us" or "our" in this Notice refers to banking and non-banking U.S. affiliates or subsidiaries of Bank of America Corporation that link to this Notice. This Notice describes how Sites may collect, use and share information from or about you, and explains how information may be collected and used for advertising purposes.
Bank of America provides other online interfaces not covered by this Notice. If you visit or access your accounts from one of these sites, please review the online privacy practices of that site to understand how your online information may be collected, used and shared.
For U.S. account holders and visitors to this Site, we will use and share any information that we collect from or about you in accordance with the Bank of America U.S. Consumer Privacy Notice, which provides choices in the use and sharing of information. For Non-U.S. account holders utilizing this Site, we will use and share your account information in accordance with the privacy disclosure that covers your account and with the privacy and security rules applicable to the Bank of America affiliate or subsidiary that provides that account to you.
Additional information on our Privacy & Security practices may be found on our Sites and within Frequently Asked Questions (FAQs). Although the additional information is provided as a resource, the terms and conditions of this Notice control, and by using the Site, you agree to the terms and conditions of this Notice.
Collecting and Using Information
Personal Information We Collect Online
Personal Information means personally identifiable information such as information you provide via forms, surveys, applications or other online fields including name, postal or email addresses, telephone, fax or mobile numbers, or account numbers.
How We Use Personal Information
We may use Personal Information:
Cookie Guide
The use of cookies and similar technologies is a common internet practice. We have developed a Cookie Guide to provide very general information on cookies and similar technologies.
View cookie guide (PDF)
(PDFs require Adobe Reader)


Bank of America
Secure Sign-In
Online ID
Passcode
Sign In
Save Online ID
Security & Help
Forgot ID
Forgot Passcode
Enroll
Banking
BankAmericard Cash Rewards™ credit
1% cash back everywhere,
2% cash back at
Bank of America
Privacy & Security
Sign In
Home
Locations
Contact Us
Help
How can we help you?
Overview
Privacy
Account & Card Security
Online & Mobile Security
Report a Problem
Online Privacy Notice
PRINT
Bank of America U.S. Online Privacy Notice
Last updated July 24, 2014
This U.S. Online Privacy Notice (Notice) applies to this Bank of America online interface (i.e., website or mobile application) and any Bank of America U.S. affiliate or subsidiary online interface that links to this Notice, (each, a Site, and, collectively, Sites). The term "Bank of America" or "we" or "us" or "our" in this Notice refers to banking and non-banking U.S. affiliates or subsidiaries of Bank of America Corporation that link to this Notice. This Notice explains how information
Cookie Guide
The use of cookies and similar technologies is a common internet practice. We have developed a Cookie Guide to provide very general information on cookies and similar technologies.
View cookie guide (PDF)
(PDFs require Adobe Reader)
Protecting children's privacy online
The Site is not directed to individuals under the age of thirteen (13), and we request that these individuals do not provide Personal Information through the Site. We do not knowingly collect information from children under 13 without parental consent. Visit the Federal Trade Commission website for more information about the Children's
Protecting individual health information
To the extent that we receive, maintain, or process an individual's protected health information, Bank of America may disclose that information as authorized by and in accordance with applicable federal and/or state law.
This U.S. Online Privacy Notice is subject to change. Please review it periodically. If we make changes to the U.S. Online Privacy Notice, we will revise the "Last Updated" date at the top of this Notice. Any changes to this Notice will become effective when we post the revised Notice on the Site. Your use of the Site following these changes means that you accept the revised Notice.
Home | Accessible Banking | Privacy & Security | Careers | Site Map | Advertising Practices
Connect with us
Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2016 Bank of America Corporation.



unexpected & surprising practices easily overlooked among practices that are expected or irrelevant for the use context

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
FTC Chairwoman
January 2015

research questions

What practices are expected or unexpected?

How can we measure expectations and mismatches in expectations?

How can we emphasize unexpected practices in privacy notices?

types of expectations

Privacy literature

- **Privacy preferences**
- **Willingness to share/disclose**
- **Desired level of privacy**
- **Actual privacy**

malleable, uncertain, context-dependent

Acquisti et al. Privacy and human behavior in the age of information. Science, 2015.
Norberg et al. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 2007.
Palen & Dourish. Unpacking “privacy” for a networked world. CHI 2003.
Altman. The environment and social behavior: Privacy, personal space, territory, and crowding. 1975.
Nissenbaum. Privacy in Context – Technology, Policy, and the Integrity of Social Life. Stanford University Press, 2009.

types of expectations

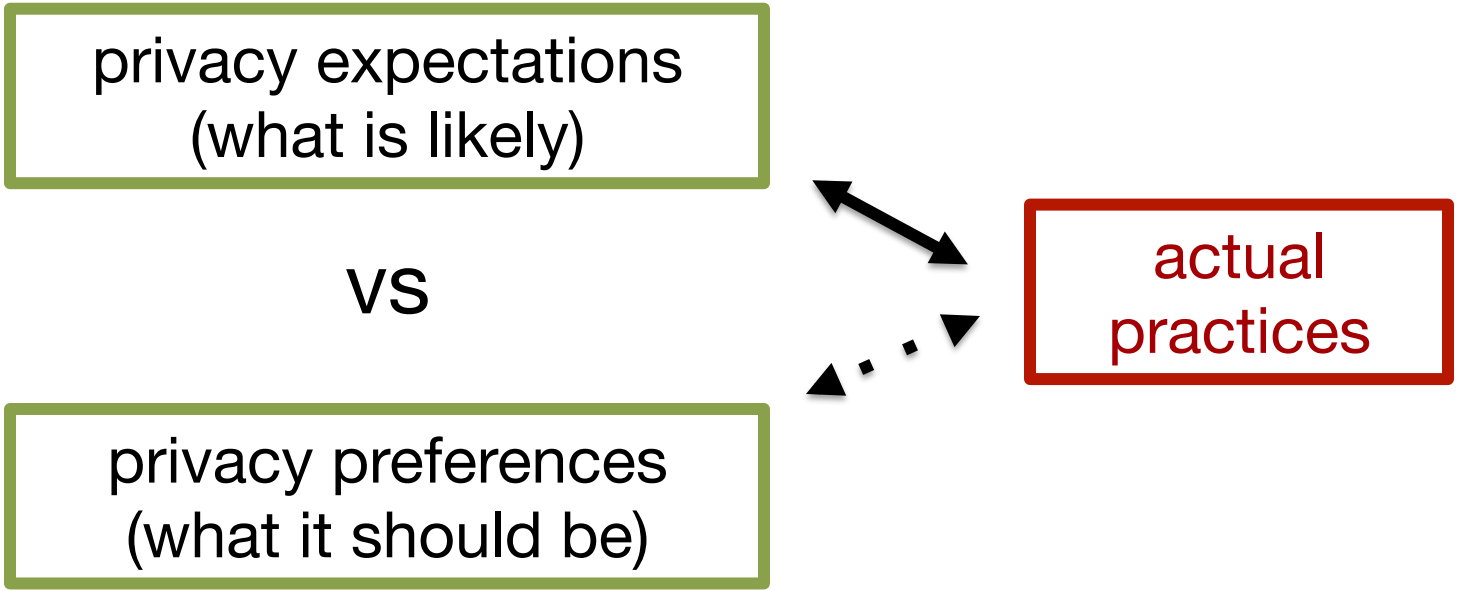
Other domains, e.g. consumer psychology, distinguish **different types of expectations**

Miller:

- **Ideal** (what it could be)
- **Expected** (what it likely will be)
- **Deserved** (what it should be)
- **Minimum Tolerable** (what it must be)

Miller J. A. Studying satisfaction … Conceptualization and Measurement of Consumer Satisfaction and Dissatisfaction 1977
Swan J. E. and Trawick I. F. Satisfaction related to predictive vs. desired expectations. Refining Concepts and Measures of Consumer Satisfaction and Complaining Behavior 1980

privacy expectations



methodology

elicit privacy expectations

- present participants with actual websites in online study
- ask participants to **rate likelihood** that website engages in certain data practices (objective expectation)

privacy policy analysis

- extract practices disclosed in website privacy policies

identify mismatches

- compare likelihood expectations with disclosed practices

data practices considered

data collection

- 4 information types: contact, financial, health, current location
- 2 scenarios: user with account, user without account

sharing with third parties

- 4 information types: contact, financial, health, current location
- 2 purposes: sharing for core purpose / other purpose

data deletion

- does the website allow deletion of personal data?

website features

website type:
finance
health
dictionary

popularity:
high rank
low rank

ownership:
private
government

user features

website experience
recent use, has account, familiarity, trust

demographics
age, gender, education, occupation, computer background

privacy
privacy protective behavior
privacy knowledge
negative online experience
online privacy concern (IUIPC)

study deployment

between-subjects study

- 16 websites
- 240 participants (Amazon Mechanical Turk)

- each participant randomly assigned to **one website**; 15 participants per website

example scenario description

"*Imagine that you are browsing [website name] website. You **do not have a user account** on [website name], that is, you have not registered or created an account on the website*"

"*What is the **likelihood that [website name] would** collect your information in this scenario? …*"

		Likely	Somewhat likely	Somewhat unlikely	Unlikely
Collects your **Contact information**	Email address	O	O	O	O
	Postal address	O	O	O	O
	Phone number	O	O	O	O
	Other Please specify	O	O	O	O

privacy policy analysis

ways to extract data practice statements from privacy policies

- machine-readable policy specification (e.g. P3P)
- (semi-)automated extraction of data practices from policy
- **manual annotation by experts**

USABLEPRIVACY.ORG
the usable privacy policy project

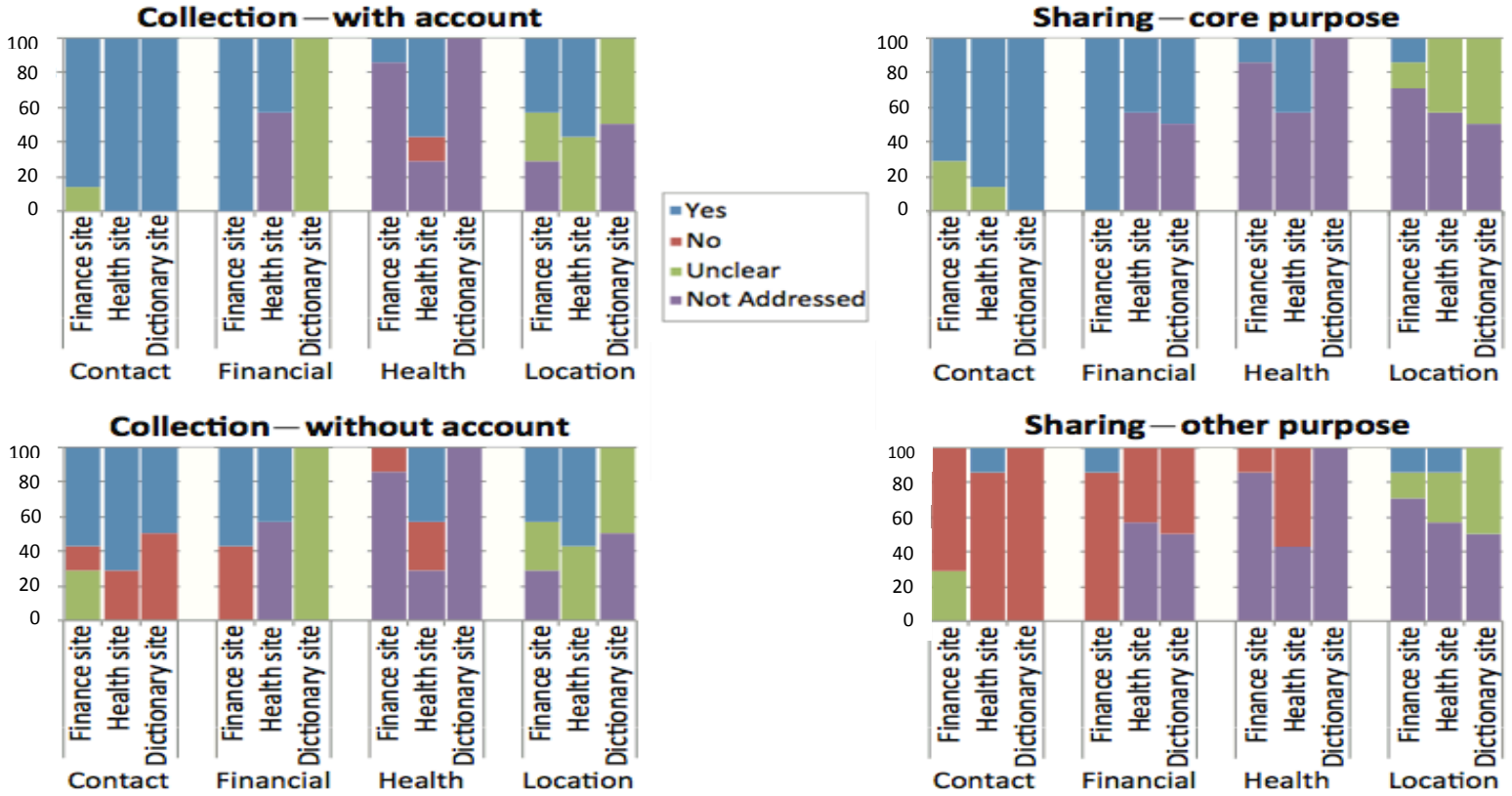
privacy policy analysis

extracting data practice statements from privacy policies

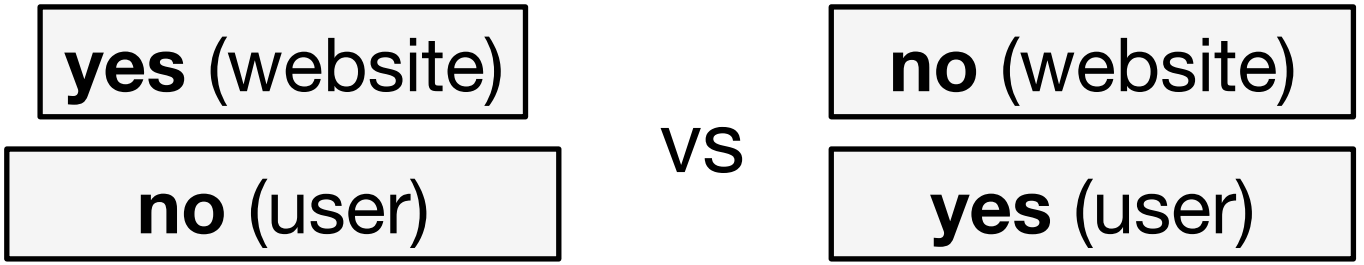
- **manual annotation by experts**
  - **Yes** website engages in practice
  - **No** website does not engage in practice
  - **Unclear** not clear if website engages in practice
  - **Not addressed** the policy is silent regarding practice

  - 2 annotators analyzed 16 websites' privacy policies

privacy policy analysis



types of mismatched expectations



- website shares data, but user doesn't expect it
- user may give up data unknowingly; website may lose trust

- website doesn't share data, but user thinks so
- user may not use website & lose utility; website may lose customer

different types of mismatches may impact user privacy differently

results

expectations

mismatches with policy statements

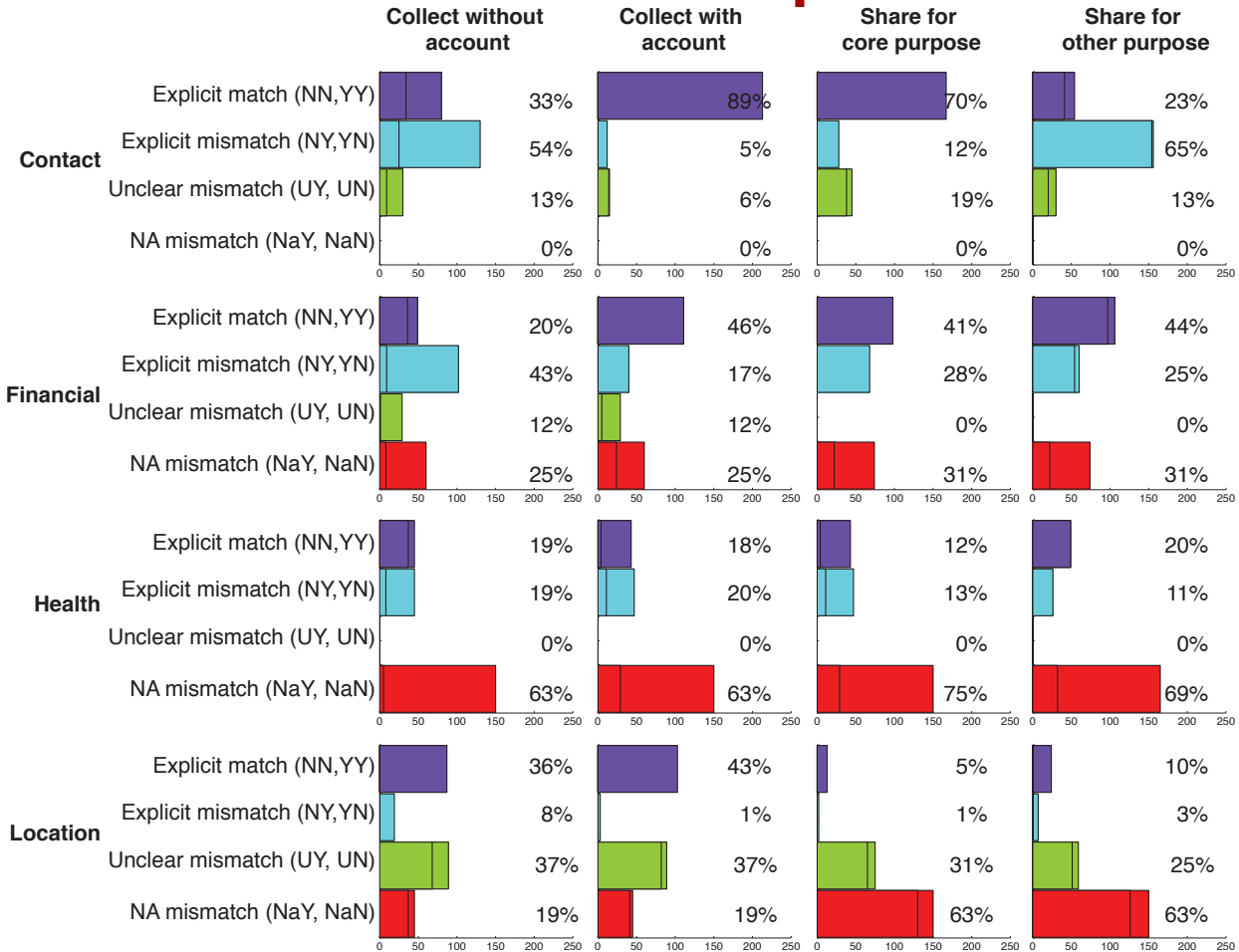
impact of website characteristics

- participants expect almost all websites to collect location and contact information and share it for core purposes
- **website type** had statistically significant effect on participants' expectations
  - for collection of financial & health information
  - for sharing of financial and health information
- popularity and ownership had no effect

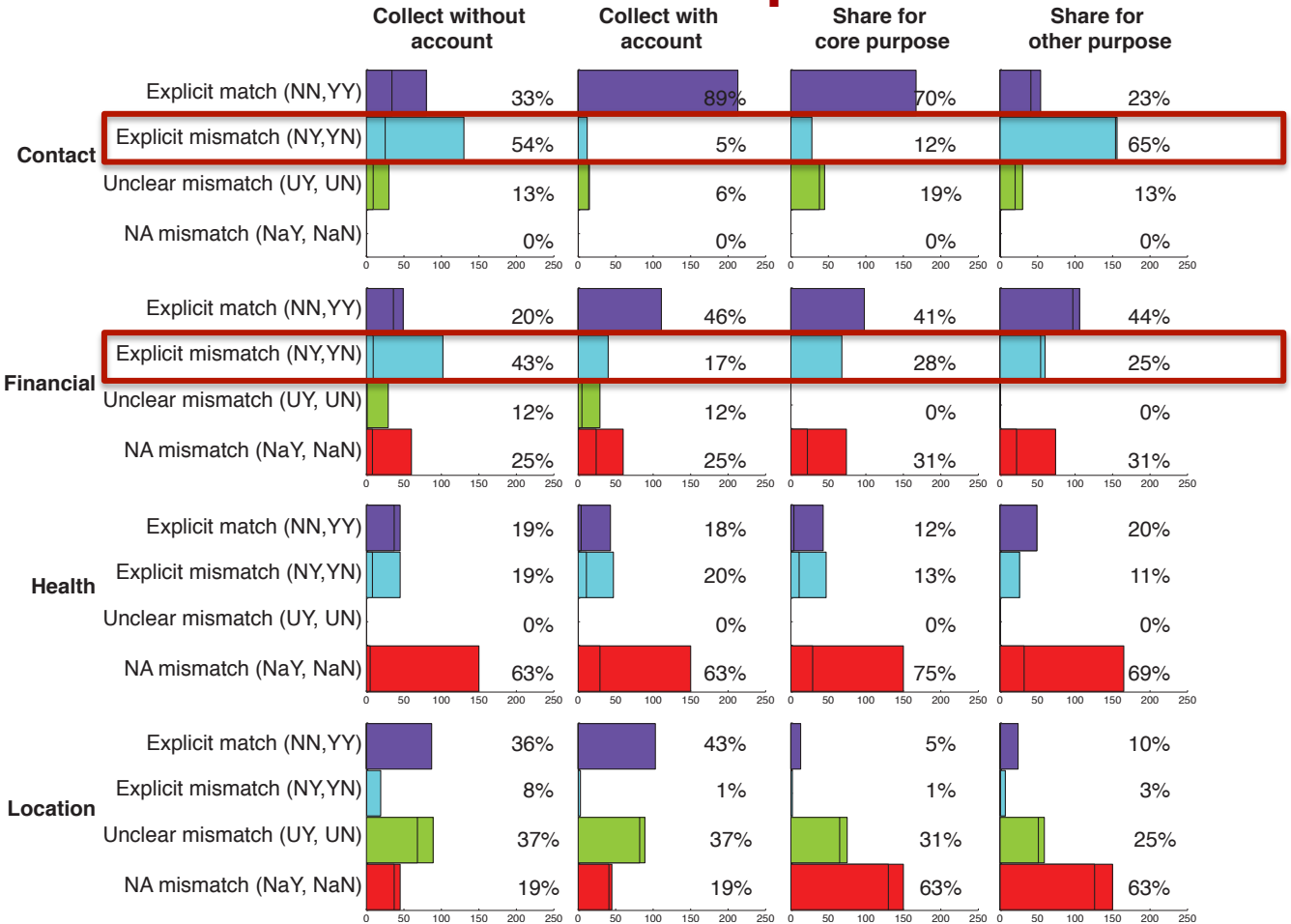
impact of user characteristics

collection of **location** information **with account**	**recent use**	➔	**NO**
	privacy concern	➔	**YES**
collection of **health** information **without account**	**privacy knowledge**	➔	**NO**
sharing of **location** information for **core purpose**	**trust in website**	➔	**YES**
	privacy concern	➔	**YES**
sharing of **contact** information for **core purpose**	**recent use**	➔	**NO**
	privacy concern	➔	**YES**
sharing of **financial** information for **other purposes**	**trust in website**	➔	**NO**
sharing of **health** information for **other purposes**	**trust in website**	➔	**YES**
allow deletion of personal data	**age**	➔	**NO**
	recent use	➔	**NO**
	trust in website	➔	**YES**

mismatched expectations



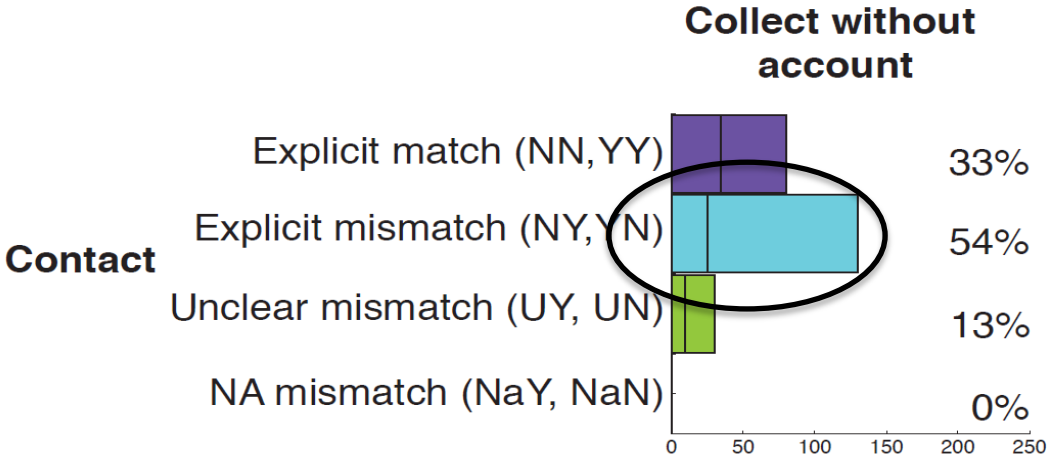
mismatched expectations



most explicit mismatches for contact and financial information

mismatched expectations

collection of contact information

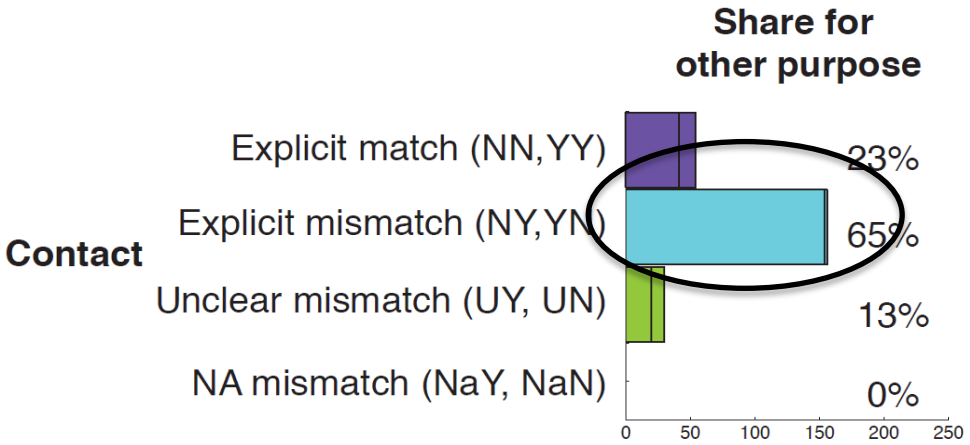


Yes—No
(Website – user)
mismatch

websites collect contact information without an account but participants don't expect it

mismatched expectations

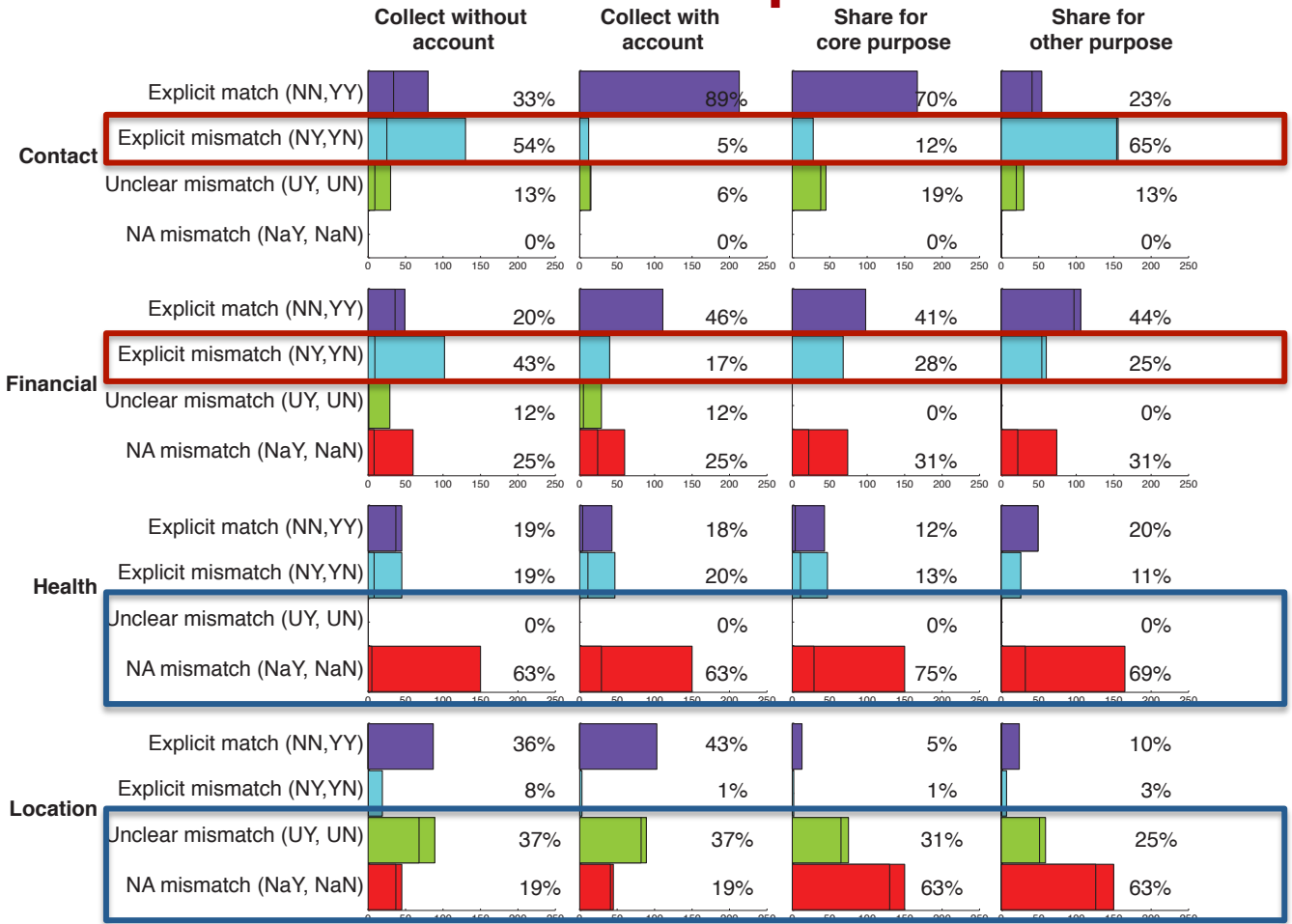
sharing of contact information for other purposes



No — Yes
(Website – user)
mismatch

participants expect that contact information is shared with third parties for any reason but websites do not share it for non-core purposes

mismatched expectations



most explicit mismatches for contact and financial information

but policies are less clear for health and location

mismatched expectations

data deletion

allow deletion	% users expect	% websites permit
Yes – full	**32%**	19%
Yes – partial	**48%**	12%
No	20%	19%

participants expect websites to permit deletion, but most websites don’t

mismatched expectations

summary

- few explicit mismatches but policies often unclear or silent on certain practices
- information collection without account often unexpected (contact, financial)
- participants assume that sharing is not limited to core purposes (e.g. also marketing)
- participants expect to be able to fully delete information, but most websites don’t allow it

limitations

- practices disclosed in privacy policy may not match service's actual behavior
- online / MTurk study to elicit expectations
- additional practices may be of interest
- additional websites may be of interest

highlighting unexpected practices

display in notice	# practices	% reduction
All practices	17	–
Mismatched practices only	11	35%
Unexpected practices only (Yes—No mismatch)	5	**70%**

potential reduction in information that users have to process in a layered or short notice

conclusions

- privacy expectations vs. preferences
- elicit expectations in surveys & compare with stated or actual data practices
- privacy expectations are affected by website type, privacy awareness, age, and experience with website
- opportunity for contextualizing and personalizing notices
- highlighting unexpected practices could reduce user burden and facilitate more informed privacy decision making

Florian Schaub
fschaub@cmu.edu
usableprivacy.org

Carnegie Mellon University

moving in the fall to

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN