18- Short-form Privacy Notices

Lorrie Cranor, Blase Ur, and Rich Shay

March 19, 2015

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

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

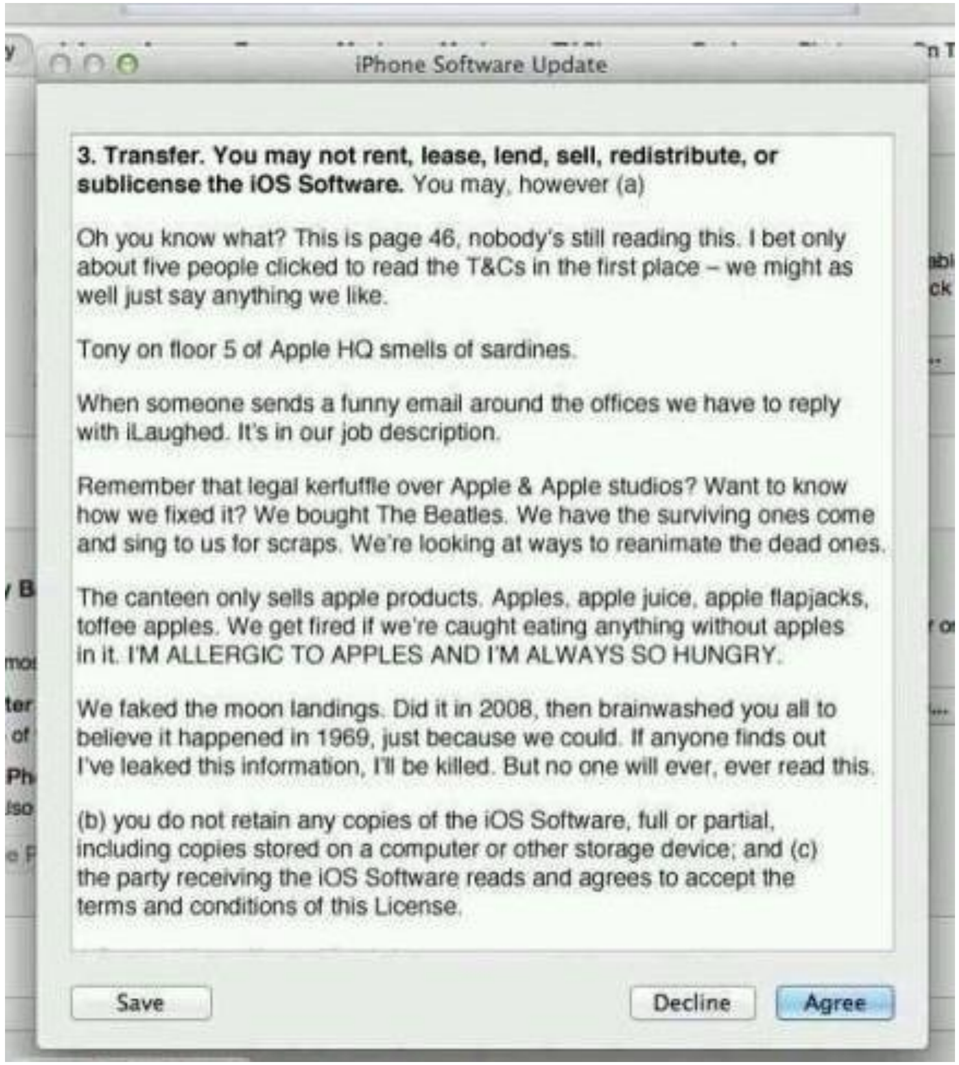
Today!

- Short-form, standardized privacy notice
- Standardized privacy notices in the U.S. financial industry
- Activity: designing a short-form notice

Problems with Privacy Policies

- They’re long…and there are many
  - A. McDonald and L.F. Cranor. The Cost of Reading Privacy Policies. ISJLP, 2008.
- They are written at a high reading level
  - “By lawyers, for lawyers”
- They may not even be in your language
  - B. Ur, M. Sleeper, L.F. Cranor. {Privacy, Privacidad, Приватност} Policies in Social Media: Providing Translated Privacy Notice. ISJLP, 2013.

Read it?

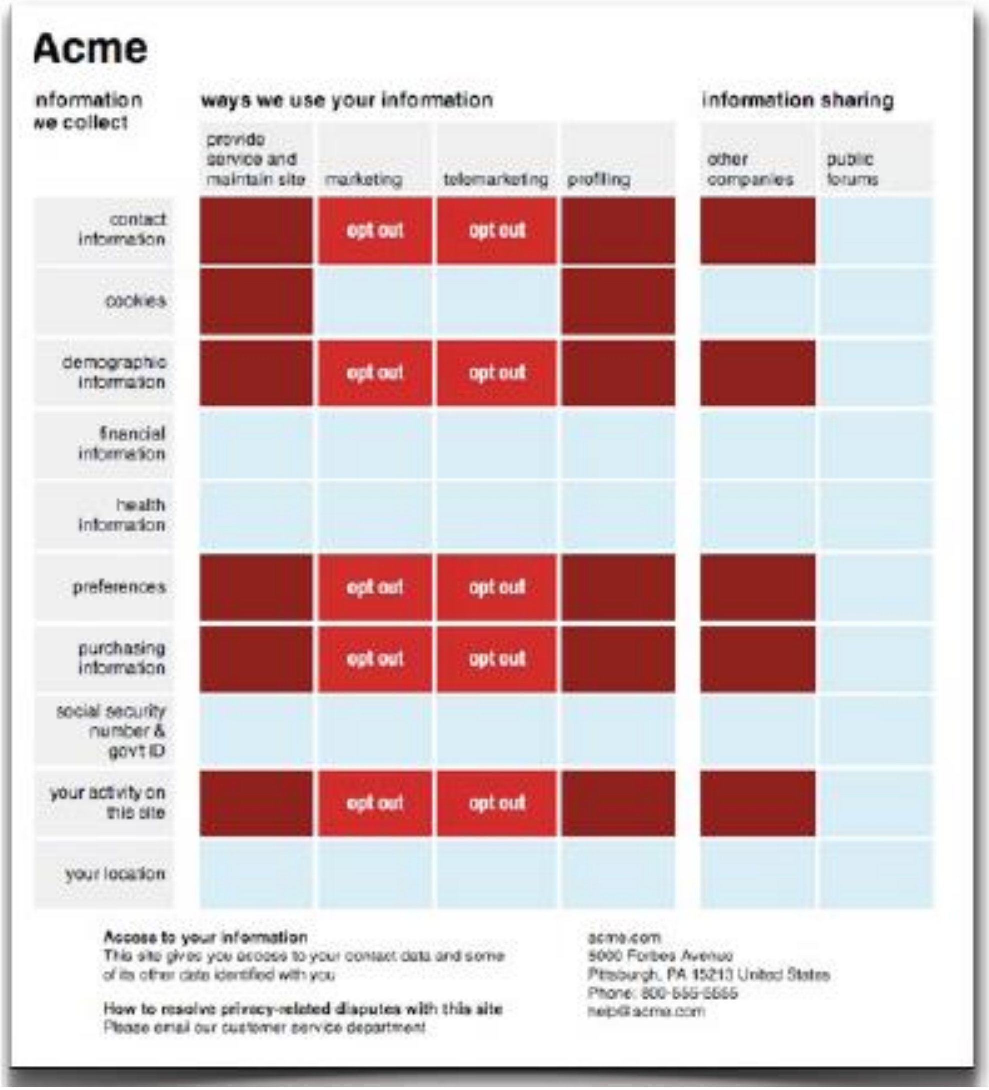


http://news.mydrivers.com/1/277/277017.htm

Short-form Privacy Notices

- Give the average consumer a succinct summary of relevant information
- *Let's brainstorm advantages*
- *Let's brainstorm disadvantages*

Privacy Nutrition Labels



Acme

information we collect	ways we use your information: provide service and maintain site	marketing	telemarketing	profiling	information sharing: 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 & govt ID						
your activity on this site		opt out	opt out			
your location						

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

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

https://cups.cs.cmu.edu/privacyLabel/

Privacy Icons

- Mozilla privacy icons

https://wiki.mozilla.org/Privacy_Icons

Terms of Service; Didn't Read

https://tosdr.org

Terms of Service; Didn't Read   Ratings   About   Follow us @tosdr   Donate: Flattr this!

Google Class C

- Google keeps your searches and other identifiable user information for an undefined period of time
- Google can use your content for all their existing and future services
- This service tracks you on other websites
- Google can share your personal information with other parties
- Google may stop providing services to you at any time

More details

YouTube Class D

- Terms may be changed any time at their discretion, without notice to the user
- They can remove your content at any time and without prior notice
- The copyright license is broader than necessary
- Reduction of legal period for cause of action
- Deleted videos are not really deleted

More details

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 B

- 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

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

Lorrie Faith Cranor, Kelly Idouchi, Pedro G. Leon, Manya Sleeper, and Blase Ur. WEIS 2013 (and forthcoming journal article)

Carnegie Mellon University

Background

- Gramm-Leach-Bliley Act (1999)
  - Annual privacy disclosures

Background

- Gramm-Leach-Bliley Act (1999)
  – Annual privacy disclosures

- “Notices have been formatted in various ways and as a result have been difficult to compare, even among financial institutions with identical practices”

Comparing Policies

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:

- to respond to your inquiries and fulfill your requests;
- to send you important information regarding the Site, changes to terms, conditions, and policies and/or other administrative information;
- to send you marketing communications that we believe may be of interest to you;
- to personalize your experience on the Site by presenting content, ads or offers tailored to you;
- to allow you to apply for products or services (e.g., to prequalify for a mortgage, apply for a credit card, or to open a retirement account, investment account or other financial product) and evaluate your eligibility for such products or services;
- to verify your identity and/or location (or the identity or location of your representative or agent) in order to allow access to your accounts, conduct online transactions and to maintain measures aimed at preventing fraud and protecting the security of account and Personal Information;
- to allow you to participate in surveys, sweepstakes, contests and similar promotions and to administer these activities. Some of these activities have additional rules, which may contain additional information about how Personal Information is used and shared;
- to allow you to use Site financial planning tools. Please note that some planning tools require that you provide Personal Information to use (e.g., mortgage interest rate tracker), whereas others do not (e.g., mortgage calculator). Information that you enter into one of these planning tools may be stored for future access and use. You have the option not to save the information;
- collected through aggregation services such as My Portfolio® and My Financial Picture® in order to consolidate your financial account information at one online location; understand what product or service may be of interest to you; and present you with offers;
- collected through our social media pages and interactions with you to assist in verifying your identity and account status. We may combine this information with information we already have;

Information Collected

There are portions of this site where we may need to collect personally identifiable information about you (such as your address, phone number and other information) for identification purposes or to fulfill your online requests. We may obtain information about you directly from you, through your use of our products and services and from third parties (such as credit bureaus and demographic firms). Any use by us of your personal information will be pursuant to the privacy policy provided to you in connection with your account with us.

In addition, When you visit our site, our web servers collect the name of the domain you used to access the Internet (such as aol.com), which pages on our site you visited and when they were visited, your Internet browser type and platform, the link that brought you to our site and any links clicked within our site. This information may be used by us, our service providers, affiliates and business partners to measure the number of visits, average time spent, page views and other statistics about visitors to our site. We also use this data to monitor site performance and make the site easier and more convenient to use.

Our web servers also seek (as many Web sites do) to place a "cookie" (a small data file) on your computer's hard drive which allows the server to determine the computer when it visits again in order to track statistical information about navigation to and throughout certain areas of our site and to promotions on other sites. This cookie is not used to obtain your name or any personal data, and the information that is tracked is used only for internal purposes, such as to improve site navigation and to measure the effectiveness of our site, and is not shared with anyone other than GECRB affiliates and contractors who assist GECRB in these efforts and who are bound to confidentiality. However, if you prefer not to accept cookies, you can set your browser to reject them or to alert you before one is placed.

Comparing Policies

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:

- to respond to your inquiries and fulfill your requests;
- to send you important information regarding the Site, changes to terms, conditions, and policies and/or other administrative information;
- to send you marketing communications that we believe may be of interest to you;
- to personalize your experience on the Site by presenting content, ads or offers tailored to you;
- to allow you to apply for products or services (e.g., to prequalify for a mortgage, apply for a credit card, or to open a retirement account, investment account or other financial product) and evaluate your eligibility for such products or services;
- to verify your identity and/or location (or the identity or location of your representative or agent) in order to allow access to your accounts, conduct online transactions and to maintain measures aimed at preventing fraud and protecting the security of account and Personal Information;
- to allow you to participate in surveys, sweepstakes, contests and similar promotions and to administer these activities. Some of these activities have additional rules, which may contain additional information about how Personal Information is used and shared;
- to allow you to use Site financial planning tools. Please note that some planning tools require that you provide Personal Information to use (e.g., mortgage interest rate tracker), whereas others do not (e.g., mortgage calculator). Information that you enter into one of these planning tools may be stored for future access and use. You have the option not to save the information;
- collected through aggregation services such as My Portfolio® and My Financial Picture® in order to consolidate your financial account information at one online location; understand what product or service may be of interest to you; and present you with offers;
- collected through our social media pages and interactions with you to assist in verifying your identity and account status. We may combine this information with information we already have;

Information Collected

There are portions of this site where we may need to collect personally identifiable information about you (such as your address, phone number and other information) for identification purposes or to fulfill your online requests. We may obtain information about you directly from you, through your use of our products and services and from third parties (such as credit bureaus and demographic firms). Any use by us of your personal information will be pursuant to the privacy policy provided to you in connection with your account with us.

In addition, When you visit our site, our web servers collect the name of the domain you used to access the Internet (such as aol.com), which pages on our site you visited and when they were visited, your Internet browser type and platform, the link that brought you to our site and any links clicked within our site. This information may be used by us, our service providers, affiliates and business partners to measure the number of visits, average time spent, page views and other statistics about visitors to our site. We also use this data to monitor site performance and make the site easier and more convenient to use.

Our web servers also seek (as many Web sites do) to place a "cookie" (a small data file) on your computer's hard drive which allows the server to determine the computer when it visits again in order to track statistical information about navigation to and throughout certain areas of our site and to promotions on other sites. This cookie is not used to obtain your name or any personal data, and the information that is tracked is used only for internal purposes, such as to improve site navigation and to measure the effectiveness of our site, and is not shared with anyone other than GECRB affiliates and contractors who assist GECRB in these efforts and who are bound to confidentiality. However, if you prefer not to accept cookies, you can set your browser to reject them or to alert you before one is placed.

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: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
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	■ Call **[phone number]**—our menu will prompt you through your choice(s) ■ Visit us online: **[website]** or ■ Mail the form below **Please note:** 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. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [website]

✂

Mail-in Form

Leave Blank **OR** [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ❑ Apply my choices only to me]	Mark any/all you want to limit: ❑ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ❑ Do not allow your affiliates to use my personal information to market to me. ❑ Do not share my personal information with nonaffiliates to market their products and services to me.

Name		**Mail to:** [Name of Financial Institution] [Address1] [Address2] [City], [ST] [ZIP]
Address		
City, State, Zip		
[Account #]		

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 ■ [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.]
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. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

Data Collection

- FDIC directory of 7,072 institutions

- Download top 10 results for Google query:

FACTS WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?

- Restrict to institution’s web domain

Data Extraction

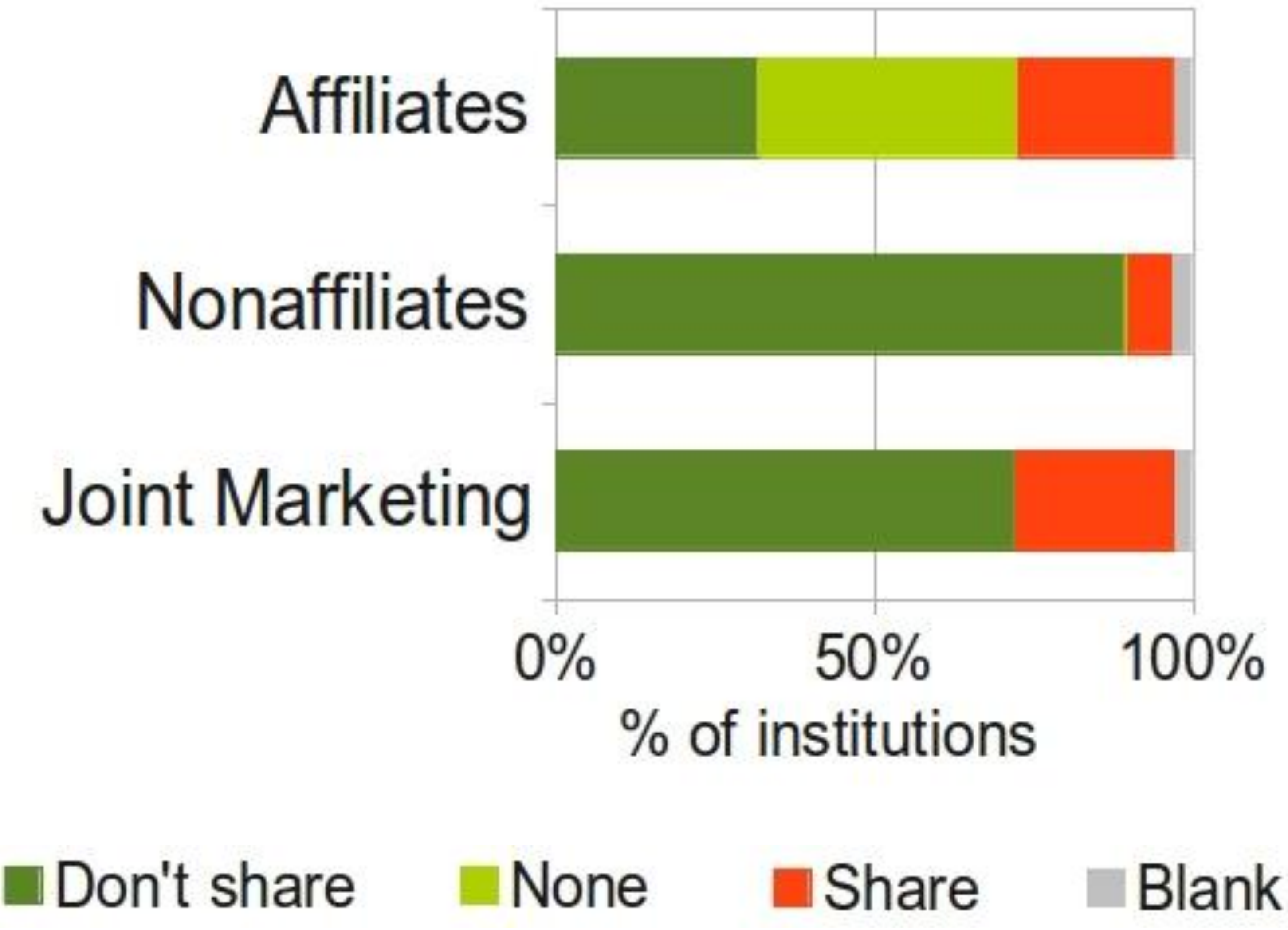
- Convert HTML or PDF to text
- Regular expressions (pattern matching)
  - Structure of document
- Manual verification: 90%+ accurate per section on a random sample of 50 policies

We compared
3,422 financial institutions’
privacy and data-sharing practices

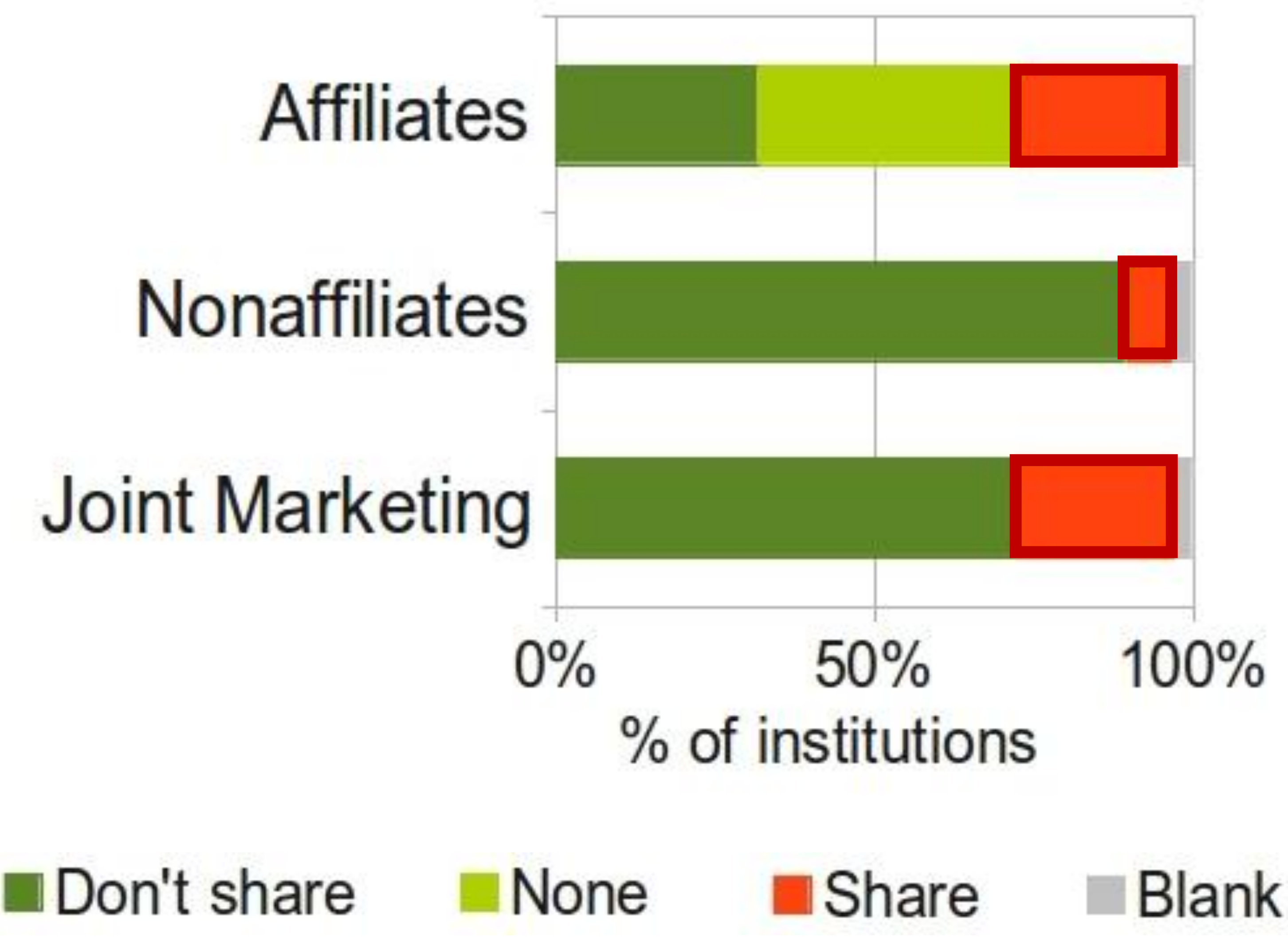
We compared 3,422 financial institutions' privacy and data-sharing practices

Creative commons: Jeff Adair, http://www.flickr.com/photos/jeffadair

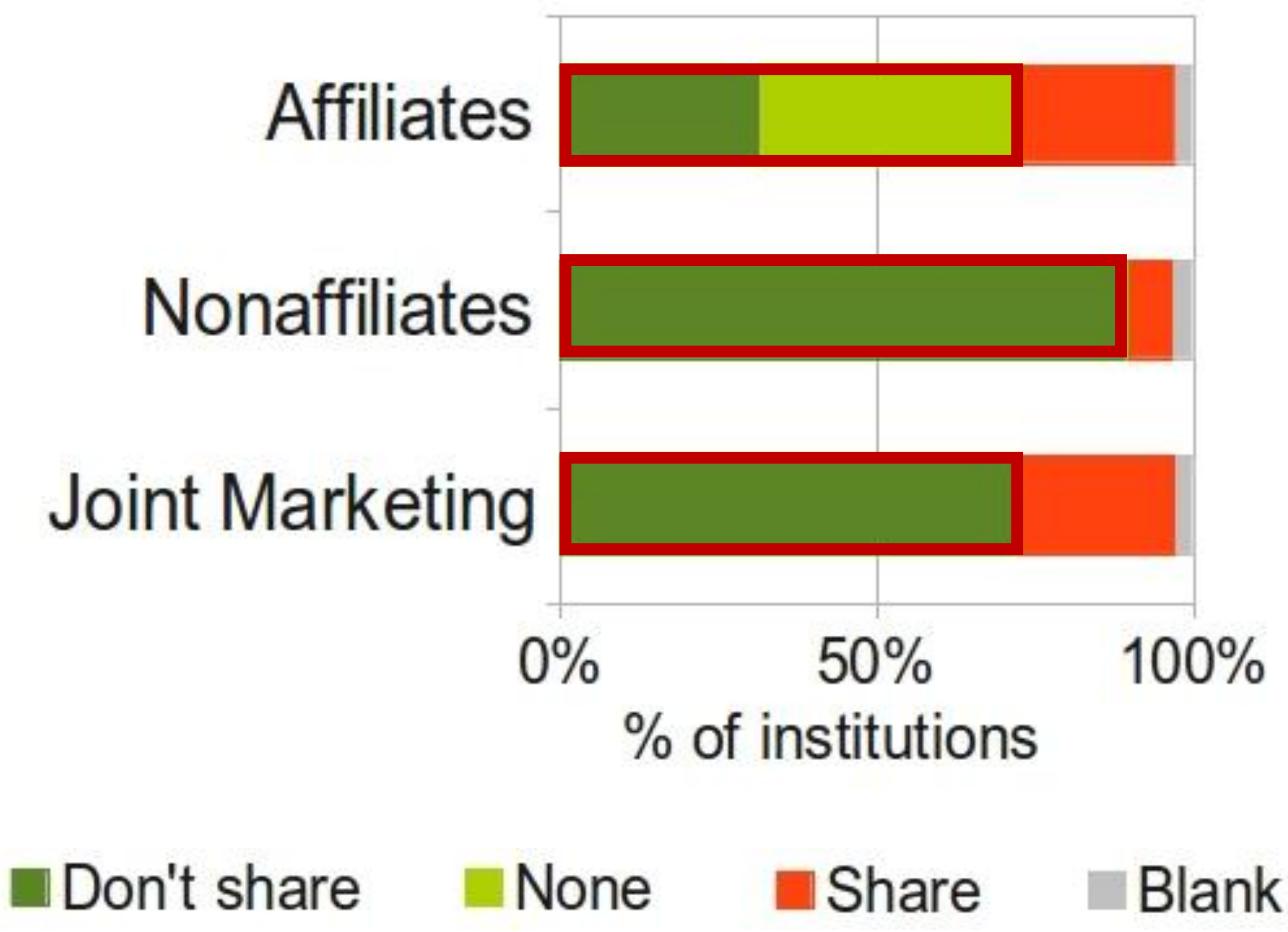
With Whom is Information Shared?



With Whom is Information Shared?



With Whom is Information Shared?



For What Reasons?

Reasons we can share your personal information	Does MB Financial Bank, N.A. 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	Yes	No
For our marketing purposes — to offer our products and services to you	Yes	Yes
For joint marketing with other financial companies	Yes	Yes
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	No	We don't share
For our affiliates to market to you	Yes	Yes
For nonaffiliates to market to you	No	We don't share

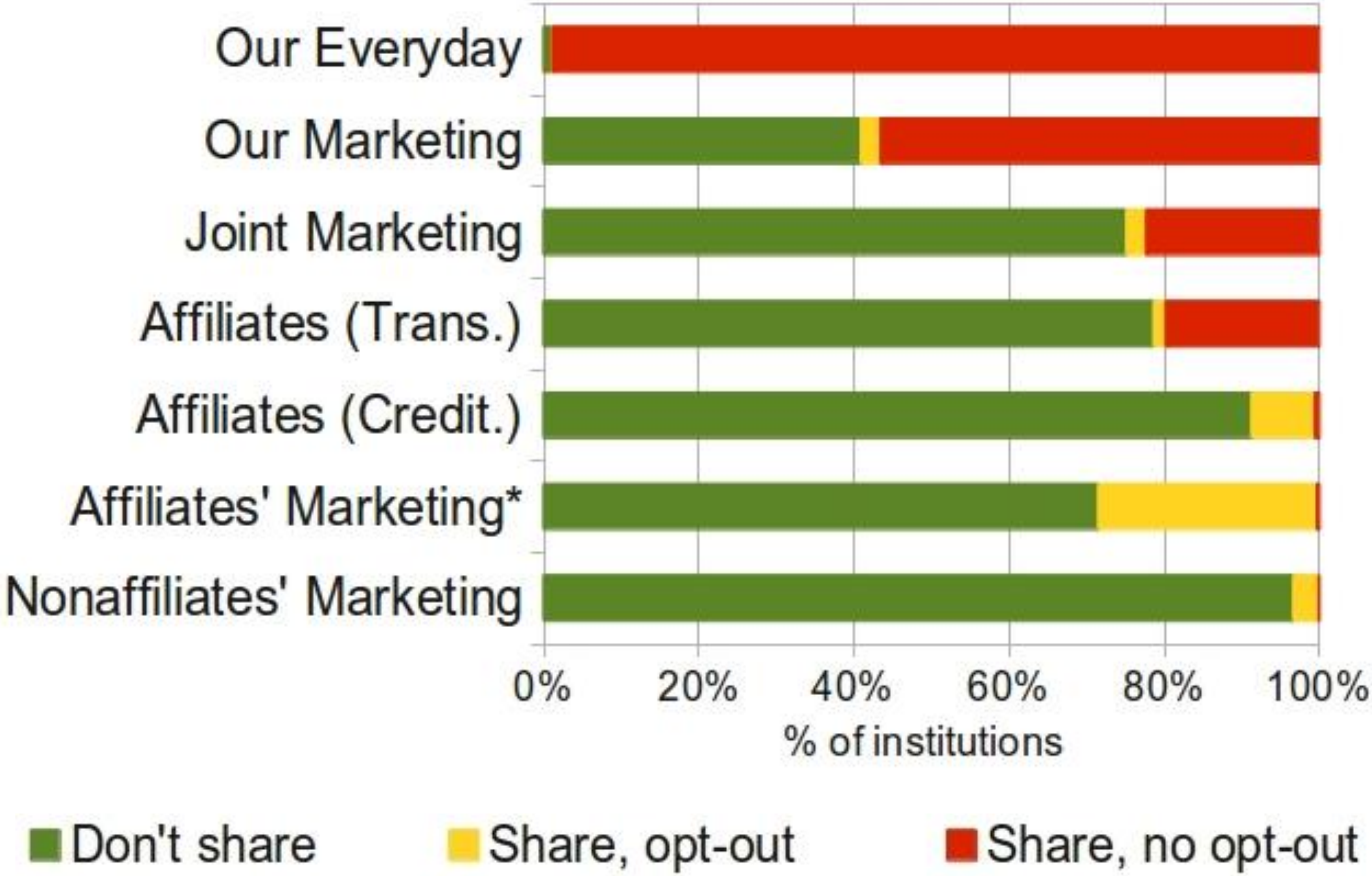
For What Reasons?

Reasons we can share your personal information	Does MB Financial Bank, N.A. 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	Yes	No
For our marketing purposes — to offer our products and services to you	Yes	Yes
For joint marketing with other financial companies	Yes	Yes
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	No	We don't share
For our affiliates to market to you	Yes	Yes
For nonaffiliates to market to you	No	We don't share

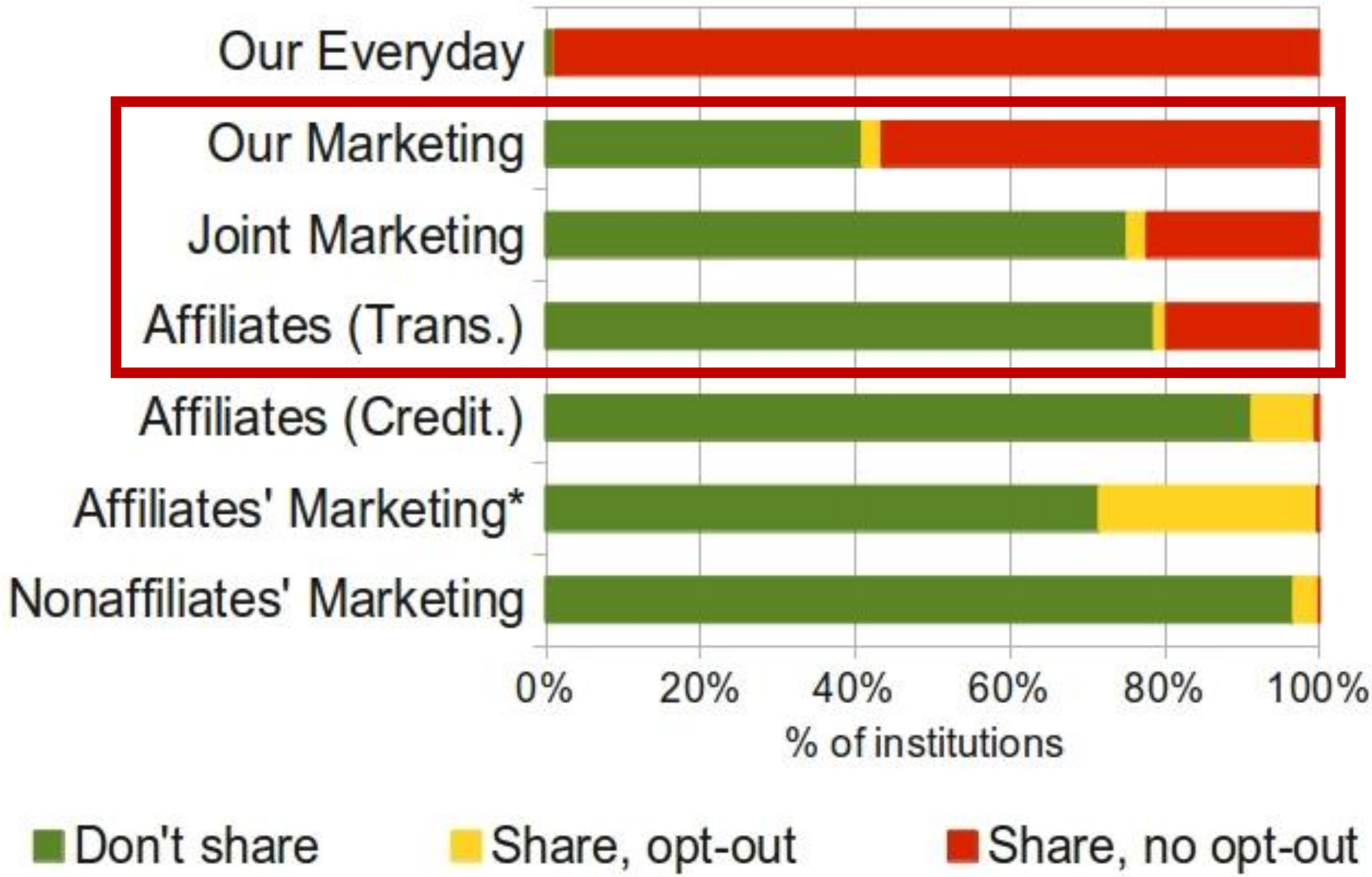
For What Reasons?

Reasons we can share your personal information	Does MB Financial Bank, N.A. 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	Yes	No
For our marketing purposes — to offer our products and services to you	Yes	Yes
For joint marketing with other financial companies	Yes	Yes
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	No	We don't share
For our affiliates to market to you	Yes	Yes
For nonaffiliates to market to you	No	We don't share

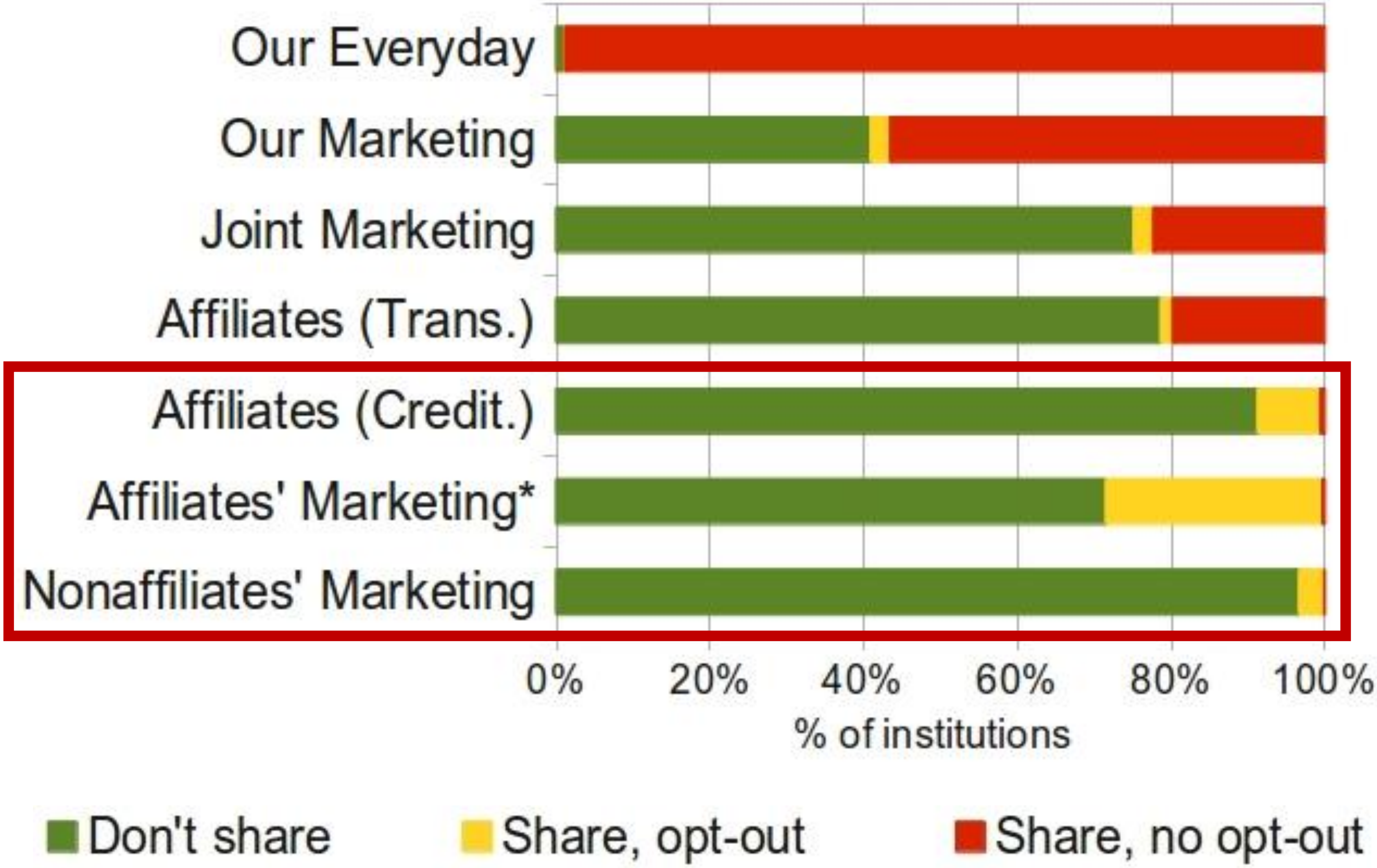
For What Reasons?



For What Reasons?



For What Reasons?



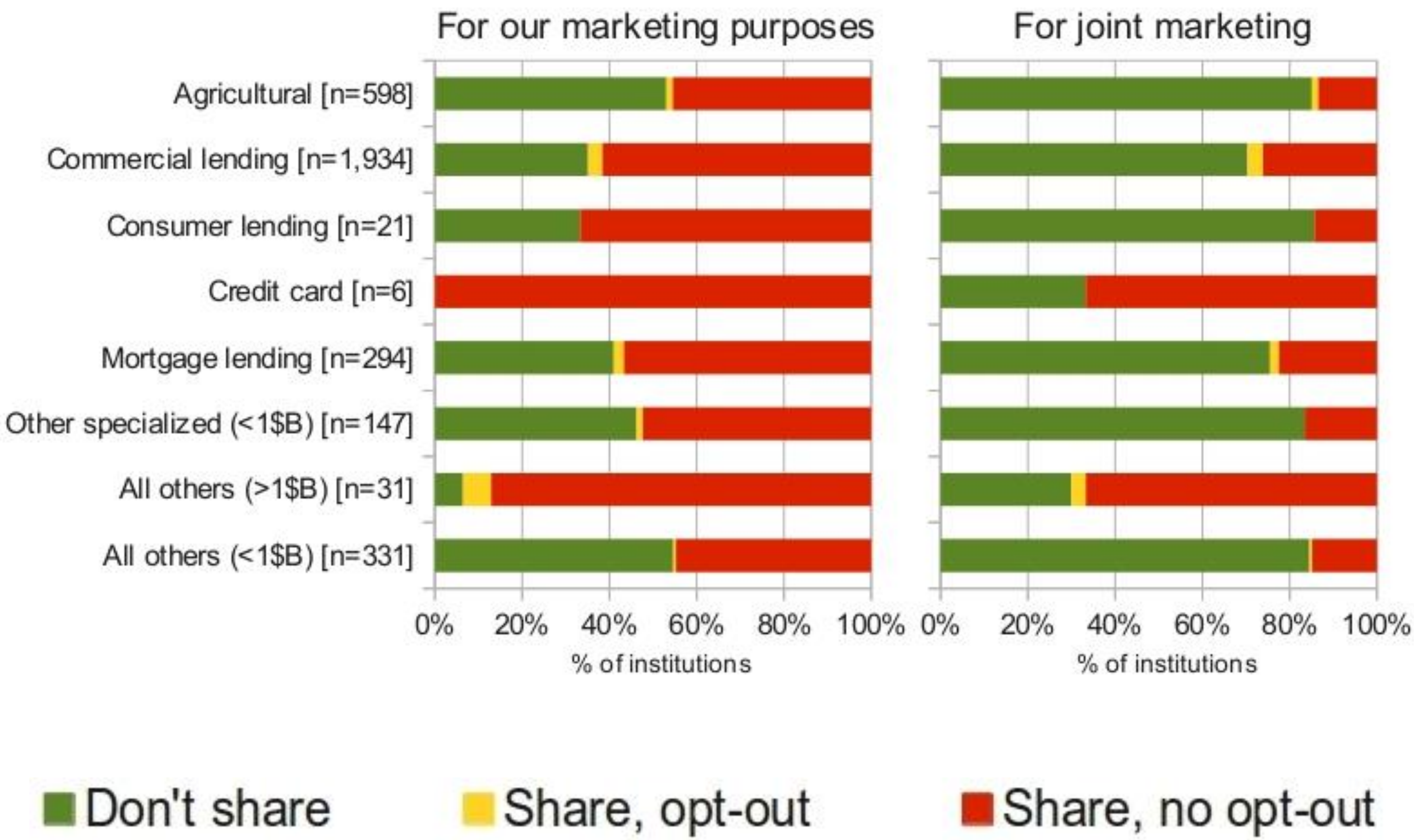
Comparing Competitors

Creative commons: Jeff Adair,
http://www.flickr.com/photos/jeffadair
and Edo, http://www.flickr.com/photos/10nl

Comparing Competitors

Creative commons: Jeff Adair,
http://www.flickr.com/photos/jeffadair
and Edo, http://www.flickr.com/photos/10nl

Comparing Competitors



Comparing Competitors

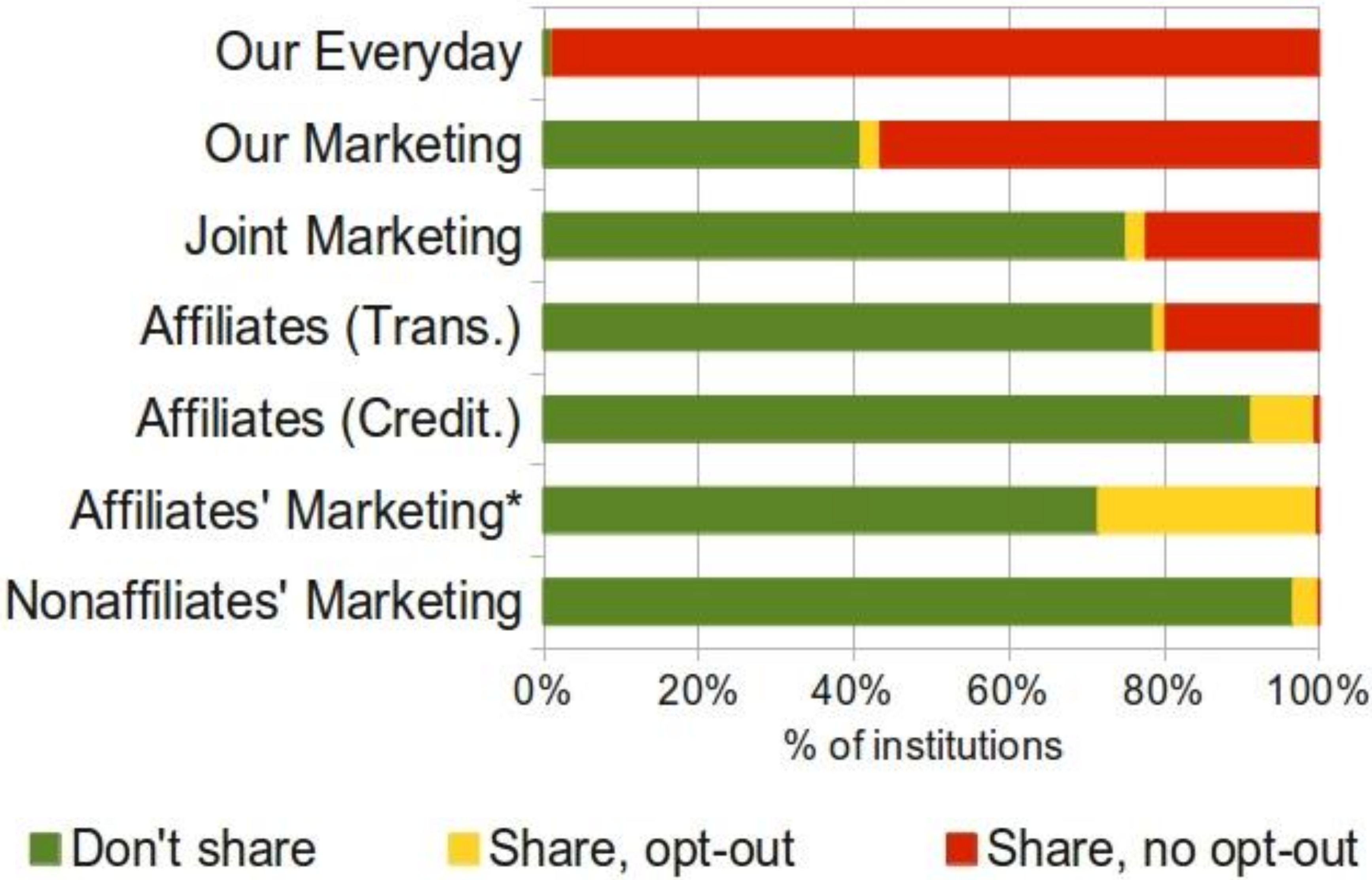
- Forbes list of the 100 largest banks

- J.D. Power credit card satisfaction survey

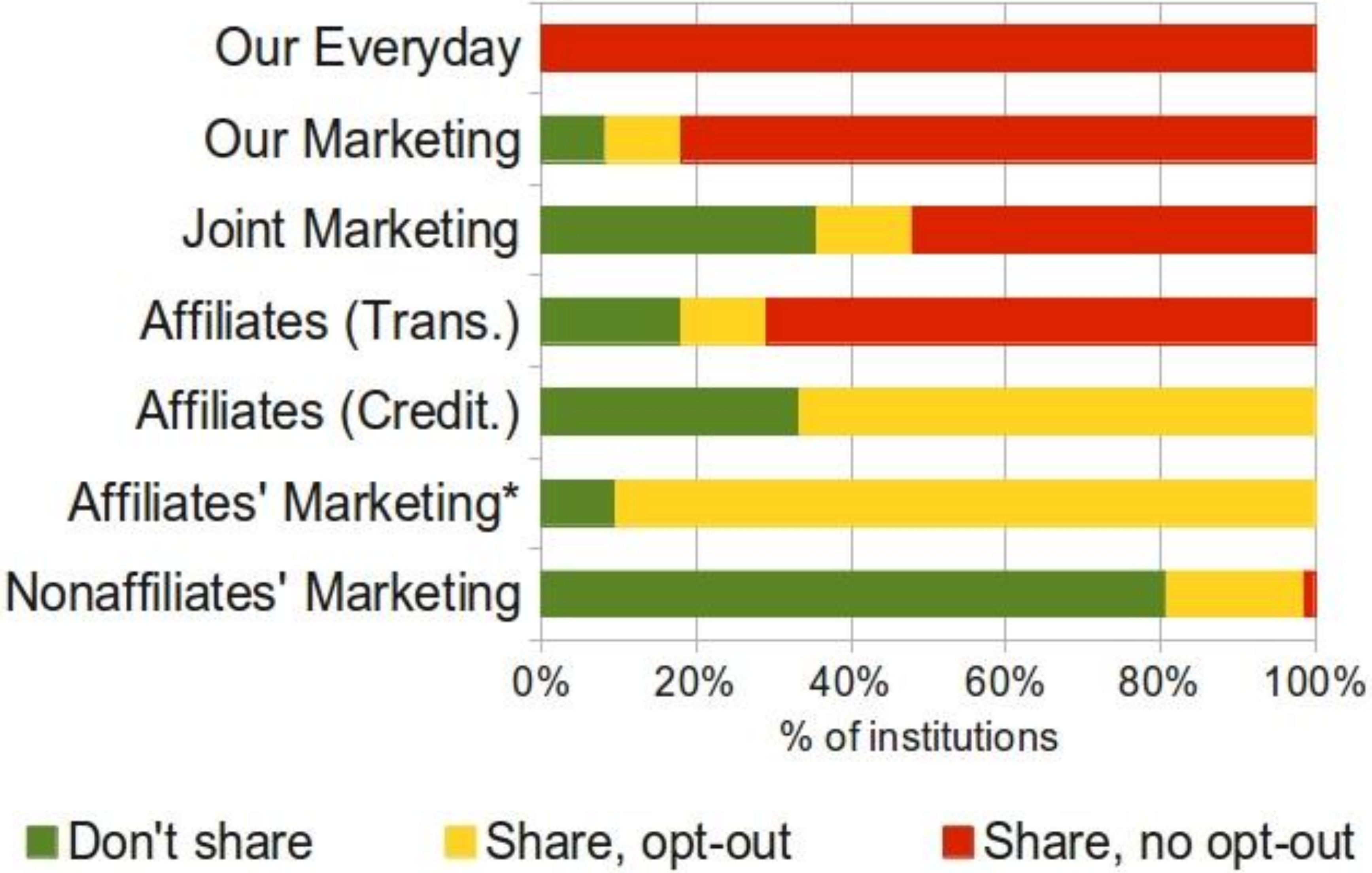
Comparing Competitors

- Forbes list of the 100 largest banks
- J.D. Power credit card satisfaction survey
- **We again found differences in practices**
  - **Opportunity for consumer privacy choice**

For What Reasons?



For What Reasons? (Largest)



Comparing Credit Cards

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

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

Opt-Out Mechanisms

- Email, phone, postal mail, website
- 69.1% of institutions did not offer a computer-based opt-out
- 32.6% offered only a phone opt-out

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

Conclusions and Future Work

- Institutions **are** actually different
  - Largest institutions have the worst practices
  - Opportunity for consumer privacy choice
- Site for consumers/banks/regulators: **http://cups.cs.cmu.edu/bankprivacy**
- Model privacy form prohibits companies from making complete disclosures
  - Most banks used standardized notice *in place of* long-form privacy disclosure

Activity

- Let’s complete a design activity we’ve borrowed from the folks at Facebook