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
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

• They are written at a high reading level
  – “By lawyers, for lawyers”

• They may not even be in your language
3. Transfer. You may not rent, lease, lend, sell, redistribute, or sublicense the iOS Software. You may, however (a)

Oh you know what? This is page 46, nobody's still reading this. I bet only about five people clicked to read the T&Cs in the first place – we might as well just say anything we like.

Tony on floor 5 of Apple HQ smells of sardines.

When someone sends a funny email around the offices we have to reply with iLaughed. It's in our job description.

Remember that legal kerfuffle over Apple & Apple studios? Want to know how we fixed it? We bought The Beatles. We have the surviving ones come and sing to us for scraps. We're looking at ways to reanimate the dead ones.

The canteen only sells apple products. Apples, apple juice, apple flapjacks, toffee apples. We get fired if we're caught eating anything without apples in it. I'M ALLERGIC TO APPLES AND I'M ALWAYS SO HUNGRY.

We faked the moon landings. Did it in 2008, then brainwashed you all to believe it happened in 1969, just because we could. If anyone finds out I've leaked this information, I'll be killed. But no one will ever, ever read this.

(b) you do not retain any copies of the iOS Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the iOS Software reads and agrees to accept the terms and conditions of this License.

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

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

- Mozilla privacy icons

https://wiki.mozilla.org/Privacy_Icons
Terms of Service; Didn’t Read

**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)
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 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 on 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 agent, distributor 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 GECCB affiliates and contractors who assist GECCB 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

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 balance] and [payment history]
- [credit history] and [credit scores]

How?
All financial companies need to share customers' personal information to run their everyday business. In this 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 | Call [phone number]—our menu will prompt you through your choice(s) | [insert]
For our marketing purposes—to offer our products and services to you | Visit our online [website] or | [insert]
For joint marketing with other financial companies | Mail the form below | [insert]
For our affiliates' everyday business purposes—information about your transactions and experiences | [Call [phone number] or go to [website]] | [insert]
For our affiliates' everyday business purposes—information about your creditworthiness | | [insert]
For our affiliates to market to you | | [insert]
For nonaffiliates to market to you | | [insert]

To limit our sharing
- Call [phone number]—our menu will prompt you through your choice(s)
- Visit our 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]

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.

How does [name of financial institution] collect my personal information?
- [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
With Whom is Information Shared?

- **Affiliates**
- **Nonaffiliates**
- **Joint Marketing**

The diagram shows the distribution of institutions that do not share, share, or leave blank for each category.
With Whom is Information Shared?

- **Affiliates**: A small percentage share information.
- **Nonaffiliates**: A significant percentage share information.
- **Joint Marketing**: A moderate percentage share information.
With Whom is Information Shared?
## For What Reasons?

<table>
<thead>
<tr>
<th>Reasons we can share your personal information</th>
<th>Does MB Financial Bank, N.A. 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>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>For our marketing purposes —</strong> to offer our products and services to you</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>For joint marketing with other financial companies</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>For our affiliates’ everyday business purposes —</strong> information about your transactions and experiences</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>For our affiliates’ everyday business purposes —</strong> information about your creditworthiness</td>
<td>No</td>
<td>We don’t share</td>
</tr>
<tr>
<td><strong>For our affiliates to market to you</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>For nonaffiliates to market to you</strong></td>
<td>No</td>
<td>We don’t share</td>
</tr>
<tr>
<td>Reasons we can share your personal information</td>
<td>Does MB Financial Bank, N.A. share?</td>
<td>Can you limit this sharing?</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>----------------------------</td>
</tr>
<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>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our marketing purposes — to offer our products and services to you</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>For joint marketing with other financial companies</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>For our affiliates’ everyday business purposes — information about your transactions and experiences</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates’ everyday business purposes — information about your creditworthiness</td>
<td>No</td>
<td>We don’t share</td>
</tr>
<tr>
<td>For our affiliates to market to you</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>For nonaffiliates to market to you</td>
<td>No</td>
<td>We don’t share</td>
</tr>
</tbody>
</table>
# For What Reasons?

<table>
<thead>
<tr>
<th>Reasons we can share your personal information</th>
<th>Does MB Financial Bank, N.A. share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For our everyday business purposes —</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>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></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>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>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>For our affiliates’ everyday business purposes —</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>information about your transactions and experiences</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For our affiliates’ everyday business purposes —</strong></td>
<td>No</td>
<td>We don’t share</td>
</tr>
<tr>
<td>information about your creditworthiness</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For our affiliates to market to you</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>For nonaffiliates to market to you</strong></td>
<td>No</td>
<td>We don’t share</td>
</tr>
</tbody>
</table>
For What Reasons?

- Our Everyday: 100%
- Our Marketing: 75%
- Joint Marketing: 90%
- Affiliates (Trans.): 85%
- Affiliates (Credit.): 95%
- Affiliates' Marketing*: 80%
- Nonaffiliates' Marketing: 70%
For What Reasons?

- Our Everyday: 100%
- Our Marketing: 80% don't share, 20% share, opt-out
- Joint Marketing: 70% don't share, 30% share, no opt-out
- Affiliates (Trans.): 80% don't share, 20% share, opt-out
- Affiliates (Credit.): 70% don't share, 30% share, no opt-out
- Affiliates' Marketing*: 80% don't share, 20% share, opt-out
- Nonaffiliates' Marketing: 90% don't share, 10% share, no opt-out

Legend:
- Don't share
- Share, opt-out
- Share, no opt-out
For What Reasons?

- Our Everyday
- Our Marketing
- Joint Marketing
- Affiliates (Trans.)
- Affiliates (Credit.)
- Affiliates' Marketing*
- Nonaffiliates' Marketing

Legend:
- Don't share
- Share, opt-out
- Share, no opt-out
Comparing Competitors

Comparing Competitors

Comparing Competitors

For our marketing purposes

- Agricultural [n=598]
- Commercial lending [n=1,934]
- Consumer lending [n=21]
- Credit card [n=6]
- Mortgage lending [n=294]
- Other specialized (<1$B) [n=147]
- All others (>1$B) [n=31]
- All others (<1$B) [n=331]

For joint marketing

- Don't share
- Share, opt-out
- Share, no opt-out
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?

- Our Everyday
- Our Marketing
- Joint Marketing
- Affiliates (Trans.)
- Affiliates (Credit.)
- Affiliates' Marketing*
- Nonaffiliates' Marketing

Legend:
- Don't share
- Share, opt-out
- Share, no opt-out
For What Reasons? (Largest)

- Our Everyday
- Our Marketing
- Joint Marketing
- Affiliates (Trans.)
- Affiliates (Credit.)
- Affiliates' Marketing*
- Nonaffiliates' Marketing

Legend:
- Don't share
- Share, opt-out
- Share, no opt-out
## Comparing Credit Cards

<table>
<thead>
<tr>
<th>Institution</th>
<th>Our everyday</th>
<th>Our marketing</th>
<th>Joint marketing</th>
<th>Affiliates-Trans.</th>
<th>Affiliates-Credit.</th>
<th>Affiliates' Marketing</th>
<th>Non-affiliates' marketing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital One, Chase, Discover, HSBC</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Bank of America, Citi</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Am. Ex.</td>
<td>Red</td>
<td>Yellow</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Barclays</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>GE Capital</td>
<td>Green</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>U.S. Bank</td>
<td>Green</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Wells Fargo</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

- **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

- Social Security number and [income]
- [account balances] and [payment history]
- [credit history] and [credit scores]

• How: 34 options, choose exactly 5

- [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)
Curiosities Encountered

• Self-contradictory statements (15)

<table>
<thead>
<tr>
<th>Does Geneva State Bank share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>We don't share</td>
</tr>
<tr>
<td>Yes</td>
<td>We don't share</td>
</tr>
<tr>
<td>Yes</td>
<td>We don't share</td>
</tr>
</tbody>
</table>
Curiosities Encountered

• Self-contradictory statements (15)

<table>
<thead>
<tr>
<th>Does Geneva State Bank share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>We don't share</td>
</tr>
<tr>
<td>Yes</td>
<td>We don't share</td>
</tr>
<tr>
<td>Yes</td>
<td>We don't share</td>
</tr>
</tbody>
</table>

• 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