Privacy regulation, self-regulation, and enforcement

Lorrie Faith Cranor
September 19, 2013

8-533 / 8-733 / 19-608 / 95-818: Privacy Policy, Law, and Technology
Privacy self-regulation

• Since 1995, the US FTC has pressured companies to “self regulate” in the privacy area

• Self regulation may be completely voluntary or mandatory (or somewhere in between)
Self-regulatory programs and initiatives

- CPOs
- Seals
- Privacy policies
- Standards – P3P and DNT
- Industry guidelines
- Voluntary compliance (safe harbor)
The newest high-level position: Chief privacy officer

Companies are hiring them to ease consumers' concerns in this age of the internet - and to prevent costly suits.

By D. Ian Hopper
ASSOCIATED PRESS

WASHINGTON - Move over, CEO, 

AT&T Appoints Michael Lamb its Chief Privacy Officer

BASKING RIDGE, N.J. -- AT&T today furthered its long tradition of protecting
Chief privacy officers

• Companies are increasingly appointing CPOs to have a central point of contact for privacy concerns

• Role of CPO varies in each company
  – Draft privacy policy
  – Respond to customer concerns
  – Educate employees about company privacy policy
  – Review new products and services for compliance with privacy policy
  – Develop new initiatives to keep company out front on privacy issue
  – Monitor pending privacy legislation
IAPP

• International Association of Privacy Professionals

• http://www.privacyassociation.org/
Seal programs

- TRUSTe – [http://www.truste.org](http://www.truste.org)
Seal program problems

• Certify only compliance with stated policy
  – Limited ability to detect non-compliance

• Minimal privacy requirements

• May not address privacy issues that go beyond the web site

• Nonetheless, reporting requirements are forcing licensees to review their own policies and practices and think carefully before introducing policy changes
Privacy policies

• Inform consumers about privacy practices
• Important part of privacy self regulation
• Consumers can decide whether practices are acceptable, when to opt-out
• Existing privacy policies are not an effective way to inform consumers or give them privacy controls
Amazon.com Privacy Notice

Last updated: October 1, 2008. To see what has changed, click here.

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.

• What Personal Information About Customers Does Amazon.com Gather?
• What Cookies?
• Does Amazon.com Share the Information It Receives?
• How Secure Is Information About Me?
• What About Third-Party Advertisers and Others Who Place Advertisements on Amazon.com?
• Which Information Can I Access?
• What Choices Do I Have?
• Are Children Allowed to Use Amazon.com?
• Does Amazon.com Participate in the Safe Harbor Program?
• Conditions of Use, Notices, and Revisions
• Examples of Information Collected

What Personal Information About Customers Does Amazon.com Gather?

The information we learn from customers helps us personalize and continually improve your shopping experience at Amazon.com. Here are the types of information we gather.

• Information You Give Us: We receive and store any information you enter on our Web site or give us in any other way. Click here to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you.

• Automatic Information: We receive and store certain types of information whenever you interact with our Web sites, such as, for example, many Web sites, we use “cookies,” and we obtain certain types of information when your Web browser accesses Amazon.com or advertisements and other content served by or on behalf of Amazon.com on other Web sites. Click here to see examples of the information we receive.

• E-mail Communications: To help us make e-mails more useful and interesting, we often confirm a subscription when you open e-mail from Amazon.com if your computer

1234567890
What’s wrong with privacy policies?

• Long
• Require college-level reading skills
• Include legalese and obfuscated language
• Difficult to compare
• May change at any time without notice
Typical policies have > 20 hedging claims

- may
- might
- perhaps
- in/at our discretion
- except as
- on a limited basis
- we reserve the right to
- including but not limited to

“Nonetheless, except as separately permitted by other provisions of this Privacy Policy, these companies are allowed to gather, receive, and use your information only for the purposes described in this paragraph or to facilitate compliance with laws.”
Privacy policy components

- Identification of site, scope, contact info
- Types of information collected
  - Including information about cookies
- How information is used
- Conditions under which information might be shared
- Information about opt-in/opt-out
- Information about access
- Information about data retention policies
- Information about seal programs
- Security assurances
- Children’s privacy

There is lots of information to convey -- but policy should be brief and easy-to-read too!
Short Notices

• Project organized by Hunton & Williams law firm around 2002
  – Create short version (short notice) of a privacy notice
  – Sometimes called a “layered notice” as short version would advise people to refer to long notice for more detail
  – Now being called “highlights notice”
  – Focus on reducing privacy policy to at most 7 boxes
  – Standardized format but only limited standardization of language

• Alternative proposals from privacy advocates focus on check boxes

• Interest Internationally
## Acme Company Privacy Notice

### Privacy Notice Highlights

**Personal Information**
- We collect information directly from you and maintain information on your activity with us, including your visits to our website.
- We obtain information, such as your credit report and demographic and lifestyle information, from other information providers.

**Uses**
- We use information about you to manage your account and offer you other products and services we think may interest you.
- We share information about you with our sister companies to offer you products and services.
- We share information about you with other companies, like insurance companies, to offer you a wider array of jointly-offered products and services.
- We share information about you with other companies so they can offer you their products and services.

**Your Choices**
- You may opt out of receiving promotional information from us and our sharing your contact information with other companies. To exercise your choices, call (800) 123-1234 or click on “choice” at ACME.com.

**Important Information**
- You may request information on your billing and payment activities.

**How to Reach Us**
- For more information about our privacy policy, write to:
  - Consumer Department
  - Acme Company
  - 11 Main Street
  - Anywhere, NY 10100
- Or go to the privacy statement on our website at acme.com.
P&G Privacy Notice

Scope
This statement applies to websites operated by or on behalf of The Procter & Gamble Company and its affiliated companies and subsidiaries (P&G).

Personal Information
- We collect information you choose to provide such as your email or postal address.
- We collect non-personal information such as browser type, operating system, and web pages visited to help manage our websites.
- We use cookies and other internet technologies to manage our website and e-mail programs. We do not use these technologies to collect or store personal information.
- We may obtain additional information about you, such as demographic information, from commercially available sources.

Uses
- We use personal information to provide you information and samples you request, to give you a customized interactive experience, and to help us develop new products and services that meet your needs.
- We do not share your personal information with other marketers unless we have asked for and obtained your explicit consent. If you do not provide your consent, we will not share your information.
- We use personal information you provide only for purposes consistent with the reason you provided it.
- When we temporarily provide personal information to companies who perform services for us, such as to send you email or samples, we require those companies to protect the information in the same manner as P&G. These service companies cannot use your personal information for any other purpose than the reason you provided it to P&G.

Your Rights & Choices
- You have the right to have a copy of the personal information you provide, and to correct or update your personal information.
- You may instruct P&G to remove you from our programs you have subscribed to by using the unsubscribe link provided in our email programs, or using the link provided below.
- You may instruct P&G to remove any previous consent you provided to share your personal information with other companies.
- Click here to select your country and be linked to the correct address to use to obtain a copy of the personal information you provided, be removed from our programs, or remove your consent for information sharing.

Important Information
- P&G is committed to working with consumers to obtain a fair resolution of any complaint or concern about privacy.
- P&G complies with country data protection laws.
- We cooperate with country data protection authorities if they believe a privacy problem has occurred.

How to Contact Us
- To contact us with a question click here (for country specific addresses)
- Or write to us at:
  P&G Privacy Team
  2 P&G Plaza
  Cincinnati, OH 45202 U.S.A.
- To read our full Online Privacy Statement click here;
- To read our Global Privacy Policy click here.
Microsoft Online Privacy Notice Highlights

(last updated January 2006)

Scope

This notice provides highlights of the full Microsoft Online Privacy Statement. This notice and the full privacy statement apply to those Microsoft websites and services that display or link to this notice.

Personal Information

- When you register for certain Microsoft services, we will ask you to provide personal information.
- The information we collect may be combined with information obtained from other Microsoft services and other companies.
- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.

Uses of Information

- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
- We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.

Your Choices

- You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
- To make proactive choices about how we communicate with you, follow the instructions listed in the Communication Preferences of the full privacy statement.
- To view and edit your personal information, go to the access section of the full privacy statement.

Important Information

- The full Microsoft Online Privacy Statement contains links to supplementary information about specific Microsoft sites or services.
- The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the Microsoft Passport Network.
- For more information on how to help protect your personal computer, your personal information and your family online, visit our online safety resources.

How to Contact Us

For more information about our privacy practices, go to the full Microsoft Online Privacy Statement. Or write us using our Web form.

Microsoft is a TRUSTe licensee and you may contact TRUSTe if a privacy question is not properly addressed.

Microsoft Privacy Microsoft Corporation
Privacy
IBM Privacy practices on the web

Scope
This statement applies to IBM Web Sites Worldwide.

Personal information
In general, you can visit us on the internet without telling us who you are or giving us personal information. There are times when we may need information from you, for instance: to process an order, to correspond, to provide a subscription or in connection with a job application. We may supplement this information to complete a transaction or to provide a better service.

Uses
• To fulfill your requests by us or by others involved in fulfillment.
• To contact you for customer satisfaction surveys, market research or in connection with certain transactions.
• By IBM and selected organizations for marketing purposes if you have permitted such use.
• In an non-identifiable format for analysis (e.g., Clickstream Data)
• To develop our business relationship if you represent an IBM Business Partner or Vendor

Your choices
• When we collect information from you, you may tell us that you do not want it used for further marketing contact and we will respect your wishes.
• You may also turn off cookies in your browser.

Important information
IBM is a member of TRUSTe (www.truste.org). IBM abides by the EU/US Safe Harbor Framework. To correct inaccuracies in IBM's record of your personal information respond to the sender or contact IBM at access_request@us.ibm.com

For IBM's complete notice see IBM's Privacy policy.
Checkbox proposal

WE SHARE [DO NOT SHARE] PERSONAL INFORMATION WITH OTHER WEBSITES OR COMPANIES.

<table>
<thead>
<tr>
<th>Collection:</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>We collect personal information directly from you</td>
<td>☑️</td>
<td>☐</td>
</tr>
<tr>
<td>We collect information about you from other sources:</td>
<td>☑️</td>
<td>☐</td>
</tr>
<tr>
<td>We use cookies on our website</td>
<td>☑️</td>
<td>☐</td>
</tr>
<tr>
<td>We use web bugs or other invisible collection methods</td>
<td>☐</td>
<td>☑️</td>
</tr>
<tr>
<td>We install monitoring programs on your computer</td>
<td>☐</td>
<td>☑️</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Uses: We use information about you to:</th>
<th>With Your Consent</th>
<th>Without Your Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send you advertising mail</td>
<td>☐</td>
<td>☑️</td>
</tr>
<tr>
<td>Send you electronic mail</td>
<td>☐</td>
<td>☑️</td>
</tr>
<tr>
<td>Call you on the telephone</td>
<td>☑️</td>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sharing: We allow others to use your information to:</th>
<th>With Your Consent</th>
<th>Without Your Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain shared databases about you</td>
<td>☐</td>
<td>☑️</td>
</tr>
<tr>
<td>Send you advertising mail</td>
<td>☑️</td>
<td>☐</td>
</tr>
<tr>
<td>Send you electronic mail</td>
<td>☑️</td>
<td>☐</td>
</tr>
<tr>
<td>Call you on the telephone</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Access: You can see and correct {ALL, SOME, NONE} of the information we have about you.

<table>
<thead>
<tr>
<th>Choices: You can opt-out of receiving from</th>
<th>Us</th>
<th>Affiliates</th>
<th>Third Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertising mail</td>
<td>☑️</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Electronic mail</td>
<td>☐</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Telemarketing</td>
<td>☑️</td>
<td>☑️</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Retention: We keep your personal data for: {Six Months, Three Years, Forever}

Change: We can change our data use policy {AT ANY TIME, WITH NOTICE TO YOU, ONLY FOR DATA COLLECTED IN THE FUTURE}

Source: Robert Gellman, July 3, 2003
Privacy policy format study

- Reading-comprehension and opinion questions for 4 policy formats
- People could accurately answer when they could find answer by scanning
  - Does Acme use cookies? (98%)
- People had trouble with questions that required more reading comprehension
  - Does this policy allow Acme to put you on an email marketing list? (71%)
  - Does this policy allow Acme to share your email address with a marketing company that might put you on their email marketing list? (52%)
- Even well-written policies are not well-liked and difficult to use

Industry privacy guidelines

- Direct Marketing Association Privacy Promise
  http://www.dmaconsumers.org/privacy.html

- Network Advertising Initiative Principles
  http://www.networkadvertising.org/

- DAA Self-Regulatory Principles
  http://www.aboutads.info/principles

- CTIA Location-based privacy guidelines

- GSMA Mobile Privacy Principles
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
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:
- Social Security number and income
- Account balances and account transactions
- Credit scores and payment history

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.

# Facts

<table>
<thead>
<tr>
<th>Reasons we can share your personal information</th>
<th>Does PNC share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus</td>
<td>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>No</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>Yes</td>
<td>Yes</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>

To limit our sharing
- Call 1-800-762-2118 — our menu will prompt you through your choice(s)
- Visit us online: www.PNC.com/privacy (Online Banking customers only.)

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 1-800-762-2118
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
Data collection and extraction

- FDIC directory of 7,072 institutions
- Download top 10 results for Google query: "What does [name of financial institution] do with your personal information?"
- 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

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

Legend:
- Green: Don't share
- Yellow: Share, opt-out
- Red: Share, no opt-out
100 largest banks

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

Legend:
- Green: Don't share
- Yellow: Share, opt-out
- Red: 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>Red</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>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Am. Ex.</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Barclays</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>GE Capital</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>U.S. Bank</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Red</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>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

- **Red**: Share, no opt-out
- **Yellow**: Share, opt-out
- **Green**: Don't share
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
Dress, Casual & Athletic Shoes | Zappos.com
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
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
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
Sells mens' and womens' shoes, sandals, boots, and sneakers.
http://www.shoebuy.com/ - Cached - Privacy Policy - Similar Pages

Footwear Shopping in the Yahoo! Directory
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... - Cached - Privacy Policy - Similar Pages

Shoes.com - Women's, Men's, and Children's Shoes
What Info is Collected, and How

• What: 24 options, SSN + choose exactly 5

<table>
<thead>
<tr>
<th>What?</th>
<th>The types of personal information we collect and share depend on the product or service you have with us. This information can include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Social Security number and [income]</td>
</tr>
<tr>
<td></td>
<td>[account balances] and [payment history]</td>
</tr>
<tr>
<td></td>
<td>[credit history] and [credit scores]</td>
</tr>
</tbody>
</table>

• How: 34 options, choose exactly 5

<table>
<thead>
<tr>
<th>How does [name of financial institution] collect my personal information?</th>
<th>We collect your personal information, for example, when you</th>
</tr>
</thead>
<tbody>
<tr>
<td>[open an account] or [deposit money]</td>
<td>[pay your bills] or [apply for a loan]</td>
</tr>
<tr>
<td>[use your credit or debit card]</td>
<td></td>
</tr>
</tbody>
</table>

• 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
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