NC STATE UNIVERSITY

CSC 495.002 – Lecture 12
Usable Privacy: Privacy Policies and Notices

Dr. Özgür Kafalı

North Carolina State University
Department of Computer Science

Fall 2017

NC STATE UNIVERSITY

PREVIOUSLY ON USABLE PRIVACY

Decision Making and Warnings

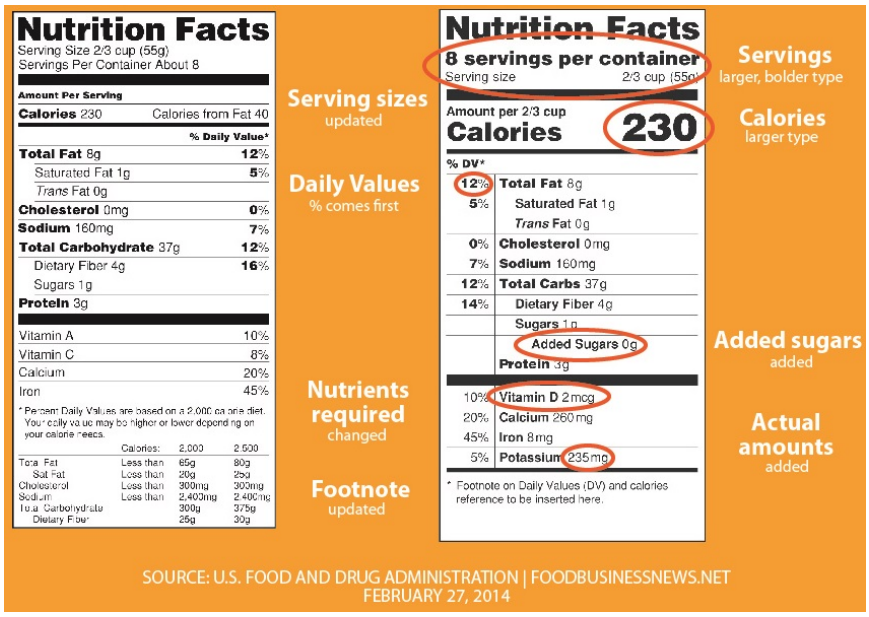
- Human decision making
- Bounded rationality
- Privacy engineering: Warnings and nudges

Problem Definition

- What is the problem with privacy policies? Nobody reads them
- What if we actually read them? What would be the cost?
- If every Internet user read privacy policies for each site they visited, it would cost $781 billion per year
- Problem: How can we make privacy policies easier to understand?

McDonald and Cranor. The cost of reading privacy policies. Technology Policy Research Conference, 2008

Potential Solution

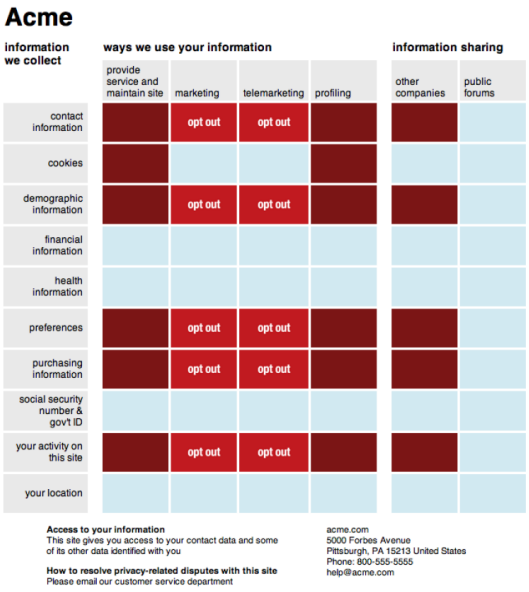


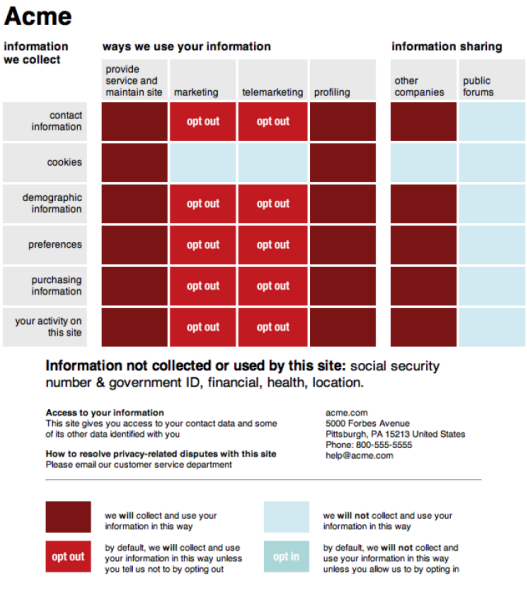
Standardizing Privacy Notices

- Research question: Do standardized policy presentations have positive effects on accuracy and speed of information finding?
- Compare five policy formats
- Traditional:
  - Full text policy
  - Layered (high level summary)
- Standardized:
  - Standardized table
  - Standardized short table
  - Standardized short text

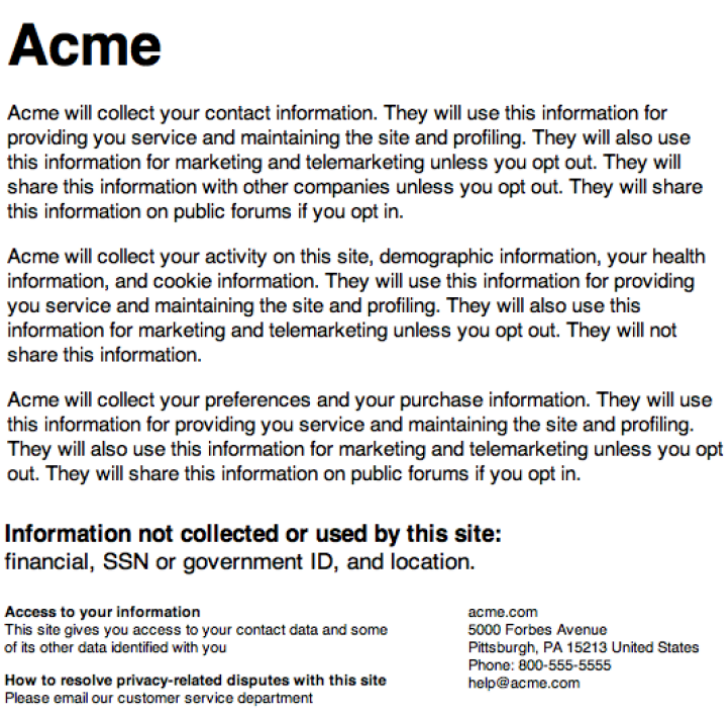
Kelley et al. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. Conference on Human Factors in Computing Systems, pages 1573–1582, 2010

Standardized Tables





Standardized Text



Acme

Acme will collect your contact information. They will use this information for providing you service and maintaining the site and profiling. They will also use this information for marketing and telemarketing unless you opt out. They will share this information with other companies unless you opt out. They will share this information on public forums if you opt in.

Acme will collect your activity on this site, demographic information, your health information, and cookie information. They will use this information for providing you service and maintaining the site and profiling. They will also use this information for marketing and telemarketing unless you opt out. They will not share this information.

Acme will collect your preferences and your purchase information. They will use this information for providing you service and maintaining the site and profiling. They will also use this information for marketing and telemarketing unless you opt out. They will share this information on public forums if you opt in.

Information not collected or used by this site:
financial, SSN or government ID, and 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

Methodology

- Deploy survey on Amazon Mechanical Turk
- Use privacy policies from
  - Microsoft
  - IBM
  - Target
  - Disney
- Anonymized company names
- A series of tasks
  - Simple: Can be answered by looking at a single row or column
  - Complex: Requires some interaction between data use and sharing
  - Comparison: Compare two policies

Word Counts

	Pol. 1	Pol 2.	Pol 3.	Pol 4.
Full Policy Text	2127	6257	4399	2912
Std. Short Text	175	127	108	90
Layered Text			409	800

Survey Tasks & Results

		#	Question	Answer	Std. Table	Std. Short Table	Std. Short Text	Full Policy Text	Layered Text
Simple Tasks	*Group A*	1	Does the policy allow Acme to collect information about	Yes	82.35	86.25	91.57	80.23	
	Group B		which pages you visited on this web site?	Yes	87.21	85.06	89.53	92.11	84.62
	Group A	2	Acme might want to use your information to improve their website.	Yes	79.41	77.50	83.13	82.56	
	Group B		Does this policy allow them to use your information to do so?	Yes	76.74	77.01	86.05	**89.47**	64.10
	Group A	3	Does the policy allow Acme to collect information	No	48.04	**23.75**	43.37	**18.60**	
	Group B		about your current location?	No	46.51	**24.14**	53.49	**3.95**	**15.38**
	Group A	4	Based on the policy will Acme register their secure certicate	The policy does not say	88.23	81.25	84.34	**52.33**	
	Group B		with VeriSign or some other company?	The policy does not say	79.07	82.76	87.21	**43.42**	**30.77**
	Group A	5	Based on the policy may Acme store cookies	Yes	89.22	92.50	**73.49**	91.86	
	Group B		on your computer?	Yes	89.53	80.46	87.21	96.05	88.46
	Group A	6	Does the policy allow Acme to collect information about your medical	Yes	84.31	76.25	**69.88**	**48.84**	
	Group B		conditions, drug prescriptions, or family health history?	No	73.25	**58.62**	81.40	**28.95**	**33.33**
Complex Tasks	*Group A*	7	Does the policy allow Acme to share some of your	Only if I allow them to	75.50	76.25	**59.04**	**15.12**	
	Group B		information on public bulletin boards?	No	61.63	57.47	65.12	**25.00**	**38.46**
	Group A	8	Does the policy allow Acme to share your home phone	Yes, unless I tell them not to	62.75	68.75	67.47	**36.05**	
	Group B		number with other companies?	Yes	68.60	60.92	**20.43**	**14.47**	**14.10**
	Group A	9	Does the policy allow Acme to use your buying history	Yes	53.92	58.75	53.01	62.79	
	Group B		to design custom functionality targeted at you?	Yes	50.00	58.62	**69.77**	64.47	**65.38**
	Group A	10	Does the policy allow Acme to share your cookie	No	69.61	67.50	**50.60**	**16.28**	
	Group B		information with other companies?	No	79.07	71.26	74.42	**26.32**	**44.87**
	Group A	11	Will Acme contact you with advertisements?	Yes, unless I tell them not to	54.90	61.25	55.42	**38.37**	
	Group B			Yes, unless I tell them not to	44.19	49.43	51.16	**14.47**	39.74
	Group A	12	Does Acme give you control regarding their sharing of	Yes	70.59	68.75	73.49	66.28	
	Group B		your personal data?	No	56.98	44.83	**37.21**	**31.58**	**24.36**
Comparison Tasks	*Group A*	14	Does either company give you options with	Only with Acme	58.82	52.50	45.78	**33.72**	
	Group B		regards to cookies?	Only with Bell	63.95	**48.28**	**19.76**	**15.79**	**42.31**
	Group A	15	Does either company collect sensitive information	Acme	64.71	**47.50**	53.01	**20.93**	
	Group B		(such as banking or medical records)?	Neither company	73.26	63.22	80.23	**52.63**	**53.85**
	Group A	16	By default, Acme can collect information about your age and gender	True	59.80	61.25	**34.94**	**19.77**	
	Group B		in order to market to you by email, but the Bell Group cannot.	False, both can	56.98	**74.71**	**77.91**	46.05	**24.36**

Effective Privacy Notices

A Design Space for Effective Privacy Notices

Florian Schaub,[1] Rebecca Balebako,[2]* Adam L. Durity,[3]* Lorrie Faith Cranor[1]

[1]Carnegie Mellon University
Pittsburgh, PA, USA
{fschaub, lorrie}@cmu.edu

[2]RAND Corporation
Pittsburgh, PA, USA
balebako@rand.org

[3]Google
Mountain View, CA, USA
adurity@google.com

ABSTRACT

Notifying users about a system's data practices is supposed to enable users to make informed privacy decisions. Yet, current notice and choice mechanisms, such as privacy policies, are often ineffective because they are neither usable nor useful, and are therefore ignored by users. Constrained interfaces on mobile devices, wearables, and smart home devices connected in an Internet of Things exacerbate the issue. Much research has studied usability issues of privacy notices and many proposals for more usable privacy notices exist. Yet, there is little guidance for designers and developers on the design aspects that can impact the effectiveness of privacy notices. In this paper, we make multiple contributions to remedy this issue. We survey the existing literature on privacy notices and identify challenges, requirements, and best practices for privacy notice design. Further, we map out the design space for privacy notices by identifying relevant dimensions. This provides a taxonomy and consistent terminology of notice approaches to foster understanding and reasoning about notice options available in the context of specific systems. Our systemization of knowledge and the developed design space can help designers, developers, and researchers identify notice and choice requirements and develop a comprehensive notice concept for their system that addresses the needs of different audiences and considers the system's limitations and opportunities for providing notice.

website, or linked to from mobile app stores or mobile apps, to signs posted in public places to inform about CCTV cameras in operation. Even an LED indicating that a camera or microphone is active and recording constitutes a privacy notice, albeit one with limited information about the data practices associated with the recording. Providing notice about data practices is an essential aspect of data protection frameworks and regulation around the world [57]. While transparency has been emphasized as an important practice for decades, existing privacy notices often fail to help users make informed choices. They can be lengthy or overly complex, discouraging users from reading them.

Smartphones and mobile apps introduce additional privacy issues as they support recording of sensor and behavioral information that enables inference of behavior patterns and profiling of users. Yet, comparatively smaller screens and other device restrictions constrain how users can be given notice about and control over data practices.

The increasing adoption of wearable devices, such as smart watches or fitness trackers, as well as smart home devices, such as smart thermostats, connected light bulbs, or smart meters, represents a trend towards smaller devices that are even more constrained in terms of interaction capabilities, but are also highly connected with each other and the cloud. While providing notice and choice is still considered essential in the "Internet of Things" (IoT) [48, 74], finding appropriate and usable notice and choice mechanisms can be challenging.

Schaub et al. A Design Space for Effective Privacy Notices. Symposium On Usable Privacy and Security (SOUPS), 2015

Motivation

- Purpose: Make users aware of data practices involving personal information
- Privacy notice: Public announcement of data practices regarding
  - Collection
  - Usage
  - Sharing
- Different forms
  - Privacy policy posted on a website
  - Signs posted in public places (CCTV cameras)
  - LED indicating that a camera or microphone is recording
  - Shutter sound

Goal

- Embed privacy notices and choice options into system design
- With minimal disruption to regular flow
- Provide transparency for users

Exercise: Roles of Privacy Notices

- For companies:
  - Demonstrate legal compliance
  - Build customer trust
- For regulators:
  - Investigate and enforce regulatory compliance
  - Treat violation as unfair or deceptive trade practice

Challenges

- Notice complexity: 244 hours annually to read all policies for websites visited
- Lack of choices: Informative, but not actionable
  "Warning: CCTV in use"
- Notice fatigue: Often shown at inopportune times, conflict with user's main task
- Decoupled notices: For example, a fitness tracking device

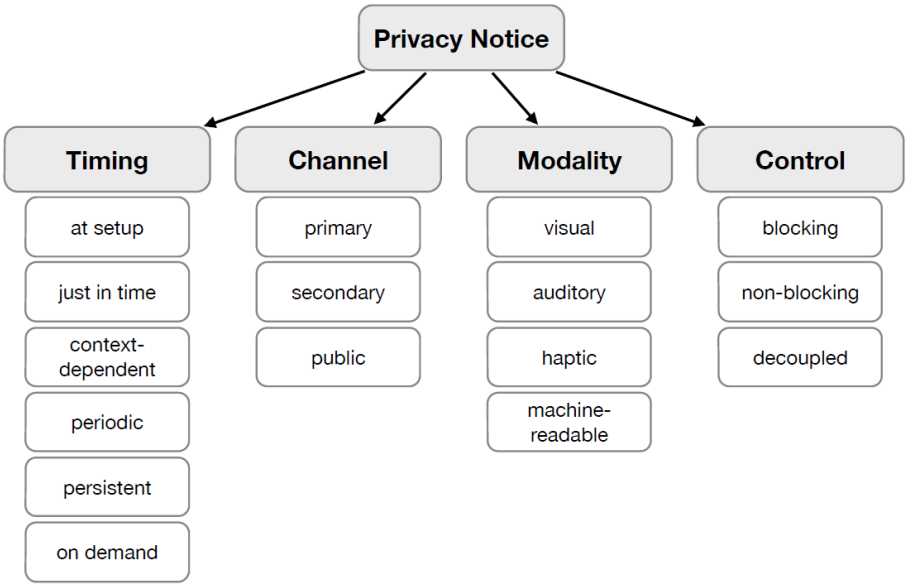
Audiences

- Which data practices affect which audience
- Let's think about Google Glass
- Primary user: Person who wears it
- Secondary users: Friends, family members
- Incidental users: Bystanders

Layered and Contextualized Notices

- Multi-layered policies
- Notices shown at different times
- With respect to the context and user's expectations

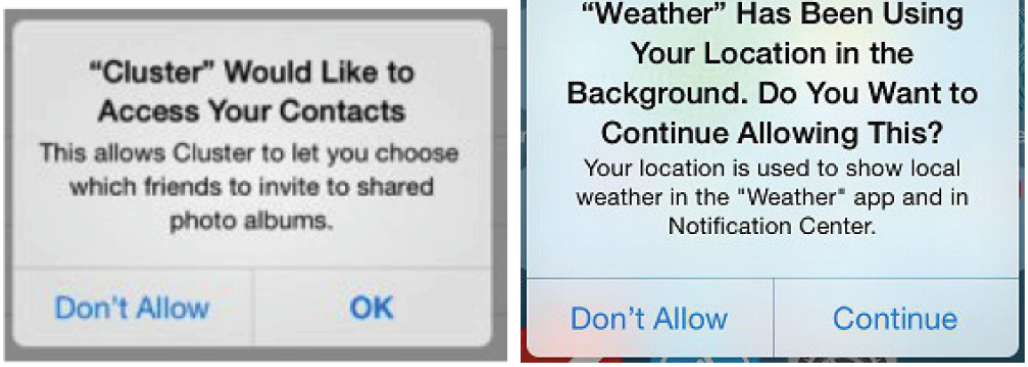
Design Space



Timing

- At setup: When used for the first time (part of installation)
- Just in time: When a data practice is active
- Context-dependent: Nudges to prevent oversharing
- Periodic: Frequency determined based on sensitivity of data
- Persistent: Unobtrusive visual notice
- On demand: User can request

Just in Time and Periodic: iOS



Context-dependent: Facebook Privacy Checkup

Channel

- Primary: Provided on the same platform or device
- Secondary: Limited primary channels, e.g., wearables, smart home devices
- Public: For incidental users, e.g., signs for video surveillance

Modality

- Complement user's activity: For example, use audio while driving
- Visual: Text, images, icons
- Auditory: Spoken words or sounds
- Haptic: Combine sound and vibration to notify about data sharing

Control

- Opt-in: User must explicitly agree to a data practice
- Opt-out: User may request to stop a specific practice
- Blocking: Requires user to make a choice
- Non-blocking: Without forcing user interaction, e.g., use same settings as previous post
- Decoupled: Privacy dashboards to control privacy settings across multiple services

Websites and Social Media

- Provide notices on demand (Timing)
- Post privacy policy on the website or app (Channel)
- Largely visual, specifically text (Modality)
- Controls are decoupled from the notice (Control)

Exercise: Smartphone Permissions

- When asks for permissions during installation: At setup
- When user sees the list of permissions: Blocking
- When an app update changes requested permissions: Periodic

Evaluation of Standardized Privacy Notices

A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices

LORRIE FAITH CRANOR, PEDRO GIOVANNI LEON, and BLASE UR,
Carnegie Mellon University

Financial institutions in the United States are required by the Gramm-Leach-Bliley Act to provide annual privacy notices. In 2009, eight federal agencies jointly released a model privacy form for these disclosures. While the use of this model privacy form is not required, it has been widely adopted. We automatically evaluated 6,191 U.S. financial institutions' privacy notices posted on the World Wide Web. We found large variance in stated practices, even among institutions of the same type. While thousands of financial institutions share personal information without providing the opportunity for consumers to opt out, some institutions' practices are more privacy protective. Regression analyses show that large institutions and those headquartered in the northeastern region share consumers' personal information at higher rates than all other institutions. Furthermore, our analysis helped us uncover institutions that do not let consumers limit data sharing when legally required to do so, as well as institutions making self-contradictory statements. We discuss implications for privacy in the financial industry, issues with the design and use of the model privacy form on the World Wide Web, and future directions for standardized privacy notice.

Cranor et al. A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices. ACM Transactions on the Web, 10(3):17:1–17:33, 2016

Limitations of Usability of Privacy Policies

- Studies show that consumers will pay a premium price to make purchases from more privacy-protective businesses
- However, numerous issues negatively impact usability of privacy policies
- Generally requires two years of college education to comprehend
- Typically unavailable in a user's language (unlike the website itself)
- Require hundreds of hours a year to read them all

Goal

- Difficult to compare privacy policies
  - Even among financial institutions with identical practices
  - Even for regulators, e.g., Federal Trade Commission, National Credit Union Administration
- Standardize the way financial institutions provide privacy disclosures
- Develop a “Model Privacy Form”

Model Privacy Form: Facts

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		

Model Privacy Form: Details

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.]

Opt-out Form

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	
Address	
City, State, Zip	
[Account #]	

Mail to:
[Name of Financial Institution]
[Address1]
[Address2]
[City], [ST] [ZIP]

Methodology

- Obtain list of financial institutions
- Determine institution's web domain
- Retrieve standardized policies
- Parse standardized policies
- Analysis

Sharing Practices

Practice	Number of Institutions	Percentage of Total
Affiliates		
Shares with affiliates	1,726	28%
Does not share	1,543	25%
No affiliates	2,632	43%
Blank	237	4%
Nonaffiliates		
Shares with nonaffiliates	730	12%
Does not share	4,038	66%
No nonaffiliates	1,085	18%
Blank	285	5%
Joint Marketing		
Jointly markets	2,575	42%
Does not jointly market	3,356	55%
Blank	207	3%

Sharing Purposes

Reason for Sharing Personal Information	Does Not Share		Offers Opt-Out		No Opt-Out		(Missing)	
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	45	0.7%	9	0.1%	6,016	97.2%	108	1.7%
For our marketing purposes– to offer our products and services to you	1,808	29.2%	410	6.6%	3,832	61.9%	127	2.1%
For joint marketing with other financial companies	3,434	55.5%	563	9.1%	2,044	33.0%	124	2.0%
For our affiliates' everyday business purposes– information about your transactions and experiences	4,492	72.6%	158	2.6%	1,331	21.5%	189	3.1%
For our affiliates' everyday business purposes– information about your creditworthiness *[Opt-out mandatory when sharing]*	5,317	85.9%	572	9.2%	80	1.3%	189	3.1%
For our affiliates to market to you *[Opt-out mandatory when sharing; row may be omitted in certain cases]*	1,682	27.2%	715	11.5%	21	0.3%	3,754	60.6%
For nonaffiliates to market to you *[Opt-out mandatory when sharing]*	5,459	88.2%	455	7.3%	31	0.5%	204	3.3%

Opt-out Mechanisms

Opt-Out Mechanism(s)	# Institutions Providing This Mechanism	% Of the Total # of Institutions Offering Opt-Outs
Only phone	391	30.8%
Phone and website	265	20.9%
Only postal mail	217	17.1%
Phone and postal mail	153	12.0%
Three or more mechanisms	152	12.0%
Phone and email	46	3.6%
Postal mail and website	25	2.0%
Only website	17	1.3%
Only email	2	0.2%
Postal mail and email	1	0.1%
Website and email	1	0.1%

Contradictions

Reasons we can share your personal information	Does Bendena State Bank/Bank of Highland 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	We don't share

Bank Privacy Interface