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

Lorrie Faith Cranor, Pedro Giovanni Leon, Blase Ur

{lorrie, pedrogln, bur}@cmu.edu

Carnegie Mellon University, Pittsburgh, PA

ABSTRACT

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. 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, and future directions for standardized privacy notice.

1 Introduction

When the United States Congress was considering the Gramm-Leach-Bliley Act of 1999 (GLBA), allowing the consolidation of different types of financial institutions, privacy advocates argued that it was important to notify consumers about these institutions' data practices and allow consumers to limit the use and sharing of their data [19]. The act passed with a provision mandating annual privacy notices. In the years that followed, these disclosures were widely criticized for being difficult to read and understand [35]. In response, eight federal agencies jointly released a *model privacy form* in 2009 [38]. This model privacy form, which combined boilerplate text with sections for institutions to fill in regarding their own practices, was designed to "make disclosure of institutions' information sharing practices and consumer choices more transparent" in an easy-to-read format [38].

Besides making it easier for consumers to find privacy information, privacy notices that provided in a standardized format also enable automated, large-scale comparisons of privacy practices. The idea of providing privacy notices in standardized formats has long held great potential for empowering consumers to compare companies' privacy practices. From standards for machine-readable privacy policies, such as the Platform for Privacy Preferences (P3P) [4], to recent attempts to have humans annotate websites' privacy policies and terms of service [46], much time and energy has gone into attempts to provide privacy information in a standardized format. Unfortunately, these initiatives generally do not reach fruition. For instance, websites have been found to misuse machine-readable privacy disclosures [27], while attempts to have humans annotate privacy practices do not scale well.

Although financial institutions in the United States are not required to use the model privacy form to enumerate their privacy practices, the use of this form provides a safe harbor for privacy disclosures under GLBA [38]. As a result, financial institutions have incentives to use this model privacy form to make their mandatory privacy disclosures. Throughout this paper, we refer to an institution's privacy disclosure using the model privacy form as a

standardized notice. We found thousands of financial institutions providing a standardized notice, giving us the opportunity to analyze privacy practices across an entire industry.

We collected lists of financial institutions in the United States and wrote a computer program that automatically queries Google in search of these companies' standardized notices. Upon finding such a notice, the program automatically parses the standardized notice and feeds the extracted information into a database, enabling a large-scale comparison of financial institutions' privacy practices. Starting from lists of financial institutions from the Federal Reserve (FED), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA), we searched for standardized notices from 19,329 financial institutions, finding standardized notices from 6,191 of these institutions.

We then compared these 6,191 institutions in terms of their data-sharing practices, consumers' ability to opt out of data sharing, and the personal information the policies state may be collected. To investigate how different factors affect institutions' sharing practices, we further conducted statistical analyses using additional information included in the FDIC list regarding various institutions' characteristics. For additional insight into how competitors compare, we also analyzed the policies of institutions on a Forbes list of the 100 largest banks [3] and a J.D. Power survey of credit card satisfaction [21].

We found wide variance in financial institutions' privacy practices. Most importantly, even institutions of the same characteristics sometimes differed in their privacy practices, suggesting that consumers might have the opportunity to pick a financial institution with more consumer-friendly privacy practices if information to help them find these institutions were more readily available. To that end, we built an interactive website[1] for consumers to compare these institutions' privacy practices based on the information we extracted from the standardized notices.

Furthermore, we found that both large institutions and those headquartered in the Northeastern region of the United States are more likely to share consumers' personal information

[1]Available at `http://cups.cs.cmu.edu/bankprivacy/`

for marketing purposes than all other institutions. Finally, we found deficiencies in both the specification and the use of the model privacy form that may counterintuitively limit consumers' access to information about financial institutions' privacy practices.

In Section 2, we summarize the relevant provisions of GLBA and prior work on standardized privacy notices. In Section 3, we describe the data set we collected and explain our methodology. We present our results in Section 4, and we discuss in Section 5 our findings and their implications for financial institutions' privacy practices and standardized privacy notices. We include an appendix with detailed results.

2 Background and related work

In this section, we describe privacy provisions of GLBA, some criticisms of those provisions, and the regulatory development of an optional standardized format for financial institutions' privacy disclosures. We also discuss relevant state laws. Finally, we highlight efforts to improve privacy notices beyond the financial industry, including the creation of formal specifications, standardized formats, and usable privacy notices.

2.1 Financial Federal Laws' Privacy Provisions

In this paper we examine financial institutions' annual privacy disclosures that are mandated by GLBA, which was signed into law on November 12, 1999 [18]. GLBA's primary purpose was to encourage competition in the financial services industry by removing barriers that prevented common ownership (affiliation) between commercial banks, investment banks, and insurance businesses [29, 42, 49].

Affiliation between different types of financial services companies presented an opportunity for newly affiliated companies to share information. In response to concerns about the privacy of consumer information, Congress included Title V, known as the Privacy Rule, in GLBA. This rule requires financial institutions to provide annual notices of their privacy

policies and practices (15 U.S.C. §§ 6802–6803). The rule also mandates that customers have the right to opt out of data sharing with nonaffiliated companies. However, the Privacy Rule provides a "joint marketing exception" to the opt-out requirements, allowing nonaffiliated financial companies to share information without offering an opt-out when there exists a formal agreement for marketing financial products or services to a consumer [14].

Although GLBA's Privacy Rule does not give consumers a general right to opt out of all data sharing, the Fair Credit Reporting Act (FCRA) does give consumers that right for certain types of credit information. The FCRA, which regulates the use and distribution of consumer information, exempts from its definition of a consumer report any communication between affiliates. However, this exemption only applies if the communication is "clearly and conspicuously disclosed to the consumer . . . and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons" (15 U.S.C. § 1681a(d)(2)(A)(iii)). In other words, consumers must be able to opt out of data sharing about their creditworthiness between affiliates.

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) [8] amended the FCRA to further restrict the use of information shared between affiliates. The rule, called the "Affiliate Marketing Rule," prohibits companies that receive information that would be considered a consumer report if not for § 1681a(d)(2)(A)(iii) from using that information for marketing unless the consumer is given notice and the opportunity to opt out (15 U.S.C. § 1681s-3(a)).

The provisions of GLBA, the FCRA, and FACTA combine to establish three contexts in which financial institutions must provide notice and the opportunity to opt out. GLBA's Financial Privacy Rule applies to the sharing of consumer financial information with non-affiliates, the FCRA restricts sharing consumer report information between affiliated companies, and FACTA limits when consumer report information shared between affiliates may be used for marketing [32].

2.2 Criticisms of GLBA's privacy provisions

The privacy protections offered by GLBA have prompted a range of criticisms. Some critics feel that GLBA offers incomplete or too few privacy protections. For instance, in an examination of GLBA privacy provisions, Janger et al. conclude that GLBA "leaves the burden of bargaining on the less informed party, the individual consumer" [20]. Schiller also argues that the notice provisions provided by GLBA do not go far enough toward providing privacy protections [40]. She recommends that GLBA further restrict information sharing among affiliates. Freeman similarly concludes that GLBA was a good start, yet "need[s] further refinement" [13], arguing that the "opt-out" provision has made it unlikely that many customers will take the active steps needed to protect their confidential data" [13]. Nojeim also argues that GLBA is incomplete because it does not prevent the flow of personal information among affiliates and uses an opt-out approach, failing to require consumers' active consent [37].

Other critics feel that the protections offered by GLBA are an impediment to the free market. Some economists have claimed that "efforts to protect privacy in the financial services industry (and elsewhere) are obstacles to the functioning of optimally efficient markets" [44]. Lacker, for example, argues that in a perfectly competitive market, financial privacy would be determined by economic forces regardless of the choice mechanisms offered [26]. Furletti and Smith claim that the open sharing of consumer information makes the market more efficient and benefits both financial institutions and consumers. They further claim that laws like the Fair Credit Reporting Act provide sufficient privacy protections for consumers [15]. In counterpoint, Swire argues that inappropriate disclosure of personal information can easily lead to a "misallocation of resources" [44].

Investigations conducted around the time GLBA came into effect studied the act's initial impact on financial institutions' privacy disclosures. Sheng et al. performed a longitudinal study of fifty financial institutions' privacy policies. They found that although privacy poli-

cies became more complete and contained more detailed information about sharing practices after GLBA, the amount of sharing among affiliates and nonaffiliates increased [41]. Antón et al. examined privacy statements from nine financial institutions covered by GLBA and concluded that these statements did not comply with the GLBA requirements of conspicuousness and clarity. They suggested the use of a standardized vocabulary to improve the readability of financial institutions' privacy policies [2].

2.3 Development of the model privacy form

A few years after GLBA was enacted, eight U.S. regulators[2] jointly noted wide variations in the privacy notices financial institutions were sending to consumers. They found these notices "difficult to compare, even among financial institutions with identical practices" and questioned "whether such notices comply with the requirement that they be clear and conspicuous." As a result, regulators started a process to create a standard model for privacy notices that "consumers could more easily use and understand" [38]. Financial institutions, researchers, and communications firms took part in this process.

The process of developing a standardized notice began in the summer of 2004. The regulators retained a communications firm, Kleimann Communication Group, to develop a prototype of a standardized notice. To this end, the firm conducted two ten-participant focus groups and 46 individual interviews, releasing a report of their findings in February 2006 [24]. Notably, the main goal of the prototype notice was to help consumers understand financial institutions' sharing practices, not necessarily to provide a comprehensive list of the types of personal information that financial institutions collect. In March 2007, the regulators issued the prototype for public comment [38].

Following public comments on the proposed model form, the regulators commissioned a

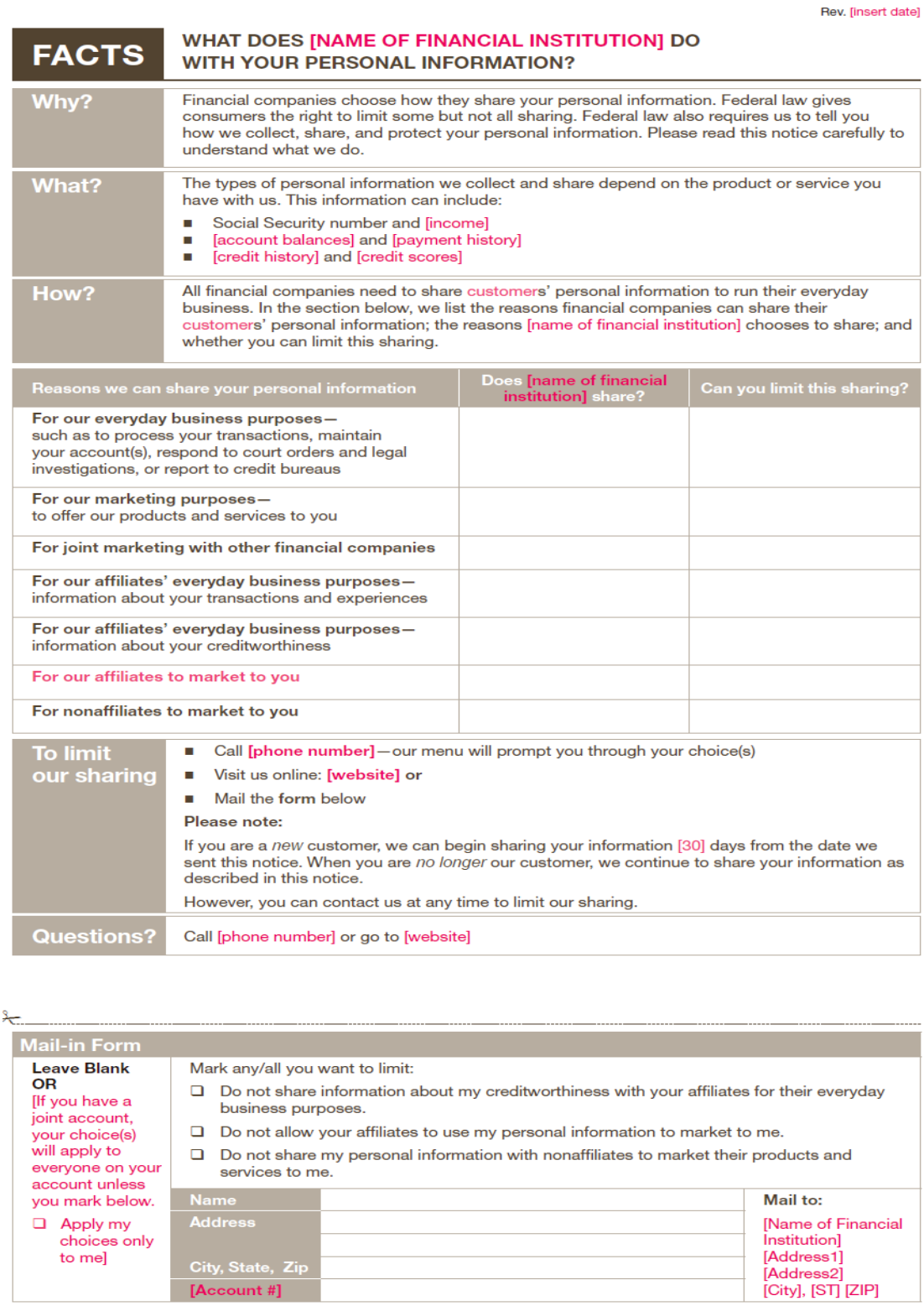
[2]The Office of the Comptroller of the Currency; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; the National Credit Union Administration; the Federal Trade Commission; the Securities and Exchange Commission; the Office of Thrift Supervision; and the Commodity Futures Trading Commission

quantitative survey designed to evaluate the effectiveness of the revised model form. The survey, which was conducted in the spring of 2008, tested comprehension and usability of the model form as compared with three other styles of notice. Notices from three fictitious banks with different sharing practices were tested among 1,032 consumers recruited from five US cities. The prototype outperformed the alternative styles tested [30].

In December 2008, Levy and Hastak submitted a report to the regulators analyzing the results of the usability testing [28]. Although participants who tested the proposed prototype better understood the differences in sharing practices, Levy and Hastak found that participants experienced problems understanding how to exercise their opt-out rights. The report proposed improvements to reduce the length of the disclosure table and to increase the clarity of opt-out choices. The regulators revised the model form again based on both the Levy-Hastak report and public comments received after publishing the survey results.

The regulators again commissioned Kleimann Communication Group to conduct validation testing. The firm conducted a seven-participant study and concluded in its February 2009 report that the improvements suggested by Levy and Hastak improved the clarity of opt-out choices without affecting understanding of sharing practices [25]. Garrison et al. give a more detailed account of the user testing behind the model forms [16].

In December 2009, the regulators released the final model privacy form, shown in Figure 1 and Figure 2. Although use of the model privacy form is voluntary, financial institutions may rely on this model privacy form as a safe harbor to provide privacy disclosures [38], potentially spurring its adoption. Notably, this model privacy form is the basis of one of the first widespread uses of a standardized format for privacy disclosures, facilitating our large-scale analysis.



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

Address

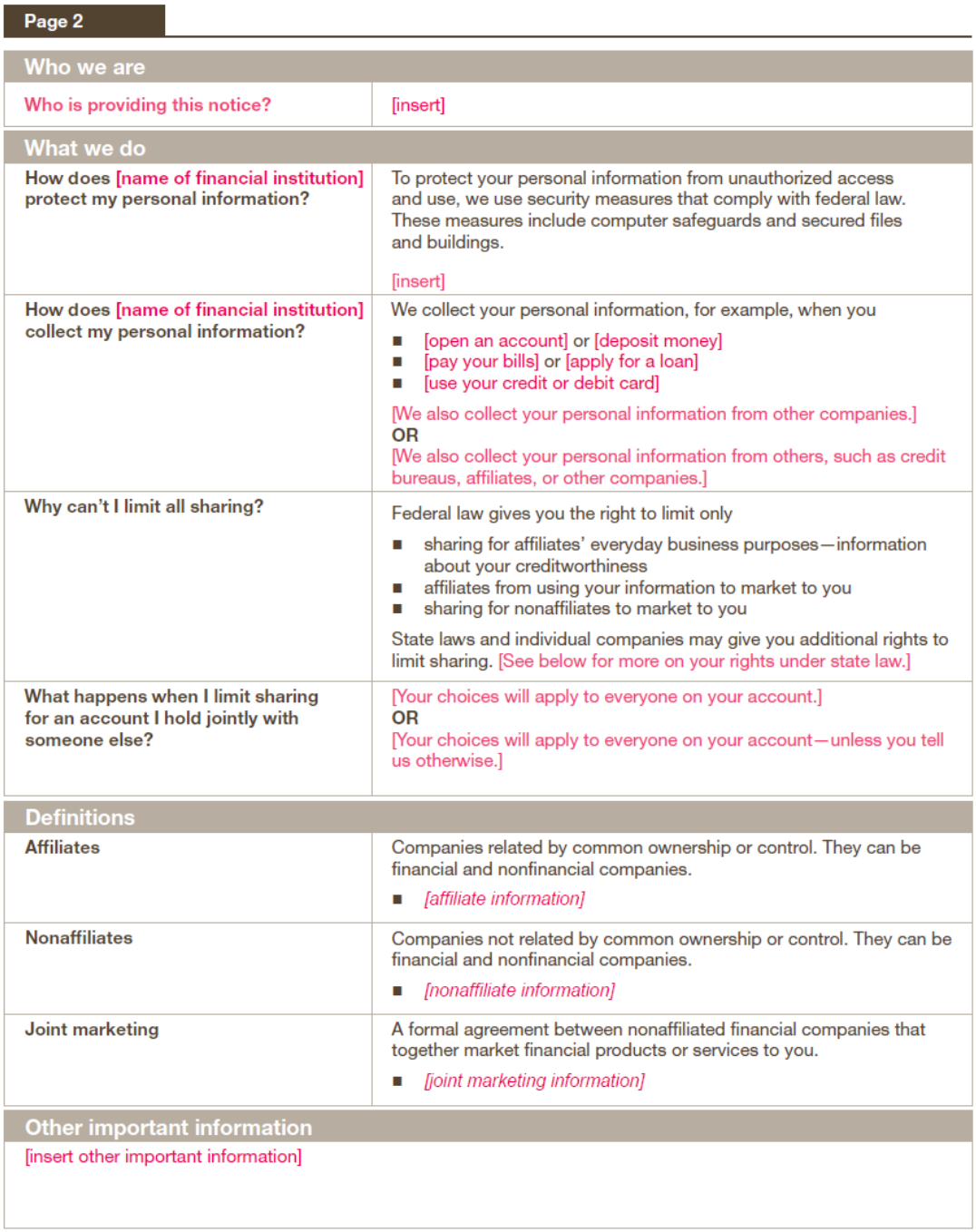
City, State, Zip

[Account #]

Mail to:

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

Figure 1: The first page of the model privacy form [38]. We extracted and analyzed what information is collected, how information is shared, including whether consumers can limit any type of sharing, and how consumers may limit sharing. The sharing table and text in pink need to be filled in by the financial institution.



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]

Figure 2: The second page of the model privacy form [38]. From this page, we extracted and analyzed how information is collected, as well as the list of affiliates, nonaffiliates, and joint marketing partners.

2.4 State laws

U.S. states have enacted a number of laws limiting financial institutions' ability to share financial data. GLBA includes a provision providing that it does not preempt state laws that are consistent with it. State laws that are inconsistent are invalid only to the extent of the inconsistency (15 U.S.C. § 6807) [34, 36]. A state law with stronger consumer protections is explicitly not inconsistent (and, thus, not preempted). Many states have laws that prohibit financial institutions from disclosing customer information unless that disclosure is authorized or required by law or court order (see Proskauer § 5:6.2 [31] for examples).

California's Financial Information Privacy Act (Cal. Fin. Code §§ 4050–60) is a notable example of a state law enacted in the wake of GLBA. It was enacted in 2004 with the intent to "afford persons greater privacy protections than those provided in ... the federal Gramm-Leach-Bliley Act" (*Id.* §4051(b)). CalFIPA requires consumers to opt in before a financial institution may share "nonpublic personal information" with a nonaffiliated third party. It allows nonpublic personal information to be shared between most types of affiliates only after notice and the opportunity to opt out.

Although GLBA seems to explicitly allow state laws with stronger provisions, the affiliate-sharing rule has been held invalid due to preemption by the FCRA. In *American Banker's Association v. Lockyer*, 541 F.3d 1214 (9th Cir. 2008), the Ninth Circuit Court of Appeals held that CalFIPA was preempted by the FCRA with regard to the opt-out requirement for the sharing of consumer report information between affiliates. Although GLBA allows state laws with stronger protections for consumers than are provided under GLBA, it does not "modify, limit, or supersede" the FCRA (15 U.S.C. § 6806). The FCRA preempts any state laws that contain provisions "with respect to the exchange of information among persons affiliated by common ownership or common corporate control" (15 U.S.C. § 1681t(b)(2)). Because CalFIPA purported to set different requirements than the FCRA for information sharing between affiliates, the Ninth Circuit ruled CalFIPA invalid with respect to consumer

report information.

2.5 Privacy policies

The idea that consumers should receive clear notice about privacy is a core principle of many privacy frameworks, including the OECD's 1980 privacy guidelines [39] and the U.S. Federal Trade Commission's Fair Information Practice Principles (FIPPs) [12]. Privacy notice is often presented to consumers in the form of a privacy policy. Overall, privacy notice has been found to impact trust and promote social welfare. For instance, in a study of retail websites, Tang et al. found that the clarity and credibility of privacy notices were crucial for influencing consumer trust [45]. When information about privacy is made accessible to consumers, Tsai et al. found that consumers will pay a premium price to make purchases from more privacy-protective businesses [47].

Unfortunately, a number of issues negatively impact the usability of current privacy policies. Privacy policies are generally written at a very high reading level. For instance, in a study of health websites, Graber et al. found the average privacy policy to require two years of college education to comprehend [17]. Similarly, Jensen and Potts examined 64 privacy policies and found that many were difficult to find and read [22]. The reading level of privacy policies is not the only barrier to comprehension; Ur et al. found instances of privacy policies being unavailable in a user's language, in contrast to the rest of a website [48]. McDonald and Cranor examined the length of privacy policies, estimating that a user would need to spend hundreds of hours a year to read all of the privacy policies relevant to their browsing [33].

Well-designed, standardized formats for privacy notice can overcome many of these obstacles. Furthermore, privacy notices can be compared easily if they are presented in a standardized format. Researchers have examined methods for presenting privacy policies in a standardized, usable manner. For example, Kelley et al. found that displaying privacy policy information in a tabular "nutrition label" format made it easier for users to find information [23]. Even when companies don't provide standardized notice about their

privacy practices or terms of use, projects like "Terms of Service; Didn't Read" have used crowdsourcing to put this information into a standardized, usable format [46].

Standardized privacy notices—whether human-readable or machine readable—help facilitate large-scale comparison and evaluation [5]. For instance, the Platform for Privacy Preferences (P3P) is an XML-based W3C standard for machine-readable privacy policies that specifies what data will be collected and how it will be used [4]. Cranor et al. conducted a study of several hundred computer-readable privacy policies encoded using P3P. They used automated tools to analyze the data collection, use, and sharing practices encoded in each policy. [6]. Unfortunately, P3P has not been widely adopted [5]. In a different study, Cranor et al. found high rates of syntax errors among the P3P policies they examined [6]. Furthermore, Leon et al. found a number of websites misrepresenting their privacy practices through erroneous or misleading P3P compact policies, which are short strings designed to summarize privacy practices associated with cookies [27].

3 Methodology

To perform our evaluation of privacy notices, we first compiled a comprehensive list of financial institutions in the United States. Then, we automatically searched for and retrieved standardized notices from these institutions' websites and parsed their contents. Finally, we performed quantitative analyses that allowed us identify some of the institutions' characteristics that impact their sharing practices. In this section, we detail these steps.

3.1 Obtaining lists of financial institutions

As the first step in searching for U.S. financial institutions' standardized notices based on the model privacy form, we needed a list of these institutions. Having a list of the names and geographic locations of these institutions enabled us to collect standardized notices in a systematic way and minimize confusion between banks with similar names (e.g., multiple,

seemingly independent banks were called "First National Bank," "Liberty Bank," "Pinnacle Bank," etc.). To this end, in March 2014 we compiled two complementary lists encompassing a total of 19,329 financial institutions. The first list comprised a number of different types of financial institutions. The second list comprised only federal credit unions, which were absent from the first list.

We created our first list of 12,511 distinct financial institutions by merging lists from the Federal Reserve (Fed) and the Federal Deposit Insurance Corporation (FDIC), two of the largest U.S. government agencies related to the financial industry. To obtain the Federal Reserve list of 6,588 financial institutions, we made a Freedom of Information Act (FOIA) request. The list of 6,781 financial institutions insured by the Federal Deposit Insurance Corporation is available online.[3] The FDIC list also includes an institution's characteristics, location, assets, and contact information [9]. We merged these two lists based on each institution's "Research, Statistics, Supervision and Regulation, and Discount and Credit" (RSSD) ID number, removing duplicate entries. The RSSD ID uniquely identifies all institutions that have reporting obligations to the Federal Reserve. Although these two lists overlapped to an extent, we found that many institutions were present on only one of these lists. Following the merging process, our list contained 12,511 financial institutions.

We also made FOIA requests to obtain lists of financial institutions from the other main United States government agencies that regulate financial institutions, notably the Consumer Financial Protection Bureau (CFPB) and the Office of the Comptroller of the Currency (OCC). Although these lists together included 101 institutions absent from both the Federal Reserve and FDIC lists, they had much less metadata about the institutions' characteristics. Therefore, we chose to exclude these additional institutions.

Our second list comprised 6,818 credit unions supervised by the National Credit Union Administration (NCUA).[4] The NCUA regulates federal credit unions in the United States.

[3]FDIC Institution Directory. `http://www2.fdic.gov/IDASP/`

[4]National Credit Union Administration. 5300 Call Report Quarterly Data. `http://www.ncua.gov/DataApps/QCallRptData/Pages/CallRptData.aspx`

In addition to the name of each credit union, the list contained each institution's full mailing address, as well as information on its peer group.

3.2 Determining an institution's web domain

While the FDIC list contained website URLs for most institutions, the lists from the Fed and credit unions did not include website URLs. To determine the website domain for those institutions, we performed an automated Google query of the string "*Institution name*, *City*, *State*" and took the domain of the first result to be that institution's domain. This heuristic is imperfect, yet we believe it conservatively minimizes false associations (incorrectly attributing a standardized notice to the wrong institution) at the expense of increasing the number of false negatives (not finding notices for institutions that have them available).

Appendix A presents the technical details of this process, as well as further methodological details about our web crawling and parsing of standardized notices.

3.3 Retrieving standardized notices

Using Google's search engine, we then conducted an automated web search to collect institutions' standardized notices. We used the header of the model privacy form, "What does *institution name* do with your personal information," as a search string, inserting the corresponding institution's name. We felt it important to minimize the chance of accidentally retrieving another institution's standardized notice, particularly in light of the large number of financial institutions with similar names. Therefore, using Google's *as_sitesearch* parameter, we restricted each query to the website domain we determined in the prior step.

We retrieved the first ten webpages returned as a result of that Google query for each company and selected the one with the largest number of hallmark elements of a standardized notice for further analysis, setting a minimum threshold of elements included to consider it valid. Appendix A details this process.

Across the 19,329 financial institutions in our two lists, we obtained standardized notices for 6,191 financial institutions. Of the 6,409 institutions whose website domain was known from the FDIC list, we obtained standardized notices for 3,594 institutions (56% of the institutions). Of the 6,102 institutions whose website domain was not listed, we obtained standardized notices for 787 institutions (13%). Finally, of the 6,818 credit unions, none of whose domains were known a priori, we found standardized notices for 1,810 credit unions (27%). The standardized notices from these 6,191 financial institutions make up the data set for all of our further analyses.

For additional insight into the practices of financial institutions that consumers may be most familiar with, we manually collected notices from the 86 financial institutions on a Forbes list of the 100 largest banks [3] for which we could manually find standardized notices. Similarly, to understand consumers' privacy options for credit cards, we collected standardized notices from all 11 credit card companies included in a J.D. Power survey of credit card satisfaction [21].

3.4 Parsing standardized notices

Having selected at most one standardized notice for each institution, our automated parsing program extracted data about each institution's privacy practices. The model privacy form has a strict document structure based on a number of subsections. As the first step in extracting data, we split the standardized notice's text into the sections specified in the model notice shown in Figure 1 (Section 2), focusing on practices regarding what and how information is collected, how information is shared, whether and how consumers can limit sharing, and whether companies have affiliates, nonaffiliates, and joint marketing partners. We extracted these practices to a CSV spreadsheet.

During the development of our parsing program, we repeatedly tested our parser on small groups of standardized notices and manually checked for instances that were not matched. Based on these manual checks, we iteratively improved our parser to capture rewordings

we commonly observed. For instance, we observed "use your credit or debit card" being replaced by the similar statements "use your credit/debit card," "use your credit card," "use your debit card," and "use your ATM card." We adjusted the parser to recognize all of these variants. Similarly, as we detail in Appendix B, we iteratively updated our parser to recognize many variants of revision dates.

We paid particular attention to parsing the *disclosure table* (Figure 1), which states an institution's data-sharing and opt-out practices across seven different purposes. We initially searched for "Yes," "No," and "We don't share," the values permitted in the specification of the model privacy form [38]. Based on our iterative verification process, we supported six additional case-insensitive variants: "we do not share"; "we don't collect"; "we do not collect"; "we have no affiliates"; "Y"; and "N."

Despite these efforts, our parser did not recognize every corner case among the thousands of standardized notices. To estimate the accuracy of our automated parser, we manually verified the parser's accuracy on a random sample of 50 institutions' privacy disclosures. For each of the sections of the document we examined, our parser was accurate for between 90% and 100% of documents. We describe this verification process in detail in Appendix B.

3.5 Analysis

A primary goal of our project was analyzing the prevalence of different privacy practices across the financial industry, as well as among potentially competing institutions with similar characteristics. For instance, we examined the types of information institutions said they collected, the occasions on which institutions said they collected data, and the different sharing practices and opt-out mechanisms institutions presented to consumers.

We further investigated whether the institution type, as reported by the Federal Reserve, was correlated with the institution's privacy practices. In addition to institution types reported by the Federal Reserve, we considered all federal credit unions to form an additional institution type, which we termed *credit union*.

Finally, using the subset of institutions for which we had additional information regarding institutions' characteristics, we investigated which of those characteristics were correlated with their sharing practices. We joined the data we parsed automatically from standardized notices with each institution's characteristics, as reported in the FDIC Institution Directory [9] and list of institutions from the Federal Reserve. In the FDIC list, these characteristics included an institution's geographic region, assets, and type of institution. We used these characteristics as independent variables and the binary indicator "shares"/"does not share" as the dependent variable to build logistic regression models. We built a regression model for six of the seven sharing practices in the disclosure table. We excluded the "for our everyday business purposes" row because nearly all institutions had identical practices.

As a secondary goal, we also investigated whether institutions' practices, as stated in their standardized notices, complied with relevant portions of GLBA and the FCRA. We also examined the degree to which institutions deviated from the specification of the model privacy form. We manually verified instances where our parser found idiosyncratic results or where automated analysis suggested violations of GLBA or the FCRA. As part of this analysis, we also visited the webpages of a random subset of 50 institutions to see how the model privacy form was used in practice.

We first performed this analyses on a smaller set of FDIC-insured financial institutions in March 2013 and published preliminary results [7]. In this earlier analysis, we identified 24 institutions whose practices stated in their standardized notice would violate GLBA, the FCRA, or both. In November 2013, we sent a letter on Carnegie Mellon letterhead to the 19 institutions for which we were able to find a postal address. This letter pointed out the problematic statements in their institution's standardized notice. In our more recent analysis using an updated and larger list of companies, we identified 109 institutions with similarly problematic disclosures in their standardized notices. In July 2014, we sent letters to the 96 institutions for which we were able to find a postal address. We discuss these institutions' responses to our letters in Section 4.4.

4 Results

We first provide an overview of institutions' privacy practices, including the reasons for which they share data and the means through which consumers can opt out. We found substantial variation in practices across institutions. To understand more fully whether competing companies' privacy practices differ, thereby providing an opportunity for consumer choice, we then compared institutions by category, again finding differences across these comparable institutions. For similar reasons, we also examined the data-sharing practices of companies that appear on lists of recommended banks and credit cards, again finding a wide range of practices. We then present statistical analyses to investigate how institutions' characteristics, including size, location, and type, correlate with sharing practices. Subsequently, we show how dozens of companies appear to be violating the law by stating in their standardized notices that they do not offer legally mandated opt outs. Finally, we present our observations of how companies misuse the model privacy form, as well as how the design of the model privacy form might impact institutions' transparency with respect to data-collection practices.

4.1 Data practices

In this section, we describe financial institutions' stated data-collection and data-sharing practices. We discuss with whom data is shared, reasons why data is shared, and the mechanisms institutions give consumers for opting out of data sharing when applicable. We also present institutions' disclosures of the information they collect and how they collect it. We argue that these final two disclosures are not particularly informative.

Overall, our results show that sharing and opt-out practices vary widely across financial institutions. This variety of practices suggests that helping consumers compare institutions' practices could empower them to select companies that better align with their privacy expectations.

4.1.1 With whom data is shared

Standardized notices present consumers with information about how a financial institution shares their data with other companies. These disclosures discuss *affiliates*, which are financial or nonfinancial companies that are "related by common ownership or control" to the institution making the disclosure. The disclosures also discuss *nonaffiliates*, which are third parties that are not affiliates; and *joint marketers*, which can be affiliates and nonaffiliates. In the "Definitions" section of the model privacy form (see last section in Figure 1), institutions must indicate whether or not they share customers' information with affiliates, nonaffiliates, and joint marketing partners. If they share with any of these entities, they must also list illustrative examples of such entities [38].

Institutions varied starkly in their practices, as shown in Table 1. On the question of sharing with affiliates, 28% of institutions said they have affiliates and share with them, 25% said that they do not share with their affiliates, and 43% said that they do not have any affiliates. The remaining 4% of institutions, labeled *blank* in Table 1, did not provide any information about whether they have affiliates. In contrast, 12% of institutions said they share with nonaffiliates, 66% said they do not, and only 18% said they do not have nonaffiliates. Joint marketing practices also differed; 42% of institutions said that they engage in joint marketing whereas 55% said that they do not. This section of the model privacy form was missing entirely for 0.9% of institutions, and the remaining institutions defined the terms without providing information about their own practices. The differences we noted suggest that financial institutions follow considerably different practices.

4.1.2 Reasons data is shared

The model privacy form's disclosure table lists seven reasons for which an institution might share data, along with the institution's own practices for each of these reasons. For each of these reasons, institutions can disclose that they do not share data at all, share data but offer an opt-out, or share data without offering an opt-out. Notably, as we discuss further in

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

Table 1: The data-sharing practices of the institutions in our primary data set. *Blank* indicates that the institution defined the term, yet provided no information about its own practices. We did not observe this section for 53 of the 6,191 institutions.

Section 4.4, some institutions' policies state that they do not offer opt-outs for data sharing even when the FCRA or GLBA mandates such an opt-out be provided.

The disclosure table comprises seven rows, each representing a reason an institution might share data, such as the institution's everyday business purposes or joint marketing purposes. One row, "for our affiliates to market to you," is optional for institutions that do not have affiliates, whose affiliates do not use personal information, or whose affiliates have a separate notice [38]. Of the 6,191 institutions in our data set, 3,754 institutions (61%) omitted this row. Note that we did not check for consistency between the disclosure table and the definitions section of the model privacy form.

We grouped institutions' practices into three primary categories based on their responses to the questions, "Does [institution name] share?" and, "Can you limit this sharing?" We labeled institutions that answered "no" to the first question as *does not share*. Institutions

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]*	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%

Table 2: A summary of 6,191 financial institutions' practices for sharing consumers' personal information. Institutions self-reported these practices in the model privacy form's disclosure table. Values that are missing could be caused by an institution omitting that row of the table, or by an error in our parser. An additional 0.2%–0.7% of institutions in each row made disclosures that were contradictory; these are not shown in the table.

that responded "yes" to the first question and "yes" to the second question provide an opt-out for this sharing, so we labeled those institutions *share, opt-out*. We assigned the label *share, no opt-out* to institutions that answered "yes" and "no," respectively. When a particular row of the table was not parsed, we labeled that value *missing*. As we discuss further in Section 4.5.1, a handful of institutions provided contradictory answers to these two questions. For example, some institutions said in the first column that they share data for the purpose represented by that row, yet said in the second column that they do not share data for that

reason. Between 13 and 42 institutions (0.2%–0.7%) per row make contradictory disclosures.

Companies are required to provide opt-outs for some types of data-sharing, but are not required to do so in other cases. As we discussed in Section 2.1, institutions that share information about creditworthiness with affiliates, or that share with either affiliates or nonaffiliates for marketing purposes, must provide an opt-out. Institutions that share for "our marketing purposes," that share "for joint marketing," or that share information about transactions and experiences with affiliates "may choose to provide an opt-out," but are not required to do so [38].

Table 2 summarizes institutions' sharing practices. Where not required to provide an opt-out, most institutions chose not to provide one. Almost all institutions shared personal information for their everyday business purposes without offering an opt out. More than half of the institutions (61.9%) said they share "for our marketing purposes" without offering an opt-out, and a third (33.0%) said they share "for joint marketing" without an opt-out. Fewer (21.5%) said they share information about transactions and experiences "for affiliates' everyday business purpose" without an opt-out.

Although many institutions did not offer an opt-out if not required to do so, some institutions chose not to share data or voluntarily chose to offer opt-outs. If comparative privacy information were easily accessible, consumers could choose to do business with the more privacy-protective institutions. We discuss our efforts in leveraging our automated methods to make such information accessible in Section 5.1.

4.1.3 Opt-out mechanisms

The mechanism for opting out of data sharing could impact consumers' likelihood to opt out. We parsed the contents of the "to limit our sharing" section of the model privacy form, searching for instructions on opting out via mail, email, web, and telephone. Table 3 shows the opt-outs offered. Overall, 20.5% of institutions offer at least one opt-out mechanism. We observed 627 institutions that provided exactly one mechanism, 491 institutions that

Opt-out mechanism(s)	Number of institutions providing this opt-out mechanism	Fraction of the total number 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%

Table 3: Institutions' opt-out mechanisms. Overall, 1,270 institutions offered an opt-out. The most common opt-out mechanisms were phone, website, and postal mail.

provided two different mechanisms, and 152 institutions that provided at least three different mechanisms.

Non-computer-based opt-out mechanisms were more prevalent than computer-based methods. Of the institutions offering an opt-out, 28.2% let consumers opt out via email or a website. In contrast, 59.9% of institutions allowed consumers to opt out over the phone, via postal mail, or using either mechanism. We counted institutions as providing a postal mail opt-out if they either instructed consumers to send mail to a particular address or, more popularly, provided a detachable, mail-in form to fill out. For 48.1% of institutions, we automatically observed such a detachable mail-in form.

4.1.4 What information is collected

The first section of the model privacy form discloses "the types of personal information that the institution collects and shares" based on a predefined list of 24 types of information financial institutions commonly collect. The model privacy form specifies that the term "Social Security number" must be the first bullet, followed by exactly five of the following

23 terms: "income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions" [38]. In total, exactly six terms should be arranged in three bullet points, as shown in Figure 1 in the background section of the paper.

The main design objective of this section of the model privacy form was to familiarize customers with the concept of personal information, but not necessarily to provide a comprehensive list of the types of personal information that institutions collect [24]. Unfortunately for consumer understanding of privacy practices, given that institutions are told to include exactly six out of 24 data types, the omission of a data type does not provide any meaningful information about whether or not the institution collects that type of data.

We parsed this section, searching for "Social Security number" and the aforementioned 23 terms, as well as close variants. Detailed results can be found in Section H of the appendix. The most common terms institutions chose to include were account balance (5,493 institutions), payment history (4,902), credit history (4,881), income (3,428), credit scores (2,842), and transaction history (2,138). Notably, these are the six terms listed in pink font (intended to be replaced by financial institutions) in the model privacy form.

Furthermore, we expect that few consumers would be surprised if a financial institution collected any of the types of information an institution is permitted to list in this section. In fact, consumers might be more concerned if their financial institutions chose *not* to collect their account balance and similar types of information. As a result, the current requirements do not provide transparency of collection practices. To provide more useful information to consumers, companies could be required to list all data they collect, or to disclose any types of data they collect that might surprise consumers.

In addition, while having a standardized language for data collection is necessary to

enhance transparency and facilitate comparison of companies' practices, we found that some of the terms are redundant and potentially ambiguous. For example, it would be difficult for an average consumer to differentiate between "transaction history" and "transaction or loss history." Similarly, it is unclear whether "account balance," "payment history," and "transaction history" are all part of "checking account information." On the other hand, as discussed in Appendix H, some institutions listed additional types of data they collect outside of those specified for use in the model privacy form. Taken together, these results suggest the need to improve this section of the model privacy form to enhance transparency and account for all institutions' practices.

4.1.5 How information is collected

On the second page of the model privacy form, financial institutions are required to say how they collect consumers' information, again using phrases from a predefined list. The specification of the model privacy notice states that "institutions must use five (5) of the following terms to complete the bulleted list for this question," followed by a list of 34 occasions [38]. We present a detailed count of these disclosures in Appendix I.

As with the types of information collected, the five most frequent terms for how information is collected were simply the five listed in pink as examples in the model privacy form [38]: "open an account," "apply for a loan," "use your credit or debit card," "deposit money," and "pay your bills." On the opposite end of the spectrum, only one institution noted collecting information when consumers tell them about investment or retirement earnings, while no institutions specified collecting information when consumers sell securities to them.

Given that institutions are permitted to include only five terms, the omission of a term again does not provide any meaningful information about whether or not the institution collects data during that type of event. Such a limitation reduces institutions' transparency and does not benefit consumers.

Furthermore, many of the current terms may not be very informative because they are

obvious. Some services requested by customers obviously necessitate collection of personal information. For example, it may not be necessary to tell people that their personal information will be collected when they open an account or apply for a loan in light of the paperwork involved in doing either. It might be more useful to inform consumers about situations when it is less obvious that personal information will be collected.

The model privacy form also contains disclosures about other sources that provide data to an institution. Under the section titled, "How does *name* collect my personal information?" institutions must include either of the following statements if they apply to their practices: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies," or, "We also collect your personal information from other companies" [38]. We observed that 82.9% of institutions collect additional information from credit bureaus, 83.4% do so from "other companies," and 73.2% collect data from affiliates.

4.2 Comparing similar institutions

The previous analyses uncovered differences in sharing practices across all institutions, yet such a general analysis does not show the degree to which direct competitors or institutions providing comparable services have similar privacy practices. One might assume that differences in practices result from institutions offering different types of services. When similar institutions vary in privacy practices, however, a consumer armed with this information could choose where to do business, enabling privacy choice.

4.2.1 Practices within a specialization

We first compare the practices of similar institutions based on their specialization. First, we split the institutions into different types using categories defined by the Federal Reserve. We also added all federal credit unions from the NCUA list as an additional type of financial institution. After eliminating categories for which we obtained fewer than ten institutions' standardized notices, the nine categories of institutions we compared are shown in Table 4.

Institution Type	Description	Examples
Bank Holding Company (BHC)	Companies that own or control one or more U.S. banks and which are supervised by the FED.	Pinnacle Bancorp Inc.
Commercial Bank - OCC (N)	Companies that engage in various lending activities and which are supervised by the OCC.	Wells Fargo Financial National Bank
Commercial Bank - FED (SM)	Companies that engage in various lending activities and which are supervised by the FED.	First State Bank of Colorado
Commercial Bank - FDIC (NM)	Companies that engage in various lending activities and which are supervised by the FDIC.	Farmers State Bank
Credit Union	Institutions created and operated by its members, who share profits. Supervised by the NCUA.	Lafayette Credit Union
Financial Holding Company (FHD)	Companies engaged in a broad range of banking-related activities, including insurance underwriting, securities dealing and underwriting, financial and investment advisory services, merchant banking, issuing or selling securitized interests in bank-eligible assets, and generally engaging in any non-banking activity authorized by the Bank Holding Company Act. They are supervised by the FED.	Capital One Financial Corporation
Savings and Loan Holding Company (SLHC)	Companies that directly or indirectly control one or more savings association.	AJS Bancorp Inc.
Savings Association - OTS (SA)	Companies that accept deposits primarily from individuals and channels their funds primarily into residential mortgage loans. They are supervised by the OTS.	Century Savings and Loan Association
Savings Bank - FDIC (SB)	Companies organized to encourage thrift by paying interest dividends on savings and which are supervised by the FDIC.	Royal Savings Bank

Table 4: The 9 institution types that we analyzed and compared. With the exception of credit unions, this classification is provided by the Federal Reserve [11].

Even among the same institution types, practices differed. Figure 3 shows a comparison of institutions of each type. In that figure, the presence of different colors in a horizontal bar indicates institutions of the same type that differ in their practices. We do not present a graph of sharing for an institution's own "everyday business purposes" because nearly all institutions shared data for that purpose without offering an opt-out.

In addition to widespread data sharing for "everyday business purposes" by all type of institutions, between 53.4% and 79.2% of institutions of each type shared data for their own marketing purposes. Whereas only 9.5% of credit unions chose not to share data for their marketing purposes, 44.0% of state commercial banks supervised by the FDIC did not share data for this purpose. Between 1.2% and 16.3% of institutions in each specialization shared data for this purpose, yet offered an opt-out.

Institutions that shared data for affiliates' marketing purposes were required to offer an opt-out. Rather than not sharing data for this purpose, many institutions indeed offered opt-outs for this type of sharing. Between 22.0% (credit unions) and 65.6% (financial holding companies) of institutions shared data for affiliates' marketing purposes, yet said that consumers could limit this sharing by opting out. Opt-outs were comparatively less common for types of sharing for which institutions were not required to provide an opt-out; no more than 24.5% of institutions in a category voluntarily offered opt-outs.

The 126 financial holding companies whose standardized notices we obtained had less consumer-friendly sharing practices than all other types of institutions. While 62.4% of financial holding companies shared data about customers' transactions and experiences with affiliates without offering an opt-out, no more than 35.0% of the institutions in any other category did the same. Similarly, only 34.4% of financial holding companies did not share data for "affiliates to market to you," whereas 53.1%–75.9% of institutions in the other categories chose not to share data for this reason.

4.2.2 Practices among the largest banks and credit card companies

We also examined even more directly whether consumers might be able to exercise privacy choice among some of the most well-known competitors. To this end, we compared the institutions on a list compiled by Forbes [3] of the 100 largest banks, as well as the institutions on a list compiled by J.D. Power & Associates of consumer satisfaction with credit card companies [21]. Even among companies in these lists, we found differences in privacy practices, suggesting that making privacy practices more salient could empower consumers to choose more privacy-protective institutions. In addition to the aforementioned categories of primary specialization, Figure 3 includes bars visualizing the practices of the *large banks* and *credit card companies* we discuss in this section.

In November 2014, we manually searched the websites of all banks in a Forbes list of the 100 largest banks in the U.S. [3] for standardized notices. We found standardized notices for 86 of these banks. Since a consumer might choose from among these large banks, we investigated how their privacy practices compare. Table 8 in the appendix summarizes large banks' practices in aggregate, while Table 9 in the appendix details each large bank's practices.

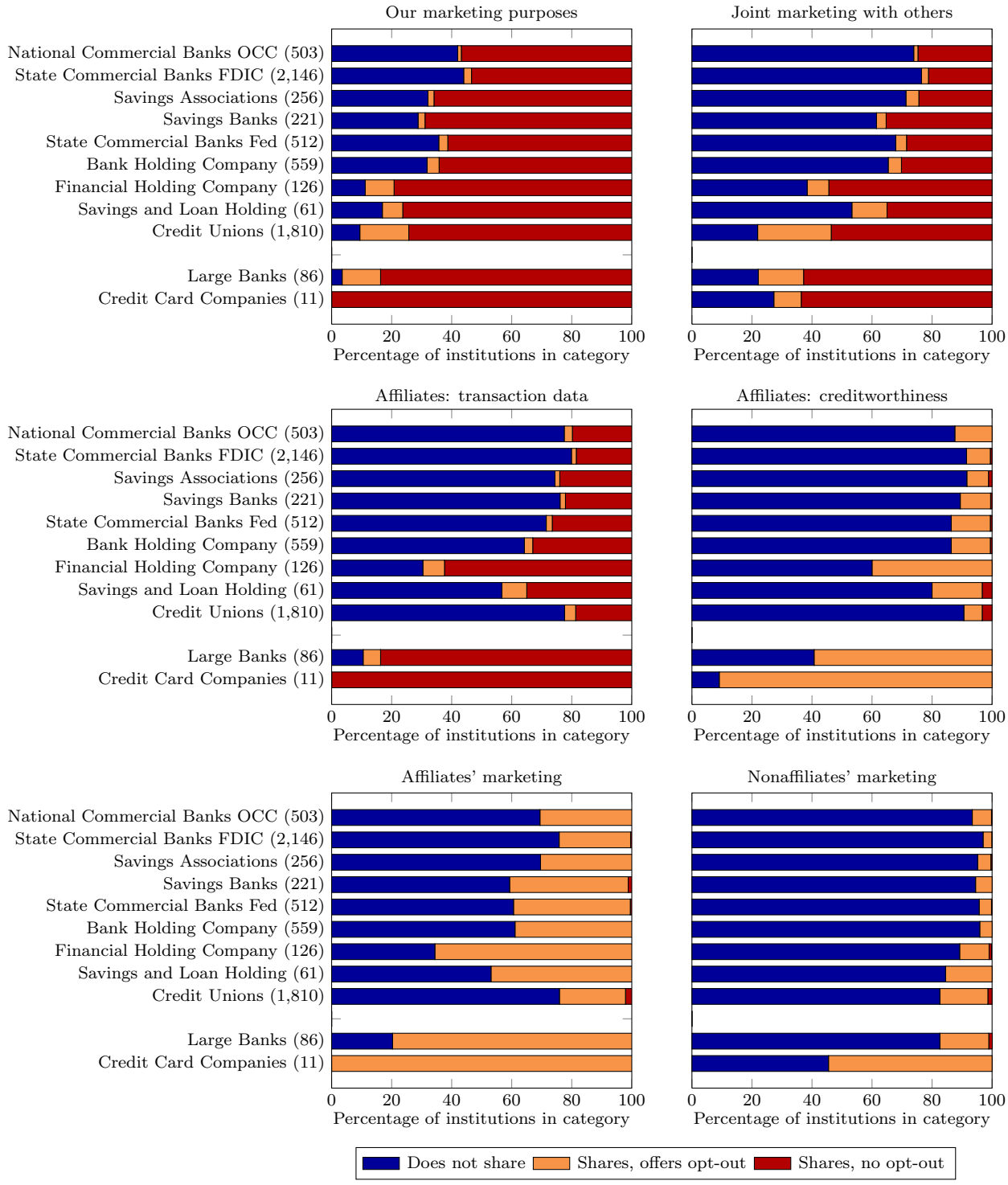


Figure 3: The prevalence of sharing practices from the disclosure table. We exclude missing data. In particular, only 2,418 institutions disclosed their practices for the optional "for our affiliates to market to you" category.

Relative to financial institutions overall, the large banks tended to be less privacy-protective. The proportion of large banks that shared data was larger than the proportion of institutions in each of the nine primary specializations that did the same for five of the six types of sharing shown in Figure 3. For example, 90.4% of large banks shared data for affiliates' marketing purposes, whereas only between 24.1% (credit unions) and 65.6% (financial holding companies) of institutions in each of the nine specializations did the same.

We also analyzed the sharing practices of the eleven credit-card companies listed in a consumer-satisfaction survey conducted by J.D. Power and Associates [21]. Most of these companies shared data for many reasons, yet a few had more privacy-protective practices for certain types of sharing. However, for the company's own marketing and for providing affiliates information about transactions and experiences, all eleven credit card companies shared data without offering an opt out. Similarly, for affiliates' marketing purposes, all eleven credit card companies shared data, though all did offer an opt-out.

Eight of the eleven credit card companies said they share consumers' personal information without offering an opt-out for "our marketing purposes," "joint marketing," and "affiliates' everyday business purposes - transactions and experiences." Only GE Capital, U.S. Bank, and Wells Fargo said they do not share for joint marketing. Similarly, more than half of the companies said they share for "nonaffiliates to market to you." Table 10 in the appendix lists the practices of each credit card company.

4.3 Factors correlated with privacy practices

Using metadata provided as part of the FDIC directory [9], we investigated how different institutional characteristics correlated with those institutions' privacy practices. Because the other lists of institutions did not include such rich metadata, we limited this analysis to institutions on the FDIC list. The factors we investigated included the institution's size in terms of assets, the type of institution according to the Fed classification, the geographic region where the institutions' headquarters were located, whether the institution had been

granted any trust powers to conduct fiduciary activities [10], and whether the institution was owned by shareholders. We list these factors alongside additional details in Table 5. We selected this subset of characteristics from a larger set in the FDIC directory to account for what we found in pilot studies [7] to be the most relevant characteristics.

For example, a number of variables in the FDIC directory all could serve as proxies for the size of an institution, including equity, income, number of offices, and whether the company is a bank holding company. We decided to measure an institution's size using its total assets because we learned that researchers at the CFPB use that metric as a proxy for size. Similarly, various variables potentially indicate an institution's location. We decided to use the four geographic districts defined by the OCC to categorize institutions into four general regions. Using only four OCC districts as opposed to individual states allowed us to make more meaningful statistical comparisons across regions. Statistical analysis across states would be problematic because only a handful of institutions are headquartered in certain states.

To evaluate the impact of these factors on institutions' sharing practices, we built logistic regression models. While we chose not to build a model for sharing related to an institution's everyday business purposes because that practice varied minimally, we built six regression models corresponding to the other six practices listed in the disclosure table. We gradually increased the number of variables in our models, always starting with assets, which was a strong predictor in our proportionality χ^2 tests. Next, we added location, institution type, and additional indicator variables. We also switched the order in which variables were added and looked at the residual errors of each model. In the end, we selected the model with the lowest residual error for each regression.

When an institution did not share consumers' personal information for a particular purpose, we assigned the binary outcome variable the value 0. When an institution shared information, regardless of whether it offered an opt-out, we assigned the outcome variable the value 1. We also tested ordinal models where the outcome variable had three levels:

not sharing, sharing with an opt-out, and sharing without an opt-out. The results of these models were similar to the binary models; we report results from the binary model in this paper as those are easier to interpret.

Factor	**Definition**	**Possible values**	**Control category**
Assets bracket*	The sum of all assets owned by the institution. Includes cash, loans, securities, and bank premises, but not off-balance-sheet accounts	We created five percentile brackets based on assets (Mean = 1.389 B, Min = 3.7 M, Max = 360 B): Very small (x<25%); Small (25%<x<50%); Medium (50%<x<75%); Large (75%<x<90%); and Very large (90%<x).	Very small
Institution Type	Classification of institutions according to the Federal Reserve	Commercial bank supervised by the OCC (N), commercial bank supervised by the Federal Reserve (SM), commercial bank supervised by the FDIC (NM), savings bank supervised by the FDIC (SB), savings association supervised by the OTS (SA)	NM
OCC District	OCC District where the institution is physically located (see discussion in Section 4.3.2)	Northeastern, Southern, Central, Western	Western
Ownership type	Whether the institution is owned by shareholders (Stock) or not (Non-stock)	Stock, Non-stock	Stock
Trust Powers	Trust powers are defined on a per-state basis	Yes, No	No
Metro Statistical Area	Is the institution in a region with at least one urban area with population $\geq$50,000?	Yes, No	No

Table 5: Independent variables considered in our logistic regression models.

As shown in Table 6, our logistic regression models revealed a number of factors to be significantly correlated with institutions' privacy practices. Chief among these factors were the institution size (measured in terms of assets) and the OCC District where the institution

was geographically headquartered. The type of institution was a significant factor for the marketing purposes of the institution itself, its affiliates, and its nonaffiliates. We discuss the impact of each of these characteristics in the following section and present detailed results for each regression model in Section F of the appendix.

Factor	**Control category**	**Own marketing**	**Joint marketing**	**Affiliates (Trans.)**	**Affiliates (Credit.)**	**Affiliates' marketing**	**Nonaffiliates' marketing**
Size (assets)	Very small	↑	↑	↑	↑	↑	↑
OCC district	Western	↓	↑	↓	N/A	↑	↑
Institution type	Commercial/FDIC	↑	N/A	N/A	N/A	↑	↑
Trust powers	No powers	N/A	↑	↑	N/A	N/A	N/A
Ownership type	Stock	N/A	N/A	N/A	↓	N/A	N/A

Table 6: Summary of characteristics that significantly impact sharing practices. ↑ and ↓ respectively denote an increase and decrease in sharing with respect to the control category. N/A denotes that the variable was not included in the corresponding final model, meaning it did not correlate strongly with sharing practices.

4.3.1 Institution size

We found that the larger the institution, the more likely they were to share consumers' data across all six sharing purposes we investigated. Table 12 in the appendix shows the fraction of institutions in each asset bracket that do not share, share yet offer an opt-out, and share without offering an opt-out. For example, only 10.5% of institutions below the 25th percentile of assets shared for joint marketing purposes without offering an opt-out, whereas 54.4% of institutions above the 90th percentile did so. Similarly, only 1.4% of institutions below the 25th percentile in terms of assets shared with non-affiliates to market to consumers, whereas 9.1% of institutions above the 90th percentile did so. Our regression models shown in Table F in the appendix detail the sharing behaviors of institutions in each asset bracket. For example, when compared with a small institution, the odds that a very large institution

would share for joint marketing purposes are over ten times higher, and the odds that a very large institution would share with non-affiliates to market to consumers are over six times higher. It is important to give special attention to joint marketing practices as the principal reason why the GLBA included an exception to permit joint marketing with non-affiliates without requiring institutions to offer an opt-out was to allow small institutions to compete with large ones [43]. Nevertheless, we have found that large companies are more likely to share for this purpose than small companies.

4.3.2 Geographical location

We also found the geographical location of the institution to be significantly correlated with its sharing practices. Table 13 in the appendix details how practices vary across OCC regions.[5] For example, only 30.3% of institutions in the Northeastern region chose not to share consumers' information for their own marketing purposes. In contrast, 47.2% of institutions in the Northern region and 50.4% of institutions in the Southern region chose not to share information for their own marketing purposes. We also found differences in sharing for joint marketing. Whereas 32.9% of institutions in the Northeastern region shared for joint marketing without offering an opt-out, fewer than 23% of institutions in the Southern and Central regions did so.

These results show that there are significant differences in sharing practices across geographical regions, and these differences ultimately impact the customers of banks headquartered in those regions. Our regression models allowed us to investigate the specific effect of geographic location for each of the sharing purposes. Institutions in the Northeastern OCC region shared at a higher rate than those in the Western region for both joint marketing

[5]The states in each of the four OCC regions are as follows:
Northeastern: Connecticut, Delaware, DC, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Puerto Rico, Rhode Island, U.S. Virgin Islands, Vermont, Virginia, and West Virginia; **Southern:** Alabama, Arkansas, Florida, Georgia, Louisiana, Mississipi, Oklahoma, Tennessee and Texas; **Central:** Illinois, Indiana, Kentucky, Michigan, Minnesota, Ohio, and Wisconsin; and **Western:** Alaska, American Samoa, Arizona, California, Colorado, Guam, Hawaii, Idaho, Iowa, Kansas, Missouri, Montana, Nebraska, Nevada, New Mexico, Oregon, South Dakota, States of Micronesia, Utah, Washington, and Wyoming

($p = 0.01$) and for affiliates to market to consumers ($p < 0.001$). Similarly, institutions in the Central OCC region shared at a higher rate than those in the Western region for both joint marketing ($p = 0.05$) and for non-affiliates to market to consumers ($p = 0.02$). In general, institutions in the Southern region were less likely to share consumer data than institutions in the Western region. Similarly, compared to institutions in the Western region, a larger fraction of institutions in the Central and Northeastern regions shared consumer data.

We looked closer at differences across states in each of the four OCC regions. In each region, we selected the state with the largest number of institutions. Table 7 shows the practices of institutions in these states regarding sharing for joint marketing and for affiliates to market to consumers. The per-state results were consistent with the OCC-region results. In particular, institutions in New York (Northeastern region) shared more than institutions in the other three states for both joint marketing without offering opt-out choices (30.9%) and affiliate marketing (47.6%). Institutions in California (Western region) shared less than institutions in the other three states for both joint marketing and affiliate marketing. It is also important to remember, as mentioned in the related work, that California's Financial Information Privacy Act (CalFIPA) mandates that consumers opt in before a financial institution may share "nonpublic personal information" with a nonaffiliated third party.

4.3.3 Institution type

The type of institution was significantly correlated with three of the six sharing practices we studied. Table 14 in the appendix shows that, in comparison to other types of institutions, commercial banks supervised by the FDIC most frequently did not share data for their own marketing purposes, or for affiliates and non-affiliates to market to consumers. Our regression models also show that savings associations are significantly more likely to share than commercial banks supervised by the FDIC ($p = 0.03$). Other commercial banks also share at higher rate than FDIC commercial banks for both affiliates and non-affiliates to

Sharing practice	Texas (Southern)		Illinois (Central)		California (Western)		New York (Northeastern)	
Joint marketing with other financial companies (N = 775)								
Don't Share	213	78.0%	207	74.7%	126	87.5%	55	67.9%
Share, Opt-Out	6	2.2%	3	1.1%	6	4.2%	1	1.2%
Share, No Opt-Out	54	19.8%	67	24.2%	12	8.3%	25	30.9%
For our affiliates to market to you (N = 287)								
Don't Share	58	73.4%	84	80.8%	52	83.9%	22	52.4%
Share, Opt-Out	21	26.6%	20	19.2%	10	16.1%	19	45.2%
Share, No Opt-Out	0	0.0%	0	0.0%	0	0.0%	1	2.4%

Table 7: Sharing practices of the state in each region with the most institutions. Overall, institutions in California shared less than institutions from the other three states, and institutions in New York shared more than institutions from the other three states. Differences were statistically significant at α=0.05 using a χ^2 proportionality test.

market users ($p < 0.05$). In general the type of institution impact differently sharing for own marketing practices and both sharing for affiliates and non-affiliates to market to consumers.

4.3.4 Other factors

Two additional characteristics were correlated with data sharing practices for joint marketing and everyday business purposes. In particular, banks with granted trust powers shared at a significantly higher rate for joint marketing and everyday business purposes (transactions and experiences). Trust powers are granted at the state level under criteria that vary by state [10] and are correlated with the institution's size. The larger the institution, the more likely it will have trust powers. Nevertheless, even when controlling for an institution's assets, institutions with trust powers were more likely to share data. We also found that companies owned by shareholders were more likely to share creditworthiness information for their affiliates' everyday's business practices than institutions not owned by sharedholders.

4.4 Compliance with the FCRA and GLBA

As discussed in Section 2.1, GLBA prohibits financial institutions from sharing nonpublic personal information with nonaffiliated third parties unless the institution offers consumers the opportunity to opt out of that sharing. Similarly, the FCRA mandates the provision of an opt-out before information about consumers' creditworthiness may be shared with affiliates and, as amended by FACTA, mandates the provision of an opt-out before consumer report information may be shared with affiliates for marketing purposes.

In our previous analysis of 3,422 standardized notices in March 2013, we found 24 companies whose opt-out practices appeared to be in violation of the FCRA, FACTA, or GLBA [7]. In November 2013, we contacted the 19 companies for which we could find a mailing address. We mailed each company a letter on Carnegie Mellon University letterhead to inform them about the problematic assertions in their standardized notice.

Five institutions formally responded to us. All five institutions stated that the problematic assertions in their standardized notices were mistakes, and all five institutions subsequently updated their standardized notices. Furthermore, we observed that four companies that did not respond to us also updated their standardized notices. The remaining 15 institutions' stated practices remain in violation of the law.

In this round of analysis, we found 96 institutions in apparent violation of the law, affirming that they share for one or more of these reasons, yet stating that consumers cannot limit this sharing. We manually verified that each institution's standardized notice was parsed correctly. A total of 61 institutions said they shared information about creditworthiness "for our affiliates' everyday business purposes" and said that consumers could not limit this sharing. Furthermore, 27 institutions did the same "for our affiliates to market to you," while 30 institutions followed the same practice "for nonaffiliates to market to you." Note that some institutions had more than one violation, which is why the total number of violations exceeds the number of companies in violation.

As a result of the larger analysis reported in this paper, we sent letters in July 2014 to 76 credit unions and 20 other institutions whose stated practices violate the law. In this round, 13 institutions formally responded to us, and 11 of those institutions have since removed the illegal assertions from their standardized notices.

In Appendix E, we list the 85 financial institutions whose standardized notices still assert sharing practices that violate GLBA or FCRA opt-out requirements as of November 2014. Even after our two rounds of informing institutions about their problematic disclosures, 52 institutions still said they shared information about creditworthiness "for our affiliates' everyday business purposes" and that consumers could not limit this sharing. A total of 19 institutions still stated the same "for our affiliates to market to you," while 25 institutions stated the same practice "for nonaffiliates to market to you."

4.5 Misuse of the model privacy form

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

Figure 4: Bendena State Bank was among 15 institutions to state that it shares a particular type of information in one column, yet to state contradictorily "we don't share" in the subsequent column.

During our manual analyses of standardized notices during the development and verification of our parser (described in Appendix B), we noticed deviations from both the letter and the goal of the model privacy form. In this section, we discuss ways in which financial institutions deviated from the specification of the model privacy form [38].

4.5.1 Self-contradictory statements

As we iteratively improved our parser, we noticed self-contradictory statements in some institutions' standardized notices. One egregious example was answering "Yes" to "Does *institution name* share" and answering "We do not share" to "Can you limit this sharing?" in a single row. As shown in Figure 4, Bendena State Bank (`bendenastatebank.com`) was among 15 banks to do so. In a less confusing inconsistency, limiting sharing that does not occur does not make complete sense, yet the Monitor Bank (`monitorbank.com`) and many others answered "No" to "Does *name* share" and answered "Yes" to "Can you limit this sharing?" Other institutions used equally confusing wording to express this concept. For instance, in the "can you limit this sharing?" section of the disclosure table, Merrimac Bank (`merrimacbank.com`) stated "Yes, if we shared." These three kinds of logical inconsistencies and convoluted statements can potentially confuse consumers.

4.5.2 Typos and Omissions

While logical inconsistencies present a major issue in communicating with consumers, a number of more minor issues also cropped up. We designed our parser to be robust to small differences in wording. For instance, we ignored capitalization, considered most punctuation to be optional, and matched either "non-affiliates" or "nonaffiliates" throughout the notices. Nevertheless, typos in standardized notices caused many of our parsing "errors." For instance, Bank of Glen Ullin (`bankofglenullin.com`) misspelled "open an account" as "open *and* account." Cape Ann Savings Bank (`capeannsavings.com`) replaced "for our everyday business purposes" with "for *your* everyday business purposes." West Texas State Bank (`ebanktexas.com`) and others used "credit *card* bureaus" in place of "credit bureaus."

Financial institutions also commonly omitted required sections of the model privacy form, again causing problems for our parser. Middlesex Savings Bank (`middlesexbank.com`), for instance, included the "definitions" section, yet left out definitions of the terms "affiliates," "nonaffiliates," and "joint marketing."

Many institutions invented their own wording. For instance, Fisco (`fisco.com`) said that they collect information when customers "complete subscription documents" and "submit contributions or redemption requests," neither of which was among the 34 standardized terms. Similarly, Monitor Bank (`monitorbank.com`) said it collects "deposit account number(s)," "phone number," "address," "date of birth," and "loan number(s)." While it was not surprising that a financial institution might collect these data, none was listed in the specification [38]. Arguably, however, these institutions' more detailed disclosures might actually be more useful to consumers.

We also observed creative wording in the disclosure table. As a result of our iterative design process, our parser handled most of these variations. For instance, to communicate that one could not limit sharing since the insitution has no affiliates, different institutions wrote each of the following values in the relevant cell of the disclosure table: "*Name* has no affiliates," "We have no affiliates," "We don't share," "We do not share," "No," and "N."

Confusingly, institutions sometimes entirely rewrote rows of the disclosure table. City Securities (`citysecurities.com`), for instance, combined three rows of the disclosure table into the single row "For our affiliates' everyday business purposes or for our affiliates to market to you." They also invented a new row for the disclosure table: "For departing Financial Advisors to take limited customer information pursuant to The Broker Protocol*."

Furthermore, institutions commonly ignored the formatting of the model notice and omitted elements. For instance, Hampden Bank (`hampdenbank.com`), like a handful of others, included most of the information that would be contained in a standardized disclosure in their website privacy policy, yet left out most of the section headers and table formatting. Rather than including a table with the words "Why?...What?...How?" in one column, they created replacement statements like "How do we use the information we collect?" While the semantic meaning is the same, either a human or a computer program would have more trouble comparing institutions' policies, losing some of the benefits of providing privacy notices in a standardized format.

5 Discussion

A major advantage of all standardized privacy disclosures is that they enable the direct comparison of companies' privacy practices. In this study, we put this theoretical advantage into action and compared 6,191 U.S. financial institutions' privacy notices, in addition to privacy notices from institutions on consumer-advice lists of the 100 largest banks and 11 top credit card companies. In this section we discuss implications of these analyses.

5.1 Users' Choices

We found differences in data-sharing practices across financial institutions, even within institutions of the same type. Some institutions were more privacy-protective and did not share consumers' personal information for purposes like marketing even when they were permitted to do so. Other institutions did share consumers' personal information, yet allowed consumers to opt out of this data-sharing even when they were not required to offer an opt-out. These results suggest that informed consumers could have the opportunity to select institutions with data practices that match their privacy expectations.

An important consideration in supporting consumers who wish to do business with more privacy-protective institutions is how consumers might identify the institutions with better privacy practices. For small-scale comparisons, the standardized layout of the model privacy form has huge advantages over traditional, non-standardized privacy policies. Because the same information is located in the same place on each standardized notice, consumers can directly compare two or more institutions' privacy practices by placing these institutions' standardized notices next to each other.

While the possibility of consumers choosing financial institutions based in part on privacy practices seems promising, the lack of a simple mechanism for a consumer to make large-scale privacy comparisons or perform open-ended searches has been a major barrier. During the course of this project, we felt it would be helpful if a consumer could go to a website and have

the ability to say, "I currently bank at Company X. Please tell me about competing banks in the same geographic area that are more privacy-protective." To this end, we built such an interactive website (`http://cups.cs.cmu.edu/bankprivacy`) to help consumers search for or compare financial institutions. The predictable structure of the standardized notices enabled our construction of an automated parser, which was the first step in enabling such an online database.

In addition to helping consumers, the interactive website we built can assist regulators in taking stock of the prevalence of different practices across the financial industry. Similarly, regulators can use our online database to uncover idiosyncratic behaviors by particular institutions, as well as to examine practices by institutions in different regions of the country or institutions that meet particular criteria. Over the course of this project, we were surprised to learn that regulators do not appear to have previously examined the privacy practices stated in institutions' standardized notices on any sort of large scale in part due to lacking an easy mechanism to make such comparisons.

With information about institutions' privacy practices in a more accessible, standardized format, one can imagine financial institutions with consumer-friendly privacy practices using these practices as a competitive advantage. In past studies, consumers have even paid a premium price to purchase items from companies with more consumer-friendly privacy practices [47], and it stands to reason that they might similarly favor financial institutions with exemplary privacy practices. Both industry and policy makers could benefit from future research investigating consumers' privacy preferences in the financial domain. Results from such research can assist the shaping of companies' practices and mandated requirements.

While consumers armed with sufficient information do appear to have privacy choices for many types of financial institutions, there are some types of institutions for which institutions consistently share data without offering an opt-out. For example, consumers looking for a credit card company would have very limited options since all the credit card companies in our study share data for their own marketing purposes and share data on transactions and

experiences with affiliates without offering opt-out choices. Most of these companies also share data for joint marketing without opt-outs.

5.2 The Role of Regulators

Our large-scale analysis enabled us to observe how financial regulations impact consumer privacy protections in practice. Many institutions did not provide opt-outs for the three types of data sharing for which they were not required to offer an opt-out. In these three cases, between 158 and 561 institutions provided an opt-out when sharing data, providing consumers choice even when not required to do so. Between 1,816 to 4,507 institutions did not share consumer data at all for each of these three purposes. In contrast, between 1,323 and 3,823 institutions shared data for each of these purposes without offering an opt-out. This practice is permitted, yet less consumer-friendly.

Limitations of Standardized Notices. We found some issues with the specification of the model privacy form itself. For instance, when specifying what personal information they collect, institutions were mandated to list "Social Security number" and exactly 5 other types of information chosen from a list of 23 possibilities. Similarly, they were required to choose exactly 5 events from a list of 34 possible occasions on which they collect personal information. A glaring issue with these two lists of possibilities is that the types of information and events on the lists were fairly obvious. Consumers probably would not be surprised if their bank collected all 23 types of information on all 34 occasions listed. Indeed, a greater cause for concern might be if, for example, a bank chose *not to* collect a customer's "account balance" when he or she "used his or her credit or debit card." This realization suggests that these particular parts of the model privacy form are not very informative to consumers, who would likely care more about unexpected or non-obvious collection practices.

Short, standardized notices have been suggested as the top layer in a "layered" privacy notice, which has been advocated by both industry groups and regulators [1]. Layered notices bring the most salient information to the forefront of a consumer's attention, yet allow the

consumer to obtain additional information easily, such as with a single click. However, the model privacy form has not been designed as a layered notice. The form arbitrarily truncates some categories of information, yet no additional information is made available about an institution's data-collection practices.

This issue is compounded by the manner in which institutions appear to be using the model privacy form. Rather than presenting the model privacy form as a supplement highlighting important points of a full-length privacy policy, the model privacy form replaced full-length policies for many of the institutions we examined. Even though full-length privacy policies are too long for average consumers to read [33], the complete absence of a full-length policy means that institutions do not disclose many of their privacy practices should privacy advocates or other experts choose to inspect them. The specification of the model privacy form [38] notes that "financial institutions may rely on [the model privacy form] as a safe harbor to provide disclosures." It is possible that this safe-harbor provision substantially reduces consumer awareness of privacy practices since institutions are required only to disclose some, rather than all, of their privacy practices on this short-form notice. While we believe the availability of short-form notices to be a good thing for consumers, we also believe that traditional privacy policies should still be made available.

Compliance and Oversight. Standardized notices can also make oversight of privacy disclosures more efficient. Because the standardized notices provided under the Gramm-Leach-Bliley Act are now posted online by many financial institutions we were able to automate the process of collecting and evaluating them. We detected notices with stated sharing practices in apparent violation of United States law. For three of these data-sharing purposes listed in the disclosure table, institutions were required to provide consumers a way to limit sharing [38]. In violation of the law, more than one hundred institutions said they shared data for these purposes, yet reported that consumers could not limit sharing. When we contacted institutions for which this was the case, some of them explained that the sharing practices they were disclosing annually to their customers were not their actual practices.

Although they amended their standardized notices accordingly, these cases make us question to what extent consumers could rely on privacy notices to evaluate companies' actual practices, and to what extent stricter regulations and enforcement are necessary. These results also call into question current oversight mechanisms for financial institutions' privacy practices. We suggest that oversight institutions like the Consumer Financial Protection Bureau (CFPB) use tools similar to those we developed for our research.

Incentives to Use Standardized Notices. Given the benefits demonstrated through this work, we believe that regulators should continue incentivizing companies to use standardized notices online. In fact, the CFPB is currently seeking the amendment of GLBA to create such incentives. Companies may be incentivized to use online standardized notices if they can use those notices instead of delivering paper notices. Specifically, if there is an online communication mechanism already established with a customer, the company may not need to deliver a paper notice as long as the customer is provided with a conspicuous link to the online notice. A pointer to the online notice can be provided when monthly statements or other notices are delivered to the customer, either via postal mail or email. If a particular customer does not currently communicate electronically with his or her financial institution, or if the company does not have a website, the company would still be required to provide a paper notice. While it is important to make sure that customers without Internet access have the opportunity to learn about and opt out of sharing practices, requiring all financial institutions with websites to post a standardized notice online would benefit all parties. If the company already has an online presence, adding an online standardized notice does not represent significant additional overhead.

5.3 Online Notices and Implementation Issues

Currently, the standardized notice tends to be delivered as a static PDF, static HTML page, or static print-out mailed to consumers. We believe there are a number of opportunities being missed for making online standardized notices interactive. In addition to the benefits

mentioned above, online notices can be personalized, enable online opt-out methods, and provide links to additional information. For example, users may be able to see a notice that applies to their particular state of residence. We have found that institutions often use the "Other Important Information" section in the model privacy form to specify exceptions to sharing practices for residents of different states. An online notice can easily provide a drop-down menu allowing customers to select their state of residence to view the applicable privacy notice. Furthermore, an online privacy notice can show whether the consumer's opt-out right is currently being exercised.

We believe that customers' privacy can further be improved if, in addition to traditional offline methods such as mail and phone, online opt-out methods were offered widely. Due to space limitations, the paper-based standardized format does not allow companies to list all the data types that they collect, all the methods that they use to collect information, and the names of the entities with whom they share customers' personal information. In an online notice, this additional and relevant information can be available just one click away from the baseline notice.

Through our large-scale analysis of financial institutions' standardized notices we found that many institutions deviate from the standard model requirements in various ways. For example, some companies use slightly different data types from what is required by the model form to refer to types of personal information that they collect. Some omit information such as the date when the notice was created, or the lists of their affiliates, non-affiliates and joint marketers. We also found inconsistencies in the sharing table entries, including companies listing a "Yes" under the sharing column, but then stating in a self-contradiction "we don't share" under the opt-out column. Also, some companies that claim to offer opt-outs don't offer any specific opt-out method under the "to limit our sharing" section.

We believe that many of these problems and inconsistencies related to institutions generating their standardized notice could be mitigated if a government agency provided an interactive tool that companies could use to generate standardized notices for online posting.

The PDF form builder currently available does not prevent these problems. We hypothesize that the small and often understaffed structure of credit unions may have contributed to their high rate, relative to larger institutions, of posting standardized notices that violate the FCRA or GLBA opt-out requirements. A more guided process for building a standardized notice could help to mitigate these problems. To this end, students at Carnegie Mellon have been developing prototype online form builders that are available alongside our interactive database at `http://cups.cs.cmu.edu/bankprivacy/`.

We faced three additional problems during our analysis of financial institutions' privacy policies: the lack of a comprehensive and publicly available database of financial institutions and their web addresses; the lack of a consistent directory path where online standardized notices are located; and a lack of consistency in the use of the standardized format. We believe that requiring companies to provide their websites URLs (if they have one) to the CFPB or appropriate authority, and subsequently making a centralized database with that information publicly available, would better enable the development of tools like our bank privacy website. To further facilitate the collection and analysis of online notices on a large scale, we suggest that companies be required to post those notices in a well-known and standardized location, such as `institution-name.com/notices/privacy/`. Finally, an online version of the standard notice could easily include a computer-readable section that would facilitate automated collection, comparison, and analysis, mitigating the errors introduced by our somewhat ad-hoc parsing methods.

5.4 Study Limitations

The automatic retrieval and parsing of standardized notices allowed us to perform a large-scale analysis of financial institutions' privacy notices, yet introduced some limitations. As we did not have access to the domain names of most of the financial institutions in our original list, we used the conservative heuristics described in Section A.1 to first find institutions' domain names and then retrieve their corresponding notices if they had one. We were able

to retrieve notices from about one-third of companies in the original set. We randomly selected 100 companies from the set of those from which we could not automatically retrieve a standardized notice and manually attempted to retrieve domain names and notices from them. We manually found notices from 40 of those 100 companies, suggesting that our heuristics could be improved. However, finding those notices was a time consuming task and required several steps that may not be possible to fully automate. Crowd sourcing could be an alternative, but likely an expensive one as it is time consuming to find notices. A possibility is to use crowd sourcing to find companies' domain names, which is less time consuming, and then use those domain names to automatically attempt to retrieve notices. We also found that small companies (e.g., credit unions) were less likely to have both Internet presence and use standardized notices and that large companies (e.g., BHC) often have multiple subsidiaries with different domains that we were unable to find automatically. However, most of these subsidiaries are not consumer facing and tend to have the same privacy policy as the parent company. In sum, our sample of notices may be slightly biased towards larger companies as they are more likely to use standardized notices. At the same time, we may have missed very large companies (e.g., BHC) that use different domain names for their subsidiaries. Nevertheless, our sample of notices was heterogeneous enough to allow us to statistically compare financial institutions of different types.

Finally, we relied on privacy notices to evaluate and compare companies' practices; however we don't know whether or not those notices accurately reflect real practices. Transparency through privacy notices can therefore only be improved if appropriate accountability mechanisms are in place.

6 Acknowledgements

Funding for this project was provided in part by the National Science Foundation under its Secure and Trustworthy Computing (SaTC) initiative grant 1330596 for "TWC SBE:

Option: Frontier: Collaborative: Towards Effective Web Privacy Notice and Choice: A Multi-Disciplinary Prospective." This research was also conducted with government support under and awarded by DoD, Air Force Office of Scientific Research, National Defense Science and Engineering Graduate (NDSEG) Fellowship, 32 CFR 168a.

We would like to thank Kelly Idouchi, Manya Sleeper, James T. Graves, and Celine Berger for their contributions to this project. Similarly, we thank Chris Hoofnagle, Daniel Solove, and the attendees of the 2014 Privacy Law Scholars Conference (PLSC) for valuable feedback on an earlier version of this work.

References

[1] Ten steps to develop a multilayered privacy notice. The Center for Information Policy Leadership, 2007.

[2] A. I. Antón, J. B. Earp, Q. He, W. Stufflebeam, D. Bolchini, and C. Jensen. Financial privacy policies and the need for standardization. *IEEE Security & Privacy*, 2(2):36–45, 2004.

[3] K. Badenhausen. America's best and worst banks 2012. Forbes, `http://www.forbes.com/sites/kurtbadenhausen/2012/12/18/full-list-americas-best-and-worst-banks-2012/`, December 2012.

[4] L. F. Cranor. *Web privacy with P3P*. O'Reilly, 2002.

[5] L. F. Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law*, 10:273–307, 2012.

[6] L. F. Cranor, S. Egelman, S. Sheng, A. M. McDonald, and A. Chowdhury. P3P deployment on websites. *Electronic Commerce Research and Applications*, 7(3):274–293, 2008.

[7] L. F. Cranor, K. Idouchi, P. G. Leon, M. Sleeper, and B. Ur. Are they actually any different? Comparing thousands of financial institutions' privacy practices. In *Workshop on the Economics of Information Security (WEIS)*, June 2013.

[8] Fair and Accurate Credit Transactions Act. Pub. L. No. 108-159, 117 Stat. 1952, 2003.

[9] FDIC. Institution directory. `http://www2.fdic.gov/IDASP/`, Accessed July 26, 2014.

[10] FDIC. Trust examination manual. `http://www.fdic.gov/regulations/examinations/trustmanual/section_10/section_x.html#A`, Accessed June 1, 2013.

[11] Federal Reserve. Federal reserve's financial institution types. `http://www.ffiec.gov/nicpubweb/content/help/LinkAdvancedSearchAllinstitutions.htm`, Accessed July 26, 2014.

[12] Federal Trade Commission. Privacy online: A report to Congress, June 1998.

[13] E. H. Freeman. Privacy notices under the Gramm-Leach-Bliley Act. *Information Systems Security*, 12(2):5–9, 2003.

[14] FTC. Privacy of consumer financial information; final rule. Federal Register, May 2000.

[15] M. Furletti and S. Smith. Financial privacy: perspectives from the payment cards industry. *Payment Cards Center Discussion Paper*, 2003.

[16] L. Garrison, M. Hastak, J. M. Hogarth, S. Kleimann, and A. S. Levy. Designing evidence-based disclosures: A case study of financial privacy notices. *Journal of Consumer Affairs*, 46(2):204–234, 2012.

[17] M. Graber, D. D'Alessandro, and J. Johnson-West. Reading level of privacy policies on Internet health web sites. *Journal of Family Practice*, 2002.

[18] Gramm-Leach-Bliley Act. Pub. L. No. 106-102, 113 Stat. 1338, 1999.

[19] O. Ireland and R. Howell. The fear factor: Privacy, fear, and the changing hegemony of the American people and the right to privacy. *North Carolina Journal of International Law and Commercial Regulation*, 29:671, 2003.

[20] E. J. Janger and P. M. Schwartz. Gramm-Leach-Bliley Act, information privacy, and the limits of default rules, the. *Minnesota Law Review*, 86, 2001.

[21] J.D. Power & Associates. 2012 U.S. credit card satisfaction study. Press release, `http://www.jdpower.com/content/press-release/xdTqU1T/2012-u-s-credit-card-satisfaction-study.htm`, August 2012.

[22] C. Jensen and C. Potts. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 471–478, 2004.

[23] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)*, pages 4:1–4:12, 2009.

[24] Kleimann Communication Group Inc. Evolution of a prototype financial privacy notice. `http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf`, February 2006.

[25] Kleimann Communication Group Inc. A report on validation testing results. `http://www.ftc.gov/reports/financial-privacy-notice-report-validation-testing-results-kleimann-validation-report`, February 2009.

[26] J. M. Lacker. The economics of financial privacy: to opt out or opt in? *Economic Quarterly-Federal Reserve Bank of Richmond*, 88(3):1–16, 2002.

[27] P. G. Leon, L. F. Cranor, A. M. McDonald, and R. McGuire. Token attempt: The misrepresentation of website privacy policies through the misuse of P3P compact policy tokens. In *Proceedings of the 9th annual ACM Workshop on Privacy in the Electronic Society (WPES)*, pages 93–104, 2010.

[28] A. Levy and M. Hastak. Consumer comprehension of financial privacy notices. Interagency Notice Project, `http://ftc.gov/privacy/privacyinitiatives/Levy-Hastak-Report.pdf`, December 2008.

[29] J. R. Macey. The business of banking: Before and after Gramm-Leach-Bliley. *Journal of Corporation Law*, 25:691, 1999.

[30] Macro International Inc. Mall intercept study of consumer understanding of financial privacy notices: Methodological report. `http://www.ftc.gov/reports/quantitative-research-macro-international-report`, September 2008.

[31] K. J. Mathews. *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*. Practicing Law Institute, 2013.

[32] P. L. McCorkell and A. M. Smith. Fair Credit Reporting Act update—2008. *Business Lawyer*, 64(2):579–591, 2009.

[33] A. M. McDonald and L. F. Cranor. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3):540–565, 2008.

[34] R. J. McMahon. Developments in the Gramm-Leach-Bliley Act during 2005–06: An overview of important changes in case law and pending legislation. *I/S: A Journal of Law and Policy for the Information Society*, 2(3):737–759, 2006.

[35] R. Nader et al. Joint petition for rulemaking on privacy notices. http://www.ftc.gov/bcp/workshops/glb/comments/, July 2001.

[36] A. L. Negroni and J. P. Kromer. Gramm-Leach-Bliley: Tip of the privacy iceberg. *Banking Law Journal*, 118(10):958–969, 2001.

[37] G. T. Nojeim. Financial privacy. *New York Law School Journal of Human Rights*, 17:81, 2000.

[38] OCC, Federal Reserve System, FDIC, OTS, NCUA, FTC, CFTC, and SEC. Final model privacy form under the Gramm-Leach-Bliley Act. *Federal Register*, 74:62890–62994, December 1, 2009.

[39] OECD. Guidelines on the protection of privacy and transborder flows of personal data, September 1980.

[40] J. C. Schiller. Informational privacy v. the commercial speech doctrine: Can the Gramm-Leach-Bliley Act provide adequate privacy protection. *Commlaw Conspectus*, 11:349, 2003.

[41] X. Sheng and L. F. Cranor. An evaluation of the effect of us financial privacy legislation through the analysis of privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 2:943, 2005.

[42] B. Shull. Banking, commerce and competition under the Gramm-Leach-Bliley act. *Antitrust Bulletin*, 47:25, 2002.

[43] P. P. Swire. Surprising virtues of the new financial privacy law, the. *Minnesota Law Review*, 86:1263, 2001.

[44] P. P. Swire. Efficient confidentiality for privacy, security, and confidential business information. *Brookings-Wharton Papers on Financial Services*, 2003(1):273–310, 2003.

[45] Z. Tang, Y. J. Hu, and M. D. Smith. Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems*, 24(4):153–173, 2008.

[46] Terms of Service; Didn't Read. `http://tosdr.org/`.

[47] J. Y. Tsai, S. Egelman, L. F. Cranor, and A. Acquisti. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2):254–268, June 2011.

[48] B. Ur, M. Sleeper, and L. F. Cranor. {Privacy, Privacidad, Приватност} policies in social media: Providing translated privacy notice. *I/S: A Journal of Law and Policy for the Information Society*, 9(2), 2013.

[49] L. J. White. The Gramm-Leach-Bliley Act of 1999: A bridge too far—or not far enough. *Suffolk University Law Review*, 43:937, 2009.

A Automatic retrieval of privacy notices

This section provides additional methodological details about our automated collection of privacy notices.

A.1 Searching for standardized notices

To search for a standardized notice from an institution without exhaustively crawling all parts of each institution's website, we chose to perform an automated Google query. To minimize the chance of accidentally retrieving another institution's standardized notice, particularly in light of the large number of financial institutions with similar names, we restricted each query to a financial institution's website domain using Google's *as_sitesearch* parameter. Among the 6,781 institutions in the FDIC list, 6,409 institutions listed a website URL. For these institutions, we considered the domain of this URL to be that institution's only official domain. The remaining financial institutions, as well as all of the credit unions, did not include a website URL among the metadata we retrieved from regulators. To determine the website domain for that institution, we performed an automated Google query of the string "*Institution name*, *City*, *State*" and took the domain of the first result to be that institution's domain. This heuristic is imperfect, yet we believe it conservatively minimizes false associations (incorrectly attributing a standardized notice to the wrong institution) at the expense of increasing the number of false negatives (not finding notices for institutions that have them available).

Armed with a website domain for an institution, we performed an automated Google Query using the search string "What does *institution name* do with your personal information," inserting the institution's name. This string was the header of the model privacy form [38], leading us to use it as the query. We disabled query autocomplete and the geographic localization of search results using Google's *complete* and *pws* parameters, respectively. For each Google query, we recorded the first page of results, containing between

zero and ten links for each institution.

We then automatically downloaded these zero to ten items linked from the first page of Google results for each institution. In our pilot testing, we found standardized notices in both HTML (webpage) and PDF formats. We therefore supported both filetypes. To provide a consistent input for our parser and to record the formatting for future display to consumers, we automatically saved both types of files in the PDF format. We downloaded each webpage using the wkhtmltopdf utility running on Ubuntu Linux.[6] The wkhtmltopdf utility renders a webpage using the webkit engine and then saves this output to PDF. In practice, we found that some links redirected automatically to PDF files, which would cause wkhtmltopdf to return a "failed loading page" error. If our program received this message, or if the URL itself ended in the extension *.pdf*, we instead fetched the PDF using the Linux utility Wget.[7] To prevent the crawler from stalling for long periods of time, we instituted a 60-second timeout that abandoned downloading a page if the download took more than 60 seconds.

A.2 Identification of standardized notices

From the 10 or fewer files downloaded for each financial institution, we chose the single file that had the largest number of features of the model privacy form and considered that to be the institution's standardized notice. If none of the files downloaded matched a substantial fraction of features of the model privacy form, we concluded that we did not have a standardized notice for that institution.

Our first step in making this determination was to extract the text from each PDF file using the Linux utility pdftotext[8] to convert PDF files to plaintext. This utility attempts to maintain the relative layout of text. Because the spacing is not always maintained perfectly, particularly for tables, we designed our parser to be robust to text from different columns

[6] wkhtmltopdf. `http://wkhtmltopdf.org/`
[7] GNU Wget. `https://www.gnu.org/software/wget/`
[8] Pdftotext. `http://linux.die.net/man/1/pdftotext`

of a table flowing together. Furthermore, to eliminate false negatives in parsing caused by unexpected whitespace being inserted in the conversion from PDF to plaintext, we removed all whitespace and non-ASCII characters before parsing the document.

The next step involved selecting at most one file per institution. We selected 25 phrases that, according to the model privacy form [38], should always appear in a standardized notice, spread approximately evenly throughout the document. For each file, we searched for all 25 phrases and recorded the number of phrases found as the file's "score." To weed out files that did not appear to be based on the model privacy form, we set a cutoff score of 21, thereby eliminating all files missing 20% or more of these expected keywords and phrases. For each institution, we chose the remaining file with the highest score, if any, to give preference to the most complete disclosure that we found for each institution. In the case of a tie, we chose the file that appeared first in the Google results.

B Verification of parsing

This section provides more detail on our manual verification of our parser's accuracy. We also provide greater detail about our parsing of the disclosure table.

The bank name and the list of six types of personal information an institution collects were both parsed correctly for all 50 institutions we manually verified (100% accuracy). We correctly parsed the document's revision date for 48 of 50 institutions (96%). One of the remaining two institutions used an unexpected hyphen in its revision date (05-2011), which we had not accounted for, while the other institution simply included a bare date in the corner of the form without the required "Rev." or similar text. We correctly identified the "who we are" section for 49 of 50 institutions (98%), missing an institution who reworded this section's header as "who are we?"

We correctly parsed the "to limit sharing" section for 50 of 50 institutions (100%), but we encountered two problems when parsing mail-in forms. Although we correctly parsed

48 of 50 institutions' mail-in forms (96%), or lack thereof, we did not recognize one mail-in form that was embedded as an image file, foiling our conversion from pdf to text. We did not recognize a second mail-in form that lacked a header, instructions, or indication that the form was detachable; instead, the form simply included fields for the consumer to fill in, as well as a series of checkboxes for limiting sharing.

We parsed other sections with slightly lower accuracy. For instance, our parser correctly identified how the institution collects information for 46 of 50 institutions (92%). All errors, however, were caused by the financial institutions deviating in small or large ways from the model privacy form. For instance, one bank rewrote "your investment or retirement portfolio" as "your investments or retirement portfolio," while another bank rewrote "pay your bills" as "pay bills online."

In our manual verification of 50 notices, we parsed 45 of 50 institutions' complete disclosure tables with perfect accuracy across all 6–7 rows (90%). For the five remaining institutions, we correctly parsed all except one or two of the rows of the disclosure table. In four of the five cases, we reported as missing one or two sections that were actually included. In three cases the errors were due to differences in spacing. In two cases, the company unexpectedly omitted a required row of the table, and in another case the company centered a column of the table vertically. In one other case we had a subtle error in our regular expression that lead to a mismatch in text, and in the final case, the institution rewrote "for our everyday business purposes" to read "for your everyday business purposes."

We also correctly parsed the "definitions" section for 45 of the 50 institutions we examined (90%). In three cases, institutions' nonstandard use of the model privacy form caused the incorrect parsing. One institution reworded the specified "doesn't have" as "don't have," another embedded the phrase "we have no affiliates" as an image even though the rest of the section was written as text, and the third institution omitted the definition of "joint marketing" entirely. Vertical centering in tables caused the remaining two errors.

Some individual elements were parsed at a lower rate; manual inspection reveals, however,

that these missing elements were often missing from the standardized notice. For instance, we parsed the name of the bank from the header "What does *institution name* do with your personal information?" for 5,973 notices. Many of the policies for which this section was not recognized seemed to omit this section, often replacing it with the institution's logo. The "Who we are...Who is providing this notice?" section was observed at an even lower rate; our parser found 3,405 of notices to contain this section. The specification for the model privacy form notes that "an institution may omit this FAQ only when one financial institution is providing the notice and that institution is identified in the title" [38]. We did not attempt to verify that this case applied for all institutions that omitted this section.

Similarly, a revision date was recognized for only 4,530 of the policies, even though we accepted a number of different phrasings for this section based on manual inspection of policies that seemed to lack revision dates. The model privacy form [38] included *Rev.* for the revision date. We also accepted the following text: *Revised*, *Privacy Notice:*, and *Revision Date*. All of these matches were case insensitive, and we treated all punctuation as optional. We supported a wide range of formats for dates, including YY/MM/DD and MM/DD/YY formats. We allowed the year to be specified with either two or four digits, we permitted only the month and year to be specified, we allowed either forward slashes or periods as delimiters, and we also recognized dates where the month was written out in words and spaces were used as the delimiter.

C Sharing practices of large banks

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	0	0.0%	0	0.0%	86	100%	0	0.0%
For our marketing purposes– to offer our products and services to you	3	3.5%	11	12.8%	72	83.7%	0	0.0%
For joint marketing with other financial companies	19	22.1%	13	15.1%	54	62.8%	0	0.0%
For our affiliates' everyday business purposes– information about your transactions and experiences	9	10.5%	5	5.8%	72	83.7%	0	0.0%
For our affiliates' everyday business purposes– information about your creditworthiness *[Opt-out mandatory]*	35	40.7%	51	59.3%	0	0.0%	0	0.0%
For our affiliates to market to you *[Opt-out mandatory; row may be omitted in certain cases]*	14	16.3%	55	64%	0	0.0%	17	19.7%
For nonaffiliates to market to you *[Opt-out mandatory]*	71	82.6%	14	16.3%	1	1.2%	0	0.0%

Table 8: A summary of data-sharing practices among the 86 of Forbes' 100 largest banks for which we found a standardized notices [3].

Institution name	Our marketing	Joint marketing	Affiliates: Transactions	Affiliates: Creditworthiness	Affiliates' marketing	Nonaffiliates' marketing
1st Source	No opt-out	Don't share	No opt-out	Opt-out	Opt-out	Don't share
Associated Banc-Corp	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
BancFirst	Don't share	Don't share	Don't share	Don't share	Missing	Don't share
BancorpSouth	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Bank of America	No opt-out	No opt-out	No opt-out	Opt-out	Missing	Opt-out

Continued from previous page

Institution name	Our marketing	Joint marketing	Affiliates: Transactions	Affiliates: Creditworthiness	Affiliates' marketing	Nonaffiliates' marketing
Bank United	Opt-out	No opt-out	No opt-out	Don't share	Missing	Don't share
BB&T	No opt-out	No opt-out	No opt-out	Opt-out	No opt-out	Don't share
BBCN Bancorp	No opt-out	No opt-out	No opt-out	Don't share	Don't share	Don't share
Beneficial Bank	No opt-out	Don't share	No opt-out	Opt-out	Opt-out	Don't share
BOK Financial	No opt-out	No opt-out	No opt-out	Don't share	Opt-out	Opt-out
Brookline Bank	No opt-out	No opt-out	No opt-out	Don't share	Don't share	Don't share
Capital Bank	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Capital One	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Cathay Bank	No opt-out	No opt-out	No opt-out	Don't share	Don't share	Don't share
Central Bancompany	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Chase	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Chemical Bank	No opt-out	Don't share	Don't share	Don't share	Missing	Don't share
Citi	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Citizens Republic Bancorp	Opt-out	Opt-out	No opt-out	Opt-out	Opt-out	Opt-out
City National Bank	No opt-out	No opt-out	No opt-out	Don't share	Missing	Don't share
Cole Taylor Bank	Opt-out	Opt-out	No opt-out	Don't share	Opt-out	Don't share
Columbia State Bank	No opt-out	No opt-out	No opt-out	Don't share	Missing	Don't share
Comerica	No opt-out	Opt-out	No opt-out	Opt-out	Opt-out	Don't share
Commerce Bank	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out	Don't share
Community Bank	No opt-out	No opt-out	No opt-out	Don't share	Opt-out	Don't share
CVB Financial	No opt-out	Don't share	Don't share	Don't share	Missing	Don't share
Doral	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
East West Bank	No opt-out	Don't share	No opt-out	Don't share	Missing	Don't share
Farmers & Merchants	No opt-out	Don't share	Don't share	Don't share	Don't share	Don't share

Continued from previous page

Institution name	Our marketing	Joint marketing	Affiliates: Transactions	Affiliates: Creditworthiness	Affiliates' marketing	Nonaffiliates' marketing
Fifth Third Bank	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
First Bancorp	No opt-out	No opt-out	Don't share	Don't share	Missing	Don't share
First Citizens Bancorp	Opt-out	Opt-out	No opt-out	Opt-out	Opt-out	Don't share
First Citizens Bancshares	Opt-out	Opt-out	No opt-out	Opt-out	Opt-out	Don't share
First Commonwealth Financial	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
First Financial Bank	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out	Don't share
First Horizon	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
First Interstate Bank	No opt-out	No opt-out	No opt-out	Don't share	Missing	Don't share
FirstMerit	Opt-out	Opt-out	No opt-out	Opt-out	Opt-out	Opt-out
First National Bank of Nebraska	No opt-out	No opt-out	No opt-out	Don't share	Missing	Don't share
First Niagara	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
First Republic Bank	No opt-out	Don't share	No opt-out	Opt-out	Opt-out	Don't share
First Midwest	No opt-out	No opt-out	No opt-out	Don't share	Don't share	Don't share
FNB Corporation	Opt-out	Opt-out	No opt-out	Opt-out	Opt-out	Don't share
Fulton Financial Corporation						
Hancock Holding	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Heartland Financial	Opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Huntington	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Iberia Bank	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Independent Bank	No opt-out	Opt-out	No opt-out	Don't share	Missing	Don't share
International Bancshares	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Investors Bank	No opt-out	Opt-out	No opt-out	Opt-out	Opt-out	Don't share

Continued from previous page

Institution name	Our marketing	Joint marketing	Affiliates: Transactions	Affiliates: Creditworthiness	Affiliates' marketing	Nonaffiliates' marketing
Keycorp	No opt-out	No opt-out	No opt-out	Opt-out	Missing	Don't share
M&T Bank Corporation	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
MB Financial	Opt-out	Opt-out	No opt-out	Don't share	Opt-out	Don't share
National Bank Holding	No opt-out	No opt-out	Don't share	Don't share	Missing	Don't share
National Penn Bancshares	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
New York Community Bancorp	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Northern Trust	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	No opt-out
Old National	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out	Don't share
Oriental Financial	No opt-out	Don't share	No opt-out	Opt-out	Opt-out	Don't share
Pacific Western	No opt-out	Don't share	No opt-out	Don't share	Don't share	Don't share
Park National Bank	No opt-out	No opt-out	No opt-out	Don't share	Don't share	Don't share
PNC Bank	No opt-out	Opt-out	No opt-out	Opt-out	Opt-out	Don't share
Popular	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Private Bancorp	No opt-out	No opt-out	No opt-out	Don't share	Don't share	Don't share
Prosperity Bank	No opt-out	No opt-out	Don't share	Don't share	Don't share	Don't share
Provident Financial	No opt-out	Opt-out	Opt-out	Opt-out	Opt-out	Don't share
Regions Financial	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Signature Bank	Don't share	Don't share	No opt-out	Don't share	Missing	Don't share
Susquehanna Bank	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out	Opt-out
Synovus Financial	No opt-out	Don't share	No opt-out	Don't share	Don't share	Don't share
Texas Capital Bank	Don't share	Don't share	Don't share	Don't share	Missing	Don't share
Trustmark	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
U.S. Bank	No opt-out	Don't share	No opt-out	Opt-out	Missing	Don't share
UMB Financial	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share

Continued from previous page

Institution name	Our marketing	Joint marketing	Affiliates: Transactions	Affiliates: Creditworthiness	Affiliates' marketing	Nonaffiliates' marketing
Umpqua Bank	No opt-out	No opt-out	No opt-out	Don't share	Don't share	Don't share
United Bancshares	Opt-out	No opt-out	No opt-out	Don't share	Opt-out	Don't share
United Community Bank	No opt-out	No opt-out	No opt-out	Don't share	Don't share	Don't share
Valley National Bancorp	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Webster Bank	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Wells Fargo	No opt-out	Don't share	No opt-out	Opt-out	Opt-out	Don't share
WesBanco	Opt-out	Opt-out	No opt-out	Don't share	Opt-out	Don't share
West America	No opt-out	Don't share	No opt-out	Don't share	Missing	Don't share
Western Alliance Bancorp	No opt-out	Don't share	Don't share	Don't share	Don't share	Don't share
Wintrust Financial	No opt-out	Don't share	Opt-out	Opt-out	Opt-out	Don't share
Zions First National Bank	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share

Table 9: The detailed sharing practices of each of the 86 financial institutions on Forbes' 100 largest banks [3] for which we found a standardized notice.

D Sharing practices of credit card companies

Institution name	Our marketing	Joint marketing	Affiliates: Transactions	Affiliates: Creditworth.	Affiliates' marketing	Nonaffiliates' marketing
Capital One; Chase; Discover Bank; HSBC	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Opt-out
Bank of America; Citi	No opt-out	No opt-out	No opt-out	Opt-out	Missing	Opt-out
American Express	No opt-out	No opt-out	No opt-out	Opt-out	Opt-out	Don't share
Barclays Bank	No opt-out	Opt-out	No opt-out	Opt-out	Missing	Don't share
GE Capital	No opt-out	Don't share	No opt-out	Don't share	Missing	Don't share
U.S. Bank	No opt-out	Don't share	No opt-out	Opt-out	Missing	Don't share
Wells Fargo	No opt-out	Don't share	No opt-out	Opt-out	Opt-out	Don't share

Table 10: Sharing practices for reasons other than "our everyday business purposes" of credit card companies that appear on a J.D. Power & Associates list [21]. Capital One, Chase, Discover Bank, and HSBC are listed in a group because they have the same sharing practices. Similarly, Bank of America and Citi have the same sharing practices. We note that institutions differ in their sharing practices. For instance, GE Capital says that it does not share data for three of the purposes listed, whereas other institutions say they share for all purposes listed in the disclosure table.

E Institutions that Appear to Violate FCRA and GLBA

"**For our affiliates' everyday business purposes** – information about creditworthiness. This reason incorporates sharing information pursuant to section 603(d)(2)(A)(iii) of the FCRA. An institution that shares for this reason must provide an opt-out" [38]. The following institutions stated that they shared for this purpose, yet said that consumers cannot limit this sharing:

Credit Unions:

- 1st Financial Credit Union (1stfinancialfcu.org)
- Acadiana Medical Credit Union (mylcu.net)
- American Partners Credit Union (apfcu.com)
- Capstone Credit Union (capstonefcu.coop)
- Cherokee County Credit Union (cherokeecountyfcu.com)
- City Employees Credit Union (cecuknox.com)
- Clarkston Brandon Community Credit Union (cbccu.org)
- Clearance Community And Schools Credit Union (ccsfcu.com)
- Community Financial Credit Union (yourlocalcreditunion.com)
- Coors Credit Union (coorscu.org)
- Credit Union South Credit Union (creditunionsouth.com)
- Destinations Credit Union Credit Union (destinationscu.org)
- Family Horizons Credit Union (familyhorizons.com)
- Fond Du Lac Credit Union (fdlcu.com)

- GR Consumers Credit Union (grccu.com)
- Greenville Credit Union (greenvillefcu.com)
- Hartford Healthcare Credit Union (hhcu.org)
- Highmark Credit Union (highmarkfcu.com)
- Homeport Credit Union (homeportfcu.com)
- Honor Credit Union (honorcu.com)
- Horizons North Credit Union (hncu.org)
- Houston Metropolitan Credit Union (hmefcu.org)
- Interstate Unlimited Credit Union (iufcu.org)
- Jersey Shore Credit Union (jerseyshorefcu.org)
- Keystone Credit Union (keystonecu.com)
- L And N Credit Union (lnfcu.com)
- Maryvale Schools Credit Union (maryvaleschoolsfcu.com)
- Nebraska Energy Credit Union (ne-fcu.org)
- Nuvista Credit Union (nuvista.org)
- PBC Credit Union (pbccu.coop)
- Pelican State Credit Union (pelicanstatecu.com)
- Penobscot County Credit Union (penobscotfcu.com)
- Pinnacle Credit Union (pinnaclecu.org)

- Proponent Credit Union (proponentfcu.org)
- Sisters Hospital Employees Credit Union (shefcu.org)
- Southern Credit Union (southernfederalcu.org)
- St. Agnes Employees Credit Union (stagnescu.com)
- St. Jules Credit Union (stjcu.com)
- The Florist Credit Union (thefloristfcu.org)
- West Branch Valley Credit Union (wbvfcu.org)

Other financial institutions:

- A.J. Smith Federal Savings Bank (ajsmithbank.com)
- Aquesta Bank (aquesta.com)
- Citizens State Bank of Loyal (csbloyal.com)
- Community Development Bank FSB (comdevbank.com)
- Community State Bank (bankcommunitystate.com)
- First County Bank (firstcountybank.com)
- Hometrust Bancshares Inc (hometrustbanking.com)
- Hyperion Bank (hyperionbank.com)
- Midwest Independent Bancshares Inc (mibanc.com)
- SunMark Community Bank (sunmarkbank.com)
- The Bank of Star Valley (bosv.com)

- West One Bank (westonebank.com)

"**For our affiliates to market to you**. This reason incorporates sharing information specified in section 624 of the FCRA. Institutions that include this reason must provide an opt-out of indefinite duration. An institution that is required to provide an affiliate marketing opt-out, but does not include that opt-out in the model form under this part, must comply with section 624 of the FCRA and 12 CFR Part 717, Subpart C, with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out." The following institutions stated that they shared for this purpose, yet said that consumers cannot limit this sharing:

Credit Unions:

- Acadiana Medical Credit Union (mylcu.net)
- Credit Union Of Denver (cudenver.com)
- Family Horizons Credit Union (familyhorizons.com)
- Hartford Healthcare Credit Union (hhcu.org)
- Healthcom Credit Union (healthcomfcu.org)
- Interstate Unlimited Credit Union (iufcu.org)
- Mountain America Credit Union (macu.com)
- Nebraska Energy Credit Union (ne-fcu.org)
- North Alabama Educators Credit Union (naecu.org)
- PBC Credit Union (pbccu.coop)
- Proponent Credit Union (proponentfcu.org)

- State Employees Credit Union (secufl.org)
- Velocity Community Credit Union (velocitycommunity.org)
- Winsouth Credit Union (winsouthcu.com)

Other financial institutions:

- Aquesta Bank (aquesta.com)
- Carolina Premier Bank (carolinapremierbank.com)
- Citizens State Bank of Loyal (csbloyal.com)
- Crest Savings Bank (crestsavings.com)
- Elmira Savings Bank (elmirasavingsbank.com)

"**For nonaffiliates to market to you**. This reason incorporates sharing described in section 6802(b)(1) of GLBA. An institution that shares personal information for this reason must provide an opt-out." The following institutions stated that they shared for this purpose, yet said that consumers cannot limit this sharing:

Credit Unions:

- Brownfield Credit Union (brownfieldfcu.com)
- Financial Center Credit Union (fccuburt.org)
- Franklin First Credit Union (franklinfirst.org)
- Goetz Credit Union (goetzcu.com)
- Harbor Credit Union (harborfcu.org)
- Hartford Healthcare Credit Union (hhcu.org)

- Heritage Valley Credit Union (heritagevalleyfcu.org)
- Lanier Credit Union (lanierfcu.org)
- Lower Columbia Longshoremen Credit Unio (lclfcu.org)
- Lubrizol Employees Credit Union (lzecu.org)
- Marisol Credit Union (marisolcu.org)
- North County Credit Union (northcountycu.org)
- Northwoods Community Credit Union (northwoodscu.com)
- Onomea Credit Union (onomeafcu.org)
- Perry Point Credit Union (perrypointfcu.com)
- Piedmont Credit Union Credit Union (piedmontcu.org)
- Priority One Credit Union (priorityonecu.org)
- Proponent Credit Union (proponentfcu.org)
- Queen Of Peace Arlington Credit Union (qpafcu.com)
- Reno City Employees Credit Union (rcefcu.com)
- San Diego Medical Credit Union (sdmfcu.org)
- San Mateo Credit Union (smcu.org)

Other financial institutions:

- Bank of Delight (bankofdelight.com)
- Northern Trust Company of New York (northerntrust.com)
- The First National Bank of Pontotoc (1stnbpontotoc.com)

F Logistic Regression Models

We built logistic regression models to investigate the factors correlated with the different sharing practices. These models were built only for the subset of FDIC-insured institutions for which we had additional institutions' characteristics. The OCC districts as used in our logistic regression models are: **Northeastern**: Connecticut, Delaware, DC, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Puerto Rico, Rhode Island, U.S. Virgin Islands, Vermont, Virginia, and West Virginia; **Southern**: Alabama, Arkansas, Florida, Georgia, Louisiana, Mississipi, Oklahoma, Tennessee and Texas; **Central**: Illinois, Indiana, Kentucky, Michigan, Minnesota, Ohio, and Wisconsin; and **Western**: Alaska, American Samoa, Arizona, California, Colorado, Guam, Hawaii, Idaho, Iowa, Kansas, Missouri, Montana, Nebraska, Nevada, New Mexico, Oregon, South Dakota, States of Micronesia, Utah, Washington, and Wyoming

Independent variable	β	Std. Err.	$P > \|Z\|$	β 95% CI
For our marketing purposes				
Size: Small	0.43	0.10	<0.001	[0.24, 0.62]
Size: Medium	0.74	0.10	<0.001	[0.54, 0.93]
Size: Large	1.46	0.13	<0.001	[1.21, 1.70]
Size: Very large	2.53	0.20	<0.001	[2.14, 2.92]
OCC District (Northeastern)	-0.14	0.12	0.25	[-0.39, 0.10]
OCC District (Central)	-0.23	0.10	0.02	[-0.42, -0.40]
OCC District (Southern)	-0.46	0.10	<0.001	[-0.66, -0.27]
Type: Commercial Bank (OCC)	0.02	0.11	0.88	[-0.20, 0.23]
Type: Savings Association (OTS)	0.34	0.15	0.03	[0.04, 0.63]
Type: Savings Bank (FDIC)	0.26	0.17	0.13	[-0.08, 0.61]
Type: Commercial Bank (FED)	0.11	0.11	0.31	[-0.10, 0.33]
For joint marketing with other financial companies				
Size: Small	0.56	0.14	<0.001	[0.30, 0.83]
Size: Medium	0.80	0.13	<0.001	[0.54, 1.06]
Size: Large	1.52	0.14	<0.001	[1.25, 1.80]
Size: Very large	2.39	0.16	<0.001	[2.08, 2.70]
Trust powers	0.35	0.09	<0.001	[0.17, 0.52]
OCC District (Northeastern)	0.34	0.12	0.01	[0.10, 0.58]
OCC District (Central)	0.22	0.11	0.05	[0.00, 0.45]
OCC District (Southern)	0.08	0.11	0.46	[-0.14, 0.31]
For our affiliates' everyday business purposes– transactions and experiences				
Size: Small	0.41	0.15	0.01	[0.12, 0.69]
Size: Medium	0.77	0.14	<0.001	[0.49, 1.04]
Size: Large	1.50	0.15	<0.001	[1.21, 1.79]
Size: Very large	2.37	0.17	<0.001	[2.04, 2.69]
Trust powers	0.23	0.09	0.01	[0.05, 0.42]
OCC District (Northeastern)	0.003	0.13	0.98	[-0.25,0.25]
OCC District (Central)	0.10	0.12	0.40	[-0.13, 0.33]
OCC District (Southern)	-0.41	0.12	0.001	[-0.65, -0.17]
For our affiliates' everyday business purposes– creditworthiness				
Size: Small	0.18	0.23	0.45	[-0.28, 0.64]
Size: Medium	0.74	0.21	0.001	[0.32, 1.15]
Size: Large	1.45	0.21	<0.001	[1.03, 1.86]
Size: Very large	2.54	0.21	<0.001	[2.14, 2.95]
Ownership: No stock	-0.85	0.35	0.02	[-1.54, -0.15]
For our affiliates to market to you				
Size: Small	0.51	0.27	0.06	[-0.02, 1.02]
Size: Medium	0.84	0.25	0.001	[0.35, 1.34]
Size: Large	1.59	0.26	<0.001	[1.09, 2.10]
Size: Very large	2.58	0.27	<0.001	[2.06, 3.09]
OCC District (Northeastern)	0.72	0.20	<0.001	[0.33, 1.11]
OCC District (Central)	0.09	0.19	0.63	[-0.29, 0.47]
OCC District (Southern)	0.17	0.19	0.37	[-0.20, 0.54]
Type: Commercial Bank (OCC)	0.06	0.21	0.79	[-0.36,0.47]
Type: Savings Association (OTS)	0.002	0.27	0.99	[-0.52, 0.53]
Type: Savings Bank (FDIC)	-0.03	0.29	0.93	[-0.59, 0.53]
Type: Commercial Bank (FED)	0.38	0.18	0.04	[0.02, -1.86]
For nonaffiliates to market to you				
Size: Small	0.49	0.34	0.15	[-0.18, 1.16]
Size: Medium	0.77	0.33	0.02	[0.13, 1.42]
Size: Large	1.51	0.33	<0.001	[0.87, 2.15]
Size: Very large	1.88	0.33	<0.001	[1.23, 2.53]
OCC District (Northeastern)	0.24	0.30	0.43	[-0.35, 0.82]
OCC District (Central)	0.62	0.26	0.02	[0.11, 1.13]
OCC District (Southern)	0.44	0.27	0.10	[-0.08, 0.95]
Type: Commercial Bank (OCC)	0.73	0.23	0.001	[0.28, 1.17]
Type: Savings Association (OTS)	0.31	0.33	0.348	[-0.34, 0.96]
Type: Savings Bank (FDIC)	0.36	0.36	0.32	[-0.34, 1.05]
Type: Commercial Bank (FED)	0.21	0.27	0.43	[-0.31, 0.72]

Table 11: Results from the logistic regression models corresponding to the different types of sharing practices. The control categories for each variable are: Size (Very small), OCC District (Western), Type (Commercial Bank, FDIC), Trust Powers (No powers), and Ownership (Shareholders). Only those variables significant at α=0.05 are shown.

G Detailed Sharing Practices

Sharing Practice	Very small		Small		Medium		Large		Very large	
Financial institutions' own marketing purposes (N = 3,552)*										
Don't Share	509	57.6%	423	47.2%	354	39.8%	126	23.6%	33	9.4%
Share, Opt-Out	6	0.7%	15	1.7%	21	2.4%	17	3.2%	27	7.7%
Share, No Opt-Out	368	41.7%	457	51.1%	515	57.9%	390	73.2%	291	82.9%
Joint marketing with other financial companies (N = 3,564)*										
Don't Share	784	88.3%	714	80.3%	678	75.6%	316	59.1%	129	36.3%
Share, Opt-Out	11	1.2%	12	1.4%	19	2.1%	17	3.2%	33	9.3%
Share, No Opt-Out	93	10.5%	163	18.3%	200	22.3%	202	37.8%	193	54.4%
For affiliates' everyday business purposes – transactions and experiences – (N = 3,537)*										
Don't Share	785	89.6%	752	85.1%	711	80.0%	349	65.1%	150	42.6%
Share, Opt-Out	6	0.7%	8	0.9%	14	1.6%	20	3.7%	17	4.8%
Share, No Opt-Out	85	9.7%	124	14.0%	164	18.5%	167	31.2%	185	52.6%
For affiliates' everyday business purposes – creditworthiness – (N = 3,530)*										
Don't Share	835	96.0%	841	95.2%	819	92.0%	455	85.1%	229	65.1%
Share, Opt-Out	31	3.6%	38	4.3%	65	7.3%	79	14.8%	119	33.9%
Share, No Opt-Out	4	0.5%	4	0.5%	6	0.7%	1	0.2%	7	1.1%
For affiliates to market to you (N = 1,284)*										
Don't Share	218	89.7%	232	82.9%	256	76.2%	129	59.5%	72	34.6%
Share, Opt-Out	25	10.3%	47	16.8%	77	22.9%	87	40.1%	136	65.4%
Share, No Opt-Out	0	0.0%	1	0.4%	3	0.9%	1	0.5%	0	0.0%
For non-affiliates to market to you (N = 3,508)*										
Don't Share	857	98.4%	852	97.4%	845	96.5%	499	93.1%	316	90.3%
Share, Opt-Out	12	1.4%	23	2.6%	30	3.4%	37	6.9%	32	9.1%
Share, No Opt-Out	2	0.2%	0	0.0%	1	0.1%	0	0.0%	2	0.6%

Table 12: Sharing practices of FDIC-insured institutions by size (assets). Asset brackets are as follows: Very small= $x <$ 25th percentile; Small= 25th percentile $< x <$ 50th percentile; Medium= 50th percentile $< x <$ 75th percentile; Large= 75th percentile $< x <$ 90th percentile; Very large= 90th percentile $< x$. Smaller institutions share consistently less than larger ones for each purpose. * denotes statistical significance at α=0.05 using a χ^2 proportionality test.

Sharing practice	Southern		Central		Western		Northeastern	
Financial institutions' own marketing purposes (N = 3,552)*								
Don't Share	460	47.2%	428	43.9%	364	37.6%	193	30.3%
Share & Opt-Out	23	2.4%	21	2.2%	20	2.1%	22	3.5%
Share & No Opt-Out	491	50.4%	525	53.9%	583	60.3%	422	66.3%
Joint marketing with other financial companies (N = 3,564)*								
Don't Share	747	75.8%	729	75.1%	745	76.7%	400	62.9%
Share & Opt-Out	18	1.8%	24	2.5%	23	2.4%	27	4.3%
Share & No Opt-Out	220	22.3%	218	22.5%	204	21%	209	32.9%
For affiliates' everyday business purposes – transactions and experiences – (N = 3,537)*								
Don't Share	817	83.4%	753	77.4%	737	77.3%	440	69.7%
Share & Opt-Out	11	1.1%	27	2.8%	9	0.9%	18	2.9%
Share & No Opt-Out	151	15.4%	193	19.8%	208	21.8%	173	27.4%
For affiliates' everyday business purposes – creditworthiness – (N = 3,530)*								
Don't Share	901	92.1%	883	90.9%	869	91.10%	526	83.9%
Share & Opt-Out	76	7.8%	83	8.9%	78	8.2%	95	15.2%
Share & No Opt-Out	1	0.1%	5	0.5%	7	0.7%	6	1.0%
For affiliates to market to you (N = 1,284)*								
Don't Share	231	73.1%	267	77.8%	277	75.1%	132	51.6%
Share & Opt-Out	85	26.9%	75	21.9%	92	24.9%	120	46.9%
Share & No Opt-Out	0	0.0%	1	0.3%	0	0.0%	4	1.6%
For non-affiliates to market to you (N = 3,508)								
Don't Share	921	95.8%	934	95.5%	927	97.4%	587	95.1%
Share & Opt-Out	38	3.4%	41	4.2%	25	2.6%	30	4.9%
Share & No Opt-Out	2	0.2%	3	0.3%	0	0.0%	0	0.0%

Table 13: Sharing practices of FDIC-insured institution by the OCC District where the institution is physically headquartered. Overall, institutions in the Southern OCC Region shared for the fewest reasons. Institutions in the Western and Northeastern OCC Regions shared for the largest number of reasons. * denotes statistical significance at α=0.05 using a χ^2 proportionality test.

Sharing Practice	Commercial bank, FDIC		Commercial bank, OCC		Commercial bank, Fed		Savings association, OTS		Savings bank, FDIC	
Financial institutions' own marketing purposes (N = 3,552)*										
Don't Share	918	43.9%	203	41.9%	180	35.7%	81	32.1%	63	28.8%
Share, Opt-Out	55	2.6%	6	1.2%	15	3.0%	5	2.1%	5	2.3%
Share, No Opt-Out	1,120	53.1%	275	56.8%	309	61.3%	166	65.9%	151	69.0%
Joint marketing with other financial companies (N = 3,564)*										
Don't Share	1,609	76.4%	359	73.9%	340	67.9%	180	71.2%	133	61.3%
Share, Opt-Out	49	2.3%	7	1.4%	18	3.6%	11	4.4%	7	3.2%
Share, No Opt-Out	449	21.1%	120	24.7%	143	28.5%	62	24.5%	77	35.5%
For affiliates' everyday business purposes – transactions and experiences – (N = 3,537)*										
Don't Share	1,664	79.8%	378	77.5%	356	71.5%	185	74.3%	164	76.0%
Share, Opt-Out	34	1.6%	13	2.7%	10	2.0%	4	1.6%	4	1.9%
Share, No Opt-Out	388	18.6%	97	19.9%	132	26.5%	60	24.1%	48	22.2%
For affiliates' everyday business purposes – creditworthiness – (N = 3,530)*										
Don't Share	1,908	91.5%	425	87.5%	429	86.3%	225	91.5%	192	89.3%
Share, Opt-Out	166	8.0%	61	12.6%	65	13.1%	18	7.3%	22	10.2%
Share, No Opt-Out	12	0.6%	0	0.0%	3	0.6%	3	1.2%	1	0.5%
For affiliates to market to you (N = 1,284)*										
Don't Share	551	75.6%	115	68.9%	133	60.5%	62	68.9%	46	58.2%
Share, Opt-Out	174	23.9%	52	31.1%	86	39.1%	28	31.1%	32	40.5%
Share, No Opt-Out	3	0.4%	0	0.0%	1	0.5%	0	0.0%	1	1.3%
For non-affiliates to market to you (N = 3,508)*										
Don't Share	2,016	97.0%	448	93.3%	468	95.7%	234	95.1%	203	94.4%
Share, Opt-Out	60	2.9%	31	6.5%	20	4.1%	11	4.5%	12	5.6%
Share, No Opt-Out	2	0.1%	1	0.2%	1	0.2%	1	0.4%	0	0.0%

Table 14: Sharing practices of FDIC-insured institution by type of institution. Relative to other types of institutions, commercial banks supervised by the FDIC most frequently did not share data. Savings banks supervised by the FDIC shared more for joint marketing and their own marketing than all other institution types. * denotes statistical significance at α=0.05 using a χ^2 proportionality test.

H What Information is Collected

The model privacy form specified that institutions state exactly six types of information they collect from a list of 24 types of personal information. We present the counts for each of the 24 terms in Table 15. As we discussed in Section 4.1.4, each institution was required by the model privacy form to choose exactly six types of information, which means that the absence of a particular type of information does not imply that the company does not collect that information.

We note that few, if any, of these 24 types of personal information seem abnormal for a financial institution to collect, raising the question of what this particular disclosure communicates to users. We further note that the six types of information that were listed most commonly are in fact the six items given in pink text as examples in the model privacy form. While institutions did vary somewhat in the types of information they listed, the fact that the examples from the model privacy form were most commonly used and the fact that not listing an item does not mean that an institution does not collect it raises the question of whether differences in institutions' disclosures are meaningful.

We also observed many instances of institutions inventing their own wordings, contrary to the specification of the model privacy form [38]. For instance, Congressional Bank (`congressionalbank.com`) listed "Date of Birth," "Driver's License," and "Passport" even though none of these three types are listed in the model regulation. Similarly, Monitor Bank (`monitorbank.com`) listed "deposit account number(s)," "phone number," "address," "date of birth," and "loan number(s)." While it was not surprising that a financial institution might collect this data, none of these five items were listed in the specification [38]. Our parser searched for these three items, though we did not include them in our total counts. Overall, 267 institutions said they collected "address," 218 said they collected "name," and 9 said they collected "phone number." Although institutions were required to say they collect a consumer's "Social Security number," 1.7% of institutions did not do so.

Type of information	# institutions
Social Security number	6,086
Account balance	5,493
Payment history	4,902
Credit history	4,881
Income	3,428
Credit score	2,842
Transaction history	2,138
Checking account information	1,403
Account transaction	1,204
Overdraft history	1,085
Transaction or loss history	590
Wire transfer instructions	525
Employment information	522
Assets	352
Credit card or other debt	333
Mortgage rates and payments	189
Investment experience	53
Purchase history	29
Insurance claim history	26
Risk tolerance	26
Retirement assets	23
Medical information	11
Credit-based insurance score	4
Medical-related debts	0

Table 15: Types of personal information financial institutions say they collect.

I When Information is Collected

As described in Section 4.1.5, the model privacy form specifies that institutions must list exactly five occasions on which they collect information [38]. As with the types of information collected, the five most common occasions on which institutions state that they collect information are the five occasions listed in pink text as examples in the model privacy form. Furthermore, one might argue that none of the occasions an institution might state that they collect information are surprising.

Occasion	# institutions
Open an account	5,882
Apply for a loan	5,431
Use your credit or debit card	3,400
Pay your bills	2,750
Deposit money	2,676
Make deposits or withdrawals from your account	1,674
Show your driver's license	1,063
Give us your contact information	1,036
Make a wire transfer	1,003
Provide account information	658
Give us your income information	522
Show your government-issued ID	518
Provide employment information	517
Apply for financing	363
Pay us by check	232
Provide your mortgage information	169
Give us your wage statements	153
Apply for insurance	141
Give us your employment history	101
Enter into an investment advisory contract	43
Seek advice about your investments	42
File an insurance claim	31
Tell us about your investment or retirement portfolio	26
Seek financial or tax advice	25
Tell us where to send the money	17
Pay insurance premiums	16
Direct us to buy securities	10
Tell us who receives the money	9
Direct us to sell your securities	6
Apply for a lease	6
Buy securities from us	3
Tell us about your investment or retirement earnings	3
Order a commodity futures or option trade	1
Sell securities to us	0

Table 16: Occasions on which financial institutions say they collect consumers' personal information. Notably, these occasions seem normal for a financial institution to collect a consumer's information.