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

Lorrie Faith Cranor, Kelly Idouchi, Pedro Giovanni Leon, Manya Sleeper, Blase Ur
Carnegie Mellon University
{lorrie, kidouchi, pedrogln, msleeper, bur}@cmu.edu

ABSTRACT

Although large-scale comparisons of privacy practices across an industry have the potential to illuminate the state of consumer privacy and to uncover egregious practices, the freeform legalese of most privacy policies makes such comparisons time-consuming and expensive. Financial institutions in the United States are required by the Gramm-Leach-Bliley Act to provide annual privacy disclosures. In 2009, eight federal agencies jointly released a model privacy form for these disclosures. While use of the model privacy form is not required, it has been widely adopted. With so many financial institutions' policies available in a standard format, large-scale comparisons are now more readily achievable.

We built an automated web crawler and document parser for the model privacy form and automatically evaluated thousands of financial institutions' disclosures. We found large variance in data-sharing practices, even among banks of the same class. While thousands of financial institutions share personal information without providing the opportunity for consumers to opt out, some institutions' practices are more consumer-friendly. Institutions' practices vary by region and by the size of the institution. Furthermore, we uncovered violations of financial regulation, such as failing to allow consumers to limit data sharing even when required to do so. We identify issues with the design and use of the model privacy form, ranging from poorly designed categories to institutions making self-contradictory statements. We discuss implications for privacy in the financial industry, as well as future directions for standardized privacy notices.

Keywords

Privacy, financial industry, bank, disclosure, data sharing, large-scale comparison, standard format, opt-out

1. INTRODUCTION

When the United States Congress was considering the Gramm-Leach-Bliley Act of 1999, 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 [15]. The act passed with a provision mandating annual privacy disclosures. However, in the year that followed, these disclosured were widely criticized for being difficult to read and understand [24]. In response, eight federal agencies jointly released a model privacy form in 2009 [27]. This standardized disclosure of privacy practices was designed to "make disclosure of institutions' information sharing practices and consumer choices more transparent" in an an easy-to read and understandable format [27].

Besides making it easier for consumers to find privacy information, standardized privacy notices 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) [5], to recent attempts to have humans annotate websites' privacy policies and terms of service [33], 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 abuse machine-readable privacy disclosures [21], while attempts to have humans annotate privacy practices do not scale well.

Financial institutions' wide adoption of the model privacy form over the past three years provides a rare opportunity to analyze companies' privacy practices across an entire industry on a large scale. To this end, we wrote a computer program that crawls the Internet in search of these standard-format disclosures and automatically parses them, enabling a large-scale comparison of financial institutions' privacy practices. Using a list of 6,701 FDIC-insured financial institutions' names and website domains as a starting point, we collected and parsed standard-format privacy disclosures from 3,422 financial instituions. We then compared these 3,422 institutions in terms of data-sharing practices, consumers' ability to opt out of data-sharing, and what personal information is collected. For additional insight into how similar institutions 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 [17].

We found wide variance in financial institutions' privacy practices across the industry. These differences in privacy practices also separated institutions in the same business class, suggesting that consumers might have the opportu-

The Twelfth Workshop on the Economics of Information Security (WEIS 2013) , June 11–12, 2013, Washington, DC.

nity to pick a financial institution with more consumer-friendly privacy practices if information to help them find these institutions was more readily available. Joining the data we parsed with information about institutions' characteristics, we performed regressions and found that large institutions and those that conduct business in multiple states more frequently share consumers' personal information. We also identified differences in institutions' practices across geographic regions of the U.S. Furthermore, we found deficiencies in both the specification and the use of the model privacy form that may actually limit consumers' access to information about financial institutions' privacy practices.

In Section 2, we summarize the relevant provisions of the GLB Act, as well as provide an overview of prior work on standardized privacy notices. In Section 3, we explain our methodology and summarize the data set we collected. We present our results in Section 4, and then discuss our findings and their implications for both financial institutions' privacy practices and for standardized privacy notices in Section 5. We include an appendix with detailed data and screenshots of model standard-format privacy disclosures.

2. BACKGROUND AND RELATED WORK

In this section, we describe the privacy provisions of the GLB. We also discuss efforts to standardize and evaluate privacy notices, including the creation of formal specifications, standardized formats, and more usable privacy notices.

2.1 Privacy provisions of the GLB Act

In this paper, we examine financial institutions' privacy disclosures that are mandated by the Gramm-Leach-Bliley (GLB) Act. The GLB Act, also known as the Financial Modernization Act of 1999, was signed into law on November 12, 1999 [37]. Its primary goal was to permit the consolidation of different types of businesses within the financial industry. As a result of consolidation, institutions could share consumers' information with affiliates that fall under the same holding company [22, 38].

The GLB Act also includes provisions related to consumer privacy. Its core privacy protections include marketing disclosure, notice, choice, security, and enforcement [4]. Title V requires financial institutions to provide annual notices and mandates that customers be allowed to opt out of data sharing with non-affiliate companies. However, joint marketing efforts are exempt from this provision [12].

The privacy protections offered by the GLB Act have prompted a range of criticisms. Some critics feel that the GLB act offers incomplete or too few privacy protections. For instance, in an examination of the GLB Act privacy provisions, Janger et al. conclude that the GLB Act "leaves the burden of bargaining on the less informed party, the individual consumer" [16]. Schiller also argues that the notice provisions provided by the GLB do not go far enough toward providing privacy protections [29]. She recommends that the GLB further restrict information sharing among affiliates. Freeman similarly concludes that the GLB Act was a good start but "need[s] further refinement" [11], arguing that the "'opt-out' provision has made it unlikely that many customers will take the active steps needed to protect their confidential data" [11]. Nojeim also argues that the GLB Act 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 [26].

Other critics feel that the protections offered by the GLB 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" [31]. Lacker, for example, argues that in a perfectly competitive market, financial privacy would be determined by economic forces regardless of the choice mechanisms offered [20]. Those who support open information sharing also often claim that it makes the market more efficient and benefits both financial institutions and consumers. They further claim that other laws, such as the Federal Credit Reporting Act, provide sufficient privacy protections for consumers [13].

In counterpoint, Swire argues that inappropriate disclosure of personal information can easily lead to a "misallocation of resources" [13]. Prior to the GLB Act, an evaluation of financial institutions' websites conducted by U.S. regulatory agencies found that only 40% of the websites posted a privacy policy [36]. Sheng et al. performed a longitudinal study of 50 financial institutions' privacy policies. They found that although privacy policies became more complete and contained more detailed information about sharing practices after the GLB Act, the amount of sharing among affiliates and non-affiliates increased [30]. Antón et al. examined 40 online privacy policies under the GLB Act and found a lack of standardized vocabulary across the policies, counter to the mandate of GLB [2]. In this paper, we provide a large-scale analysis and comparison of financial institutions' privacy practices in a post-GLB environment.

After financial institutions were required by the GLB Act to provide annual privacy disclosures, "many notices provided to consumers were long and complex" at the beginning, resulting in privacy notices that were "difficult to compare, even among financial institutions with identical practices" [27]. As a result, eight federal agencies in the United States jointly released a model privacy form for disclosures under the GLB Act; we include screenshots of this form in the appendix. This model privacy form was designed to make "sharing practices and consumer choices more transparent" in a format that is clear and understandable for users [27]. Financial institutions may rely on this model privacy form as a safe harbor to provide privacy disclosures under the released rules [27]. The model privacy form provides a relatively standardized format for privacy disclosures, facilitating our large-scale, automated comparisons.

2.2 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 [28] and the U.S. Federal Trade Commission's Fair Information Practice Principles [10]. 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 [32]. 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 [34].

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 [14]. Similarly, Jensen and Potts examined 64 privacy policies and found that many were difficult to find and read [18]. 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 [35]. 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 [23].

For privacy notices to be effective, they must be clear and comparable across websites. Standardized privacy notices — whether human-readable or machine readable — help facilitate large-scale comparison and evaluation [6]. 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 [5]. 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. [7]. Although adopted to some degree, P3P has not received support across different browsers, minimizing its usefulness. Cranor et al. found high rates of syntax errors among the P3P policies they examined [7]. 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 [21].

Standardized formats for privacy notice can mitigate many usability problems if well designed. Furthermore, privacy notices can be compared easily if they are presented in a standardized format. The model privacy form we examine in this paper is such a standardized privacy policy. Other 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 [19]. 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 aimed to crowdsource the problem of putting this information into a standardized, usable format [33].

3. METHODOLOGY AND DATA SETS

Our large-scale comparison of financial institutions' privacy practices took place in three main parts. First, we conducted an automated web crawl to collect instances of the model privacy form, which we describe in Section 3.1. After obtaining candidate forms, we automatically selected one form per institution and extracted the contents of the form (Section 3.2 and Section 3.3). We manually verified the accuracy of parsing for a small set of disclosures (Section 3.4). The analysis of our data formed the third and final part of our comparison (Section 3.5). In that section, we discuss our approaches to comparing the prevalence of different practices, as well as the logistic regressions we ran based on institutions' characteristics. To gain additional insight into the privacy choices a consumer might have, we collected two small, supplemental data sets, which we discuss in Section 3.6.

3.1 Data collection

As our first step, we automatically searched for different financial institutions' privacy disclosures that use the model privacy form. To collect the disclosures in a systematic way and minimize confusion between banks with similar names (e.g., multiple, seemingly independent banks called "First National Bank," "Liberty Bank," and "Pinnacle Bank"), we based our search on a directory of financial institutions maintained by the US Federal Deposit Insurance Corporation [8]. At the time of our research in February 2013, this online directory listed 7,072 financial institutions, along with their characteristics, location, assets, and contact information. To further minimize confusion between similarly named institutions, we restrict our search for policies from a particular institution to the website domain name listed for that institution in the FDIC directory. Of the 7,072 institutions in the directory, 6,701 listed a domain name, either in the form of web or email addresses.

To search for a disclosure from an institution, regardless of whether it was linked from the institution's homepage, we performed an automated Google query. We used the search string, "What does *institution name* do with your personal information," inserting the name listed in the FDIC database, because this was the header of the model privacy form [27]. We restricted queries to a bank's FDIC-listed domain using the *as_sitesearch* URL parameter. For each Google query, we considered only the first page of results, containing between zero and ten links for each institution.

For each institution, we automatically downloaded every item linked from the first page of the Google results. In our pilot testing, we found disclosures in both HTML (webpage) and PDF formats. We therefore built our crawler to support both filetypes. To provide a consistent input for our parser, we automatically saved both HTML and PDF files in the PDF format. When an item's URL ended in the extension *.pdf*, we fetched it using the Wget package.[1]

Querying Google for each of the 6,701 institutions with domain names, we received at least one result for 6,328 institutions. Because the first page of Google results contains between one and ten results for each query, we attempted to download 53,292 files, and 52,564 downloaded successfully.

3.2 Data selection

Our first step in parsing notices that follow the model privacy form was to extract the text. We used the Linux utility *pdftotext*[2] 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 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 from the 1–10 candidates linked from the Google results. We selected 25 phrases that always appear in the model disclosure [27], spread approximately evenly throughout the document. For each candidate file, we searched for all 25 phrases and recorded the number of phrases found as

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

the candidate's "score." Table 7 in the appendix shows the distribution of these scores. To weed out candidates that did not appear to be based on the model privacy form, we set a cutoff score of 21, eliminating all candidates that contained 80% or fewer of our expected keywords and phrases.

Of the 52,564 files we downloaded, 805 files (1.5%) were unable to be converted to text, while 47,636 files (90.6%) matched 4 or fewer of the 25 features we used to identify the model privacy form. These files were likely not model-privacy-form notices. On the other end of the spectrum, 3,892 files (7.4%) matched between 21 and 25 of the 25 features, indicating that these files were likely based on the model privacy form. The remaining 231 files (0.4%) matched between 5 and 20 of the 25 features, indicating files that might have deviated substantially from the standard-format policy or that otherwise contained some of the text from standard-format policies, but not all.

For each institution, we chose the remaining candidate with the highest score, if any. This procedure thus gave preference to the most complete disclosure that we found for each institution. In the case of a tie, we chose the candidate that appeared first in the Google results. Of the 6,701 banks with domains, 3,441 (51.4%) had at least one policy that met our score threshold (21/25). This number is smaller than the 3,892 files that met our score threshold because some institutions had multiple copies or multiple revisions of a single policy.

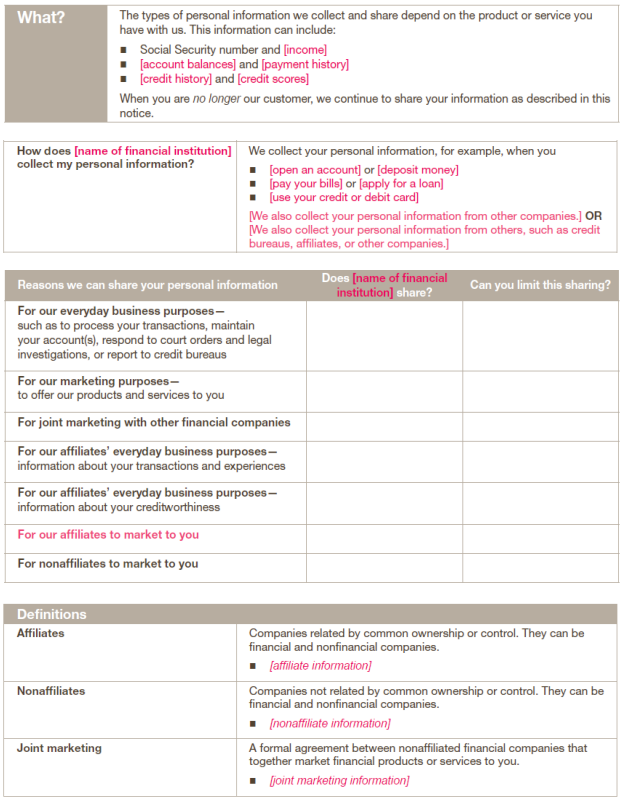
Some of the financial institutions in the FDIC database, however, listed the same web domain as another financial institution in the database, likely due to mergers, partnerships, or other business relationships. To verify that the file we associated with a particular institution came from that institution, rather than another institution using the same web domain, we manually examined the institution names listed on 104 policies from these domains. We removed 19 policies where the name listed on the policy did not approximately match the institution name in the FDIC database. For example, both the State Bank of Missouri and The State Bank listed gostatebank.com as their domain. The only policy we downloaded from this domain listed The State Bank as the name of the institution, so we disassociated the State Bank of Missouri from this policy. In contrast, both USAA Federal Savings Bank and USAA Savings Bank list usaa.com as their domain, and searches for both banks return the same policy. The policy lists "USAA" as the institution. Since it appears that USAA's policy would extend equally to both institutions, we associate this policy with both institutions.

Following these removals, we were left with 3,422 policies. These 3,422 policies make up our primary data set.

3.3 Data extraction

Having selected at most one disclosure for each institution, our parser extracted data about the institution's privacy practices. The model privacy form has a strict document structure, with a number of subsections. As the first step in extracting data, we split the disclosure's text into the sections specified in the model notice, primarily using the four subsections shown in Figure 1.

We wrote regular expressions defining particular text patterns based on the specification and model notices of the model privacy form [27]. For instance, the disclosure contains a section for listing "Social Security number" and five other types of personal information that the institution collects. The topmost screenshot in Figure 1 depicts this section. The specification of the model privacy form [27] lists 23 types of information that can replace the 5 written in pink in the model notice. Therefore, we wrote regular expressions that searched for each of these 23 types of information. Our parser similarly searched for patterns in other sections of the form and wrote the extracted practices to a spreadsheet.



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]

When you are *no longer* our customer, we continue to share your information as described in this notice.

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.]

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		

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]*

Figure 1: Four primary sections of the model-privacy-form disclosure from which we extracted data. From top to bottom, these sections state what information is collected, explain how information is collected, state data-sharing practices, and identify partner companies. These screenshots are taken from the model notice [27]; institutions should replace the pink text as they fill out the table. A complete example of the model privacy form is shown in Appendix I.

During its creation, we repeatedly tested our parser on small groups of policies 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 (e.g., 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," and we adjusted the parser to recognize all of these variants). Similarly, as we describe in Appendix B, we iteratively updated our parser to recognize many variants of revision dates. That said, it would be intractable to update the parser to recognize every corner case among the 3,422 policies.

We paid particular attention to parsing the *disclosure table* (the third table shown in Figure 1), which states an in-

stitution'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 [27]. Based on our iterative 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").

3.4 Verification of parsing

While automated parsing of the 3,224 privacy disclosures allowed us to compare privacy practices on a larger scale than would have been possible through manual analysis, automated parsing can introduce errors. 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.

The vast majority of sections were present in each policy. For instance, the parser observed the disclosure table ("reasons we can share your personal information") for 3,413 (99.7%) of the 3,422 policies. The section that was recognized at the lowest rate ("How does *institution name* collect my personal information?") was recognized for 3,357 (98.1%) of the policies. Sections that were not recognized are either missing from the document itself or parsed incorrectly.

3.5 Analysis

The first half of our analysis focuses on the prevalence of different privacy practices and is based on institutions' disclosures in the model privacy form. 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.

As a secondary goal, we also investigated whether institutions complied with relevant portions of the GLB Act and adhered to the specification of the model privacy form. As part of this analysis, we visited the webpages of a random subset of 50 institutions to see how the model privacy form was used in practice. We also manually investigated instances where our parser found idiosyncratic results, uncovering a number of deviations from the specification of the model privacy form.

In the second half of our analysis, we investigated whether an institution's characteristics, such as geographic location, were correlated with its privacy practices. We joined our data with institutional characteristics reported in the FDIC Institution Directory [8], such as an institution's geographic region, assets, and specialization. We also used these characteristics as independent variables and ran a logistic regression. The dependent variable for this regression was an institution's sharing practice for one of the seven reasons listed in the disclosure table. We repeated this logistic regression for six of the seven sharing practices in the disclosure table; we excluded the "for our everyday business purposes" row, for which nearly all institutions had identical practices. Similarly, we ran a logistic regression in which an institution's characteristics were independent variables, and its adherence to the model privacy form and compliance with Title V of the GLB Act was the dependent variable.

3.6 Supplemental data sets

Although analyzing financial institutions by their specialization gives some insight into the practices of similar banks, we collected two additional, small-scale data sets to examine whether consumers could conceivably choose a more privacy-protective institution from among direct competitors. Our first supplemental data set comprises the model privacy forms from Forbes' "America's Best and Worst Banks" list, which includes the 100 largest publicly-traded banks and thrifts [3]. Of these 100 institutions, we were unable to retrieve a model-privacy-form notice or were unable to parse this notice for 27 institutions. Furthermore, some of these institutions used a scanned version or other image of the notice, preventing us from extracting text. Since credit cards are one of the most common consumer financial products, our second supplemental data set was based on a list of 11 credit card companies with the highest satisfaction ranking, according to J.D. Power [17]. We were able to retrieve model-privacy-form disclosures from all eleven companies, six of which were also in the Forbes list.

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 companies, as well as 24 companies that appear to be violating the law by not offering mandated opt-outs. To understand more fully whether direct competitors' practices vary, providing an opportunity for consumer choice, 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 discuss institutions' data-collection practices and how the design of the model privacy form might impact institutions' transparency with respect to these practices.

In the second part of this section, we present the results of regression models we built to investigate how institutions' practices are correlated with various factors, including the institution's size, specialization, and the state in which it is headquartered. Finally, we present our observations about misuse of the model privacy form.

4.1 Data-sharing practices

In this section, we describe financial institutions' stated data-sharing practices. We discuss with whom data is shared, the reasons why this data is shared, and the mechanisms institutions give consumers for opting out of data sharing, when applicable. We also present institutions' disclosures of what information they collect, and how, yet find these disclosures not to be particularly informative.

Our results show that there is a large variety of sharing and opt-out practices across financial institutions. This variety of practices suggests that helping consumers easily compare institutions' practices could empower them to select companies that best align with their privacy expectations.

4.1.1 With whom data is shared

The model privacy form presents 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

Practice	Number of institutions	Percentage of total
Affiliates		
Share with affiliates	836	24.4%
Do not share	1,077	31.5%
No affiliates	1,383	40.4%
Blank	94	0.3%
Nonaffiliates		
Share with nonaffiliates	241	7.0%
Do not share	3,031	88.6%
No nonaffiliates	15	0.4%
Blank	103	3.0%
Joint Marketing		
Jointly market	854	25.0%
Do not jointly market	2,447	71.5%
Blank	89	2.6%

Table 1: Sharing practices for the 3,422 institutions in our primary data set. *Blank* indicates that the institution defined the term, yet provided no information about its own practices.

disclosure. They also discuss nonaffiliates, which are nonaffiliated third parties. In the definitions section of the model privacy form, institutions not only provide boilerplate definitions of the terms "affiliates," "nonaffiliates," and "joint marketing," but also list their partners in each category.

Institutions varied starkly in their practices, as shown in Table 1. While 24.4% of institutions said they have affiliates and share with them, 31.5% do not share with their affiliates, and 40.4% do not have any affiliates. In contrast, 7.0% of institutions said they share with nonaffiliates, 88.6% said they do not, and only 0.4% said they do not have nonaffiliates. Joint-marketing practices also differed; 25.0% of institutions said they engage in joint marketing, whereas 71.5% of institutions said they do not. This section of the model privacy form was missing entirely for 0.9% of institutions, and a handful of institutions defined the terms without providing information about their own practices (labeled *blank* in Table 1). 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 the reasons for which an institution shares data. Our analysis of this table further demonstrates that institutions vary from not sharing data at all to sharing data without offering an opt-out. Notably, a few institutions do not offer opt-outs for data sharing even when required to do so by the GLB Act.

The disclosure table comprises seven rows, each representing a reason an institution might share data, such as everyday business purposes or 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 [27]. Of the 3,422 institutions in our data set, 2,255 institutions omitted this row. We therefore expected to parse either 6 or 7 rows of the disclosure table for each institution, and we indeed parsed either 6 or 7 rows for 93.9% of institutions. We do not check for consistency between the disclosure table and other parts of the model privacy form.

We grouped institutions' practices into three primary categories based on their responses to the questions "does *name* share?" and "can you limit this sharing?" We labeled institutions that answered "no" to the first question as *does not share*. Institutions 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 4.4.1, we assign the label *illogical* when answers to these two questions are self-contradictory (e.g., an institution says it shares in the first column, but says it does not share in the second); this occurs for 10–25 institutions (0.3%–0.7%) per row.

Companies are required to provide opt-outs for some types of data-sharing, but are not required to do so in other cases. In particular, the GLB Act states that 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," "for joint marketing," or that share information about transactions and experiences with affiliates "may choose to provide an opt-out" [27].

Table 2 presents a summary of financial 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 (56.8%) of the institutions said they share "for our marketing purposes" without offering an opt-out, and over one-fifth (22.4%) said they share "for joint marketing" without an opt-out. Fewer (19.7%) said they share information about transactions and experiences "for affiliates' everyday business purpose" without an opt-out.

While many institutions did not offer an opt-out if they were not required to do so, other institutions did not share data, or chose to offer an optional opt-out. If comparative privacy information were made easily accessible, consumers who are concerned about privacy could choose to do business with more privacy-protective institutions.

Companies that share for any of the remaining three reasons were required to offer an opt-out as a result of the Fair Credit Reporting Act (FCRA) [27]. If the policy that they state in the model privacy form is their actual policy, 24 different institutions in our data set are violating the law. Each institution said they shared for one or more of these reasons, and also said that consumers could not limit this sharing. We provide a list of these institutions in Section C of the appendix. We manually verified that the policy for each institution was parsed correctly. A total of 19 institutions said they shared information about creditworthiness "for our affiliates' everyday business purposes" and said that consumers could not limit this sharing. Furthermore, four institutions did the same "for our affiliates to market to you," while four institutions followed the same practice "for nonaffiliates to market to you."

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,

Reason for sharing personal information	Does not share		Shares, offers opt-out		Shares, no opt-out		Missing		Illogical	
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	33	1.0%	5	0.1%	3,319	99.3%	52	1.6%	12	0.4%
For our marketing purposes– to offer our products and services to you	1,373	41.1%	85	2.5%	1,898	56.8%	51	1.5%	13	0.4%
For joint marketing with other financial companies	2,518	75.3%	86	2.6%	748	22.4%	53	1.6%	20	0.6%
For our affiliates' everyday business purposes– information about your transactions and experiences	2,618	78.3%	52	1.6%	659	19.7%	81	2.4%	14	0.4%
For our affiliates' everyday business purposes– information about your creditworthiness *[Opt-out mandatory]*	3,040	91.0%	272	8.1%	19	0.6%	81	2.4%	22	0.7%
For our affiliates to market to you *[Opt-out mandatory when sharing; row may be omitted in certain cases]*	834	25.0%	328	9.8%	4	0.1%	2,247	67.2%	10	0.3%
For nonaffiliates to market to you *[Opt-out mandatory when sharing]*	3,192	95.5%	106	3.2%	4	0.1%	110	3.3%	25	0.7%

Table 2: A summary of 3,422 financial institutions' sharing practices regarding consumers' personal information. Institutions self-reported these practices in the disclosure table of the standard-format disclosure. Values that are missing could be caused by an institution omitting that row of the table, or by an error in our parser. Values that are labeled illogical contradict themselves, as discussed in Section 4.4.1.

email, web, and telephone. The opt-outs offered are shown in Table 3. Overall, 13.6% of institutions offer at least one opt-out mechanisms. We observed 259 institutions that provided exactly one mechanism, 164 institutions that provided two different mechanisms, and 42 institutions that provided at least three different mechanisms. There were 23 institutions for which we parsed this section overall, yet did not observe any of these four opt-out mechanisms.

More traditional opt-out mechanisms were more prevalent than computer-based methods. Of the institutions offering an opt-out, 69.1% 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 observed a full mail-in form. Computer-based opt-outs were relatively less popular; 30.7% of institutions let consumers opt-out via email or a website.

Opt-out mechanism(s)	Institutions	Percentage
Only phone	152	32.6%
Only postal mail	103	22.1%
Phone and website	70	15.0%
Phone and postal mail	67	14.4%
Three or more mechanisms	42	9.0%
Phone and email	15	3.2%
Postal mail and website	10	2.1%
Postal mail and email	2	0.4%
Only email	2	0.4%
Only website	2	0.4%

Table 3: Institutions' opt-out mechanisms. Overall, 466 institutions offered an opt-out. The most common opt-out mechanisms were phone and postal mail, while computer-based mechanisms were relatively less popular.

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" 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" [27]. In total, exactly six terms should be arranged in three bullet points, as shown in Figure 1.

We parsed this section, searching for "Social Security number" and the aforementioned 23 terms, as well as close variants. Section D in the appendix presents detailed results of this analysis.

Unfortunately, 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. Over 1,000 different institutions listed each of the following terms: account balances; payment history; credit history; income; credit scores; transaction history. These terms are six of the first seven terms listed in the specification of the model privacy form. "Transaction or loss history" was the only term among the first seven that was not also among the seven most frequently listed terms, which may be due to its similarity to the included "transaction history."

As a result, the current requirements do not provide adequate transparency of practices. Customers with access to different institutions' notices would not have a complete perspective of those institutions' collection practices and therefore would be unable to make decisions on that basis. It is important to provide a mechanisms for consumers to learn about all collected data. This could be done by requiring companies to either list all data types collected or provide a link to more detailed information. Moreover, consumers would likely benefit more if companies were required to disclose less obvious types of collected data or types of data that consumers might not expect to be collected.

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," "transaction history" are all part of "checking account information." On the other hand, as discussed in Section D of the appendix, some institutions create additional terms for the data they collect. Taking together, these results suggest the need for improving 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 were 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 events [27]. We present our detailed analysis of these disclosures in Section E of the appendix.

The five most frequently listed occasions were simply the first five listed in the model privacy form [27]. These occasions were when consumers open an account, apply for a loan, use their credit or debit card, deposit money, or pay bills. On the opposite end of the spectrum, only one institution noted collecting information when consumers tell them about investment or retirement earnings, and no institutions noted that they collect information when consumers sell securities to the institution.

Given that institutions are permitted to include only five terms, the omission of a term 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 of practices and does not benefit consumers. Furthermore, many of the current terms are arguably not very informative as it is obvious that companies need to collect certain types of data when customers request a service. On the other hand, informing consumers about less obvious means of collecting information may be more useful.

The model privacy form also contains disclosures about other sources that provide data to an institution. Under the "how does *name* collect my personal information?" section, 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" [27]. We observed that 82.6% of institutions collect additional information from credit bureaus, 82.5% do so from "other companies," and 72.7% collect data from affiliates.

4.2 Comparing similar institutions

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

In this section, we compare the practices of similar institutions. First, we split the institutions from the FDIC directory [8] into the eight different specializations they list, finding that institutions' practices differ even within a specialization. We then examine even more directly whether consumers might be able to choose between more and less privacy-protective institutions when making decisions where to bank or what credit card to open. To do so, we compare 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 cards [17]. Even among companies in these lists, we find differences in privacy practices, suggesting that making privacy practices more salient could empower consumers to choose privacy-protective institutions.

4.2.1 Institutions with the same specialization

Figure 2 summarizes the results of comparing financial institutions with the same primary specialization. We found differences both within a specialization and across categories. We found that financial institutions with agricultural specializations shared least frequently. On the other hand, mortgage lending, commercial lending, and consumer lending institutions shared most frequently, which often included sharing with nonaffiliates. Figure 2 shows that institutions share more for "our marketing purposes," "joint marketing," and "affiliates' everyday business purposes - transactions and experiences" than for other purposes. Detailed results are shown in Table 20 in the appendix.

We found that all six credit card companies in the FDIC database shared for their own marketing purposes. In contrast, we found that two credit card companies don't share customers' information with nonaffiliates, whereas four companies do. Similarly, we found differences among mortgage lending companies, 22% of which share information for joint marketing without offering an opt-out, while 76% do not share for joint marketing. We found that the majority of consumer lending companies don't share for joint marketing purposes, yet some do.

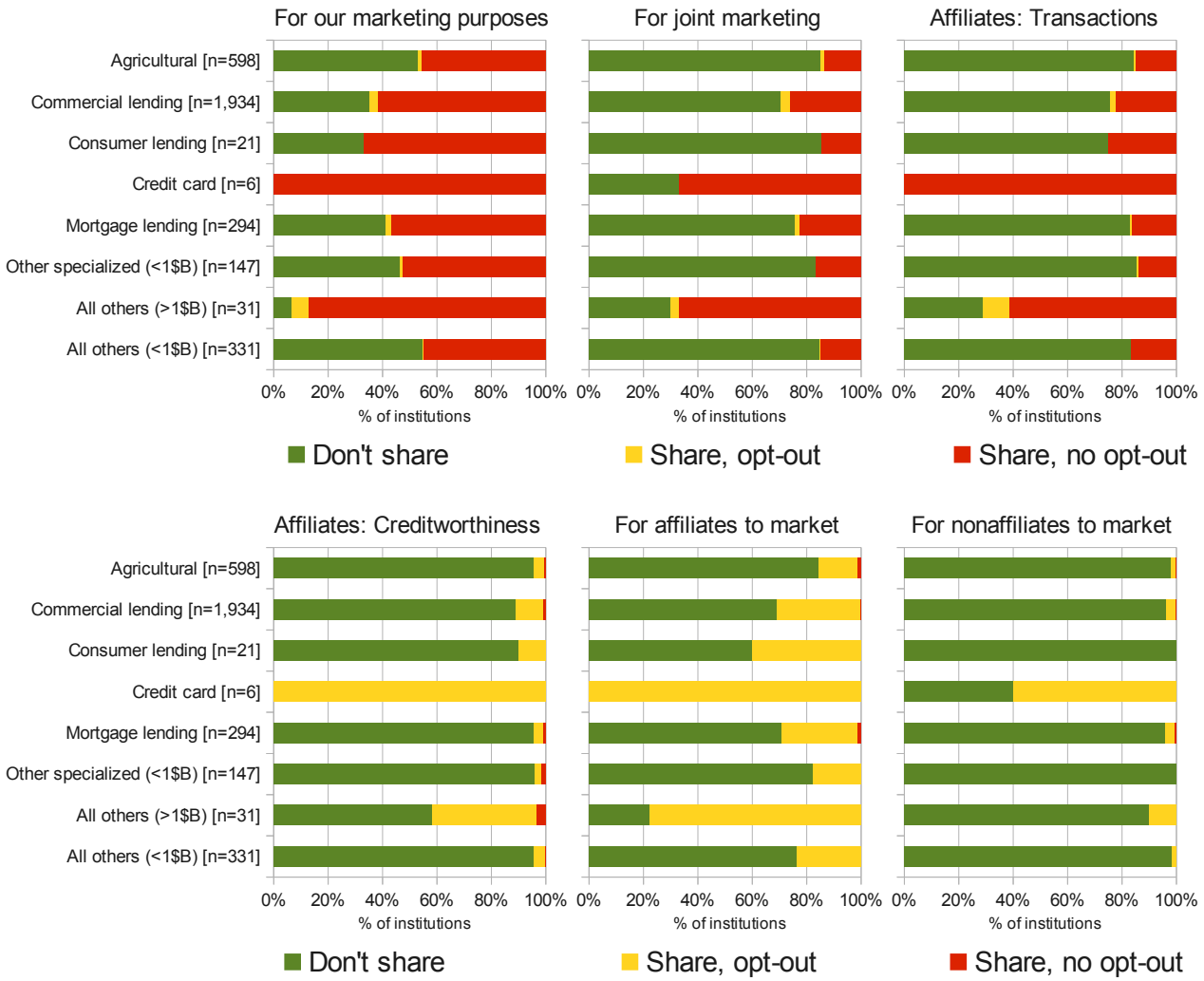


Figure 2: Sharing practices for financial institutions with different asset concentrations (specializations). The presence of different colors within a single asset-concentration class represent opportunities for consumer choice. That is, some institutions within a class have more consumer-friendly privacy practices than other institutions within the same class. Red bars in the three bottom graphs represent violations of the law.

4.2.2 *Practices of Forbes' largest banks*

From a Forbes list of the 100 largest banks in the U.S. [3], we obtained model privacy forms for 73 banks. Since a consumer might consider choosing a bank from among candidates on this list, we investigated how their privacy practices compare. Some of the remaining institutions used image files of the model privacy form, which were not possible to parse, while others did not appear to use the model privacy form.

Table 4 summarizes the sharing practices of these banks. Detailed practices for each bank are shown in Table 14 in the appendix. Relative to all institutions in the FDIC database, a larger proportion of these largest banks shared data. For example, while only 22.4% of the institutions in the FDIC database (Table 2) shared for joint marketing without offering an opt-out, 52.1% of the largest banks did so (Table 4). Similarly, while only 19.7% of the institutions in the FDIC database shared "transactions and experiences" for "affiliates' everyday business purposes," 69.9% of the largest banks did so. Furthermore, while only 9.8% of institutions overall shared for "affiliates to market to you" without an opt-out, 64.4% of the largest banks did.

4.2.3 *Credit Card Companies' Practices*

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 [17]. Six of these companies were also in the FDIC database. While most of these companies said they share data for many reasons, a few had more privacy-protective practices.

In particular, eight of the eleven companies said they share consumers' personal information without offering an opt-out for "our marketing purposes," "joint marketing," and "affiliates' everyday business practices - 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." The practices of each credit-card company are listed in Table 13 in the appendix.

Reason for sharing personal information	Does not share		Shares, offers opt-out		Shares, no opt-out		Missing		Illogical	
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%	73	100.0%	0	0.0%	0	0.0%
For our marketing purposes– to offer our products and services to you	6	8.2%	7	9.6%	59	80.8%	1	1.4%	0	0.0%
For joint marketing with other financial companies	26	35.6%	9	12.3%	38	52.1%	0	0.0%	0	0.0%
For our affiliates' everyday business purposes– information about your transactions and experiences	13	17.8%	8	11.0%	51	69.9%	1	1.4%	0	0.0%
For our affiliates' everyday business purposes– information about your creditworthiness *[Opt-out mandatory]*	24	32.9%	48	65.8%	0	0.0%	1	1.4%	0	0.0%
For our affiliates to market to you *[Opt-out mandatory when sharing; row may be omitted in certain cases]*	5	6.8%	47	64.4%	0	0.0%	21	28.8%	0	0.0%
For nonaffiliates to market to you *[Opt-out mandatory when sharing]*	59	80.8%	13	17.8%	1	1.4%	0	0.0%	0	0.0%

Table 4: A summary of data-sharing practices among the 73 of Forbes' 100 largest banks for which we obtained model privacy forms [3].

4.3 Factors correlated with privacy practices

We next investigated how different characteristics of financial institutions correlated with those institutions' privacy practices. The factors we investigated included the institution's physical location, charter type (commercial bank or savings institution), charter agent (state or federal), specialization, regulator, number of offices, and assets. We list these factors with more detail in Table 5. We obtained these characteristics from the Federal Deposit Insurance Corporation (FDIC) directory [8]. To evaluate the impact of these factors on institutions' sharing practices, we used logistic regression models. In total, we built six regression models corresponding to six of the seven practices listed in the disclosure table. We chose not to build a model for sharing associated with the institution's everyday business purposes because that practice varied minimally.

When an institution does not share consumers' personal information for a particular purpose, the binary outcome variable in the regression takes the value 0. When an institution shares information, regardless of whether it offers an opt-out, the outcome variable takes the value 1. We also built 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 outcome models, and we report results from the binary model in this paper as those are easier to interpret.

Our logistic regression models revealed a number of factors that were significantly correlated with institutions' privacy practices (Table 6). Chief among these factors were the OCC District where the institution is geographically located, number of offices, and whether the institution is part of a bank holding company. Asset concentration hierarchies (specializations) impacted sharing in different directions with respect to the control specialization depending on the particular specialization. We present detailed results for each regression model in Section G in the appendix.

Institutions in the Central OCC region shared at a lower rate than those in the Western region for both their own marketing purposes ($p = 0.003$) and joint marketing ($p = 0.010$). In contrast, institutions in the Northeastern OCC region shared at a higher rate for their affiliates' everyday business practices, and for their affiliates' marketing purposes (all $p < 0.001$). Additionally, all five types of sharing listed in Table 6 increased as the number of offices increased (all $p < 0.050$). We also found that banks with granted trust powers shared at a significantly higher rate. Trust powers are granted at the state level under criteria that vary by state [9]. Although we have left the full investigation of how state-level privacy regulations impact institutions' practices for future work, the significant correlations between both OCC region and granted trust powers and sharing practices suggest that state regulations may impact sharing practices.

4.3.1 Bank charter class

We also looked at how different types of commercial and savings banks, as well as other savings associations, share consumers' information. With the exception of sharing for their own marketing purposes, under 30% of these institutions said they share with affiliates. This finding suggests that, if consumers had easy access to information about institutions' sharing practices, they could select more privacy-protective ones. We also found that savings banks supervised by the FDIC (64%) and savings associations supervised by the OTS (63%) said at a higher rate that they share for their own marketing purposes, while commercial banks supervised by the FDIC said they share at the lowest rate. Detailed results of sharing practices across different types of charter classes are shown in Table 17 in the appendix.

Factor	Definition	Possible values	Control category
Assets	The sum of all assets owned by the institution. Includes cash, loans, securities, and bank premises, but not off-balance-sheet accounts	N/A	N/A
Equity Capital	Total equity capital (includes preferred and common stock, surplus and undivided profits)	N/A	N/A
Net Income	Net interest income plus total non-interest income plus realized gains (losses) on securities and extraordinary items, less total non-interest expense, loan loss provisions, and income taxes	N/A	N/A
Offices	Number of Branches or Offices, including its main office	N/A	N/A
State Name	State where the institution is physically located	50 US States	All but California
Bank Charter Class	Classification code assigned by the FDIC based on the institution's charter type (commercial bank or savings institution), charter agent (state or federal), Federal Reserve membership status (Fed member, Fed nonmember) and its primary federal regulator	Commercial bank supervised by the OCC (N), commercial bank supervised by the Federal Reserve (SM), commercial bank supervised by the FDIC (NM), saving bank supervised by the FDIC (SB), savings association supervised buy the OTS (SA)	NM
Chartering Agency	The type of chartering authority	OCC or State	State
FDIC Supervisory Region	One of the six FDIC Supervisory Regions	Atlanta, Chicago, Dallas, Kansas City, New York, San Francisco	San Francisco
Asset Concentration Hierarchy	Institution's primary specialization in terms of asset concentration	Agricultural, Credit card, Commercial lending, Mortgage Lending, Consumer Lending, Other Specialized (<1$B), All other (<1$B), All other (>1$B)	Commercial Lending
OCC District	OCC District where the institution is physically located (see Section G in the appendix)	Northeastern, Southern, Central, Western	Western
Bank Holding Company	Whether the institution is a member of a multibank holding company	Yes, No	No
Regulator	Federal regulator	FDIC, Federal Reserve Board, Office of the Comptroller of the Currency	FDIC
Ownership type	Whether the institution is owned by shareholders or not	Stock, Non-stock	Stock
Interstate Branches	Whether the institution has branches in more than one state	Yes, No	No
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 urbanized area with population $\geq$50,000?	Yes, No	No

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

4.3.2 OCC district

We also found the geographical location of the institution to be significantly correlated with its sharing practices. Table 16 in the appendix contains detailed results of how practices vary across OCC regions. One possible explanation of these results is that state laws significantly impact sharing practices. In particular, Negroni and Kromer found that certain states' laws favor opt-in approaches [25].

Only 32% of institutions in the Northeastern region don't share customers' information for their own marketing purposes, while 64% share without offering an opt-out. In contrast, the proportions of companies in the Southern region that share and do not offer an opt-out (49%) and do not share (48%) information are roughly equal. We also found differences in sharing for joint marketing. Whereas 32% of institutions in the Northeastern region share for joint marketing without offering an opt-out, only 20% 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 customers in those regions.

Factor	Control category	Own marketing	Joint marketing	Affiliates' (Trans.)	Affiliates' (Credit.)	Affiliates' marketing
OCC District	Western	↓	↓	↑	↑	↑
Offices	NA	↑	↑	↑	↑	↑
Bank Holding Company	No bank holding company	↑	↑	↑	↑	↑
Trust Powers	No powers	none	↑	↑	↑	↑
Interstate Branches	No branches	↑	↑	↑	↑	none
Metro Statistical Area	No metro area	↑	none	↑	↑	↑
State Name	All but California	none	↓	↑	none	↓
Asset Concentration Hierarchy	Commercial Lending	↓	↑ & ↓	none	none	none
FDIC Supervisory Region	San Francisco	↑	↑	none	none	none
Bank Charter Class	Commercial bank, FDIC	↑	none	none	none	none

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. Sharing "for everyday business purposes" or "for non-affiliates to market to you" were not significantly correlated with the factors evaluated.

4.3.3 Other factors

Those institutions that are part of a bank holding company (BHC) and institutions with interstate branches said at higher rates that they share data. In particular, 33% of BHC institutions said they share for joint marketing without offering an opt-out, versus 21% of non-BHC institutions. Similarly, 48% of BHC institutions said they share with affiliates for marketing purposes, compared with 24% of non-BHC institutions. Detailed results are shown in Table 18 in the appendix.

Although one could imagine that an institution with interstate branches would need to comply with many different states' regulations, limiting its sharing practices, we found the opposite. A larger fraction (41%) of institutions with interstate branches said they share for joint marketing purposes without offering an opt-out, as opposed to those without interstate branches (20%).

4.4 Problems with the model privacy form

During our manual analyses of the model-privacy-form policies during the development of our parser, and again when we verified our parser's accuracy, we noticed deviations from both the letter and the goal of the model privacy form. In this section, we first discuss ways in which financial institutions deviated from the specification [27] of the model privacy form. We then show widespread usage of the standard-format disclosure as a replacement for traditional online privacy policies, rather than as a supplement.

4.4.1 Contradictions, deviations, typos, omissions

As we iteratively improved our parser, we noticed a number of issues, both small and large. Logical inconsistencies in the disclosure table were particularly confusing for consumers. One egregious example was answering "Yes" to "Does *name* share" and answering "We do not share" to "Can you limit this sharing?" in a single row. As shown in Figure 3, Geneva State Bank (`genevastatebank.com`) was among 15 different 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."

While we would argue that logical inconsistencies are a major issue in communicating with consumers, a number of more minor issues cropped up. For instance, we designed our parser to be robust to small differences in wording, such as by ignoring capitalization, considering most punctuation to be optional, and matching either "non-affiliates" or "nonaffiliates," yet typos in standard-format disclosures caused many of our parsing errors. Most of these typos were small, yet caused problems since our regular expressions searched for particular wording. 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." In many cases, institutions used the model privacy form as their website's privacy policy, replacing the form's headers with the bank's logo and other branding.

Many institutions invented their own wording, despite the model specifications [27]. 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 [27].

Reasons we can share your personal information	Does Geneva State Bank 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	We don't share
For our marketing purposes - to offer our products and services to you	Yes	We don't share
For joint marketing with other financial companies	Yes	We don't share

Figure 3: Geneva 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.

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 the standard-format disclosure in their 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.

4.4.2 *Standard-format disclosure as sole policy*

In our manual analysis, we noticed a number of institutions using the standard-format disclosure on their website in place of an online privacy policy. Because it would be intractable to visit thousands of websites manually, we investigated this phenomenon on a smaller scale by visiting the websites of the previously described random sample of 50 institutions.

We visited each institution's website and noted whether the model privacy form was used as a supplement to a standard website privacy policy, as a complete replacement, or not at all. We found that only 19 of the 50 institutions in our random sample (38%) had on online privacy policy separate from the standard-format disclosure.

We also examined the file format for the model privacy form and found both HTML and PDF versions to be common. Of the 50 random institutions, 40% had HTML disclosures, 24% had PDF disclosures, and 32% had both. Two other institutions (4%) did not provide a clear link to a disclosure on the site itself, but a PDF disclosure could be found when doing a Google search.

5. DISCUSSION

A major advantage of all standardized privacy disclosures is that they enable the direct comparison of companies' privacy practices. In this particular study, we put this theoretical advantage into action and compared privacy practices of 3,422 financial institutions listed by the FDIC in the United States, as well as the institutions on consumer-advice lists of 100 largest banks and 11 top credit card companies. A privacy pessimist might have approached such an exercise assuming that all financial institutions have comparable (and perhaps poor) privacy practices, while slightly more optimistic expectations might still have suggested that all financial institutions in a particular industry (e.g., "credit cards" or "savings banks") would have similar privacy practices.

Instead, we found stark differences in data-sharing practices across financial institutions, even within the same industry and among companies on the same consumer-advice lists. Some institutions were more privacy-protective and did not share consumers' personal information for purposes like marketing, even though 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.

Alongside the differences we observed in data-sharing practices across institutions in the same category of bank, we found significant correlations between institutions' characteristics and privacy practices. For instance, we found that large companies and those with branches in multiple states were more likely to share data. We also found that financial institutions in some geographic regions, such as the northeastern United States, share data at a higher rate. While a number of factors ranging from differences in tax laws to state-level financial regulations might explain these differences, we believe that the interaction between the size or geographic location of a financial institution and its privacy practices warrants further investigation.

Furthermore, our large-scale analysis enabled us to observe how financial regulation might impact consumer privacy protections in practice. The disclosure table in the model privacy form provides an interesting test case for this idea. This disclosure table lists six reasons for sharing consumers' personal information. In three of these cases, institutions were required to provide consumers a way to limit sharing [27]. In violation of the FCRA, between 4 and 19 institutions in each case shared data, yet reported that consumers could not limit sharing.

The proportion of institutions providing or not providing opt-outs was much different for the three types of sharing for which institutions were not required to provide an opt-out. In these three cases, between 52 and 86 institutions provided

an opt-out when sharing data, providing consumers choice even when not required to do so. In contrast, between 659 and 1,898 institutions shared data without offering an opt-out, which they were permitted to do.

Overall, our results showed that consumers do have the option to do business with more privacy-protective financial institutions, for some categories of financial services, if they so choose. Our analysis also suggests that privacy-friendly choices may be harder to come by for some types of services, and in some regions of the country.

The model privacy form we investigated enables consumers to compare two or more institutions' privacy practices directly, with the same information located in the same place on each disclosure, just as we did in an automated fashion. We noted that a strength of this particular privacy notice is the disclosure table. We found substantial differences in privacy practices across institutions simply by examining this table, suggesting that consumers can similarly be empowered to compare institutions' privacy practices.

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 these comparisons presents a major barrier. For instance, one can imagine an online database that helps consumers search for or compare financial institutions, perhaps similar to prior search engines that have been designed to present privacy-relevant information.[3] One can similarly imagine financial institutions with consumer-friendly privacy practices emphasizing this fact and perhaps using privacy 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 [34], and it stands to reason that they might similarly favor financial institutions with exemplary privacy practices.

Unfortunately, we also found 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 unsurprising and 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 a bank chose *not to* collect a consumer's account balance when he or she used his or her credit or debit card, for example. This realization suggests that these particular parts of the model privacy form are not very informative to consumers, who would likely be more concerned by 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 [23], 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 [27] 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.

As a final thought, our analysis of the model privacy form, particularly the instances of non-compliance with the GLB Act that we discovered, calls into question current oversight mechanisms for these financial institutions' privacy practices. Simply relying on a computer program that we wrote to crawl the Internet for the model privacy form, notably without any ability to audit companies or request additional information on a large scale, we uncovered more than twenty companies whose self-reported data-sharing practices appear to violate federal regulation. We also uncovered many more companies whose privacy notices deviated from the required specification [27] in both small and large ways, as well as over a dozen companies that made self-contradictory disclosures. If we as academics can quickly uncover these issues, why have regulators who are charged with overseeing these financial institutions not already done so?

[3]For instance, PrivacyFinder. `http://privacyfinder.org/`

6. 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] V. Boyd. Financial privacy in the United States and the European Union: A path to transatlantic regulatory harmonization. *Berkeley J. Int'l L.*, 24:939, 2006.

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

[6] L. F. Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice, 2012.

[7] 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.

[8] FDIC. Institution directory. http://www2.fdic.gov/IDASP/, Accessed February 26, 2013.

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

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

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

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

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

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

[15] O. Ireland and R. Howell. The fear factor: Privacy, fear, and the changing hegemony of the American people and the right to privacy. *NCJ Int'l L. & Com. Reg.*, 29:671, 2003.

[16] E. J. Janger and P. M. Schwartz. Gramm-Leach-Bliley Act, information privacy, and the limits of default rules, the. *Minn. L. Rev.*, 86, 2001.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] J. R. Macey. The business of banking: Before and after Gramm-Leach-Bliley. *J. Corp. L.*, 25:691, 1999.

[23] 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.

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

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

[26] G. T. Nojeim. Financial privacy. *NYL Sch. J. Hum. Rts.*, 17:81, 2000.

[27] OCC, Board, FDIC, OTS, NCUA, FTC, CFTC, and SEC. Final model privacy form under the Gramm-Leach-Bliley Act. Federal Register, December 2009.

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

[29] 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.

[30] X. Sheng and L. F. Cranor. An evaluation of the effect of us financial privacy legislation through the analysis of privacy policies. *ISJLP*, 2:943, 2005.

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

[32] 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.

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

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

[35] B. Ur, M. Sleeper, and L. F. Cranor. {Privacy, Privacidad, Приватност} policies in social media: Providing translated privacy notice. *ISJLP*, 9(2), 2013.

[36] US Financial Regulators. Interagency financial institution web site privacy survey report. Technical report, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Comptroller of the Currency, Office of Thrift Supervision, 1999.

[37] U.S.C. Gramm-Leach-Bliley Act. Pub. L. No. 106-102, 113 Stat. 1338.

[38] L. J. White. The Gramm-Leach-Bliley Act of 1999: A bridge too far-or not far enough. *Suffolk UL Rev.*, 43:937, 2009.

APPENDIX

A. DETAILED RESULTS OF CRAWLING AND PARSING POLICIES

# elements matched	# files
(File conversion error)	805
0	32,690
1	12,923
2	1,442
3	484
4	97
5	22
6	8
7	6
8	3
9	9
10	5
11	6
12	5
13	7
14	21
15	17
16	20
17	18
18	17
19	32
20	35
21	60
22	108
23	334
24	1,087
25	2,303

Table 7: The number of files in our set of 52,564 for which a particular number of elements (out of 25 selected headers and phrases contained in the standard-format policy) was parsed. This distribution was bimodal, with peaks on the lower and upper extremes of the scale representing, respectively, files that almost certainly were not standard-format policies and those that likely were.

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 automated evaluation, we observed the expected number of rows in the disclosure table of most notices we parsed, as shown in Table 8. 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 disclosure. For instance, we parsed the name of the bank from the header "What does *institution name* do with your personal information?" This phrase was observed and parsed in 3,299 (96.4%) of the policies. Many of the policies for which this section was not recognized omitted this section, instead including the institution's logo or other non-standard identifying information. The "Who we are...Who is providing this notice?" section was observed at an even lower rate; only 1,803 (52.7%) of the policies appeared 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" [27]. 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 2,416 (70.6%) 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 [27] 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.

# rows	# institutions	
7	1,094	(32.0%)
6	2,118	(61.9%)
5	118	(3.4%)
4	40	(1.2%)
3	25	(0.7%)
2	10	(0.3%)
1	5	(0.1%)
0	12	(0.4%)

Table 8: The number of rows of the disclosure table parsed. The disclosure table contained 7 rows, one of which was optional. We parsed either 6 or 7 rows for 93.9% of the 3,422 institutions.

C. PRACTICES THAT APPEAR TO VIOLATE THE FCRA

"**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" [27]. The following institutions stated that they shared for this purpose, yet said that consumers cannot limit this sharing:

- 1st United Bank (1stunitedbankfl.com)
- Abacus Federal Savings Bank (abacusbank.com)
- ACCESSbank (accessbank.com)
- A.J. Smith Federal Savings Bank (ajsmithbank.com)
- American National Bank (amnat.com)
- Bank of Star Valley (bosv.com)
- Brentwood Bank (brentwoodbank.com)
- Citizens State Bank of Loyal (csbloyal.com)
- Community State Bank (bankcommunitystate.com)
- First County Bank (firstcountybank.com)
- First National Bank of LaGrange (fnblg.com)
- Kansas State Bank (mykansasstatebank.com)
- Midwest Independent Bank (mibanc.com)
- NorthStar Bank (northstarbankiowa.com)
- ParkeBank (parkebankcom10.pdf)
- State Bank of Illinois (mysbi.com)
- Stonebridge Bank (stonebridgebank.biz)
- SunMark Community Bank (sunmarkbank.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:

- Citizens State Bank of Loyal (csbloyal.com)
- Farmers State Bank (fsbelmwood.com)
- Hilltop Community Bank (hilltopcommunitybank.com)
- Torrington Savings Bank (torringtonsavings.com)

"**For nonaffiliates to market to you**. This reason incorporates sharing described in §§ 716.7 and 716.10(a) of this part. 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:

- 1st United Bank (1stunitedbankfl.com)
- Abacus Federal Savings Bank (abacusbank.com)
- First National Bank in Amboy (fnbamboy.com)
- Mitchell Bank (mitchellbank.com)

D. WHAT INFORMATION IS COLLECTED

As part of the model privacy form, institutions specified what types of information they collect from a list of twenty-four types of personal information. Over 90% of the institutions we examined listed six or more types of information (Table 9).

# data types	# institutions	
≥7	53	1.5%
6	3,058	89.4%
5	190	5.6%
4	55	1.6%
3	24	0.7%
2	10	0.3%
1	11	0.3%
0	21	0.6%

Table 9: Number of types of data disclosed by financial institutions. The model privacy form states that institutions must list exactly six types.

We present the counts for each of the 24 terms in Table 10. 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.

Interestingly, we observed many instances of institutions inventing their own wordings, contrary to the specification of the model privacy form [27]. For instance, Congressional Bank (`congressionalbank.com`) listed "Date of Birth," "Driver's License," and "Passport" even though none of these three types of information are among those 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)" as types of information it collects. While it was not surprising that a financial institution might collect any of this data, none of these five items was among the 23 items listed in the specification [27]. Our parser searched for these three items, though we did not include these items in our total counts. Overall, 62 institutions said they collected "address," 40 said they collected "name," and 6 said they collected a consumer's "phone number." Although institutions were required to list that they collect a consumer's "Social Security number," 2.3% of the institutions we examined did not do so.

Type of information	# institutions
Social Security number	3,342
Account balance	3,097
Payment history	2,758
Credit history	2,675
Income	1,859
Credit score	1,450
Transaction history	1,271
Checking account information	818
Overdraft history	724
Account transaction	684
Transaction or loss history	319
Wire transfer instructions	304
Employment information	235
Assets	199
Credit card or other debt	110
Mortgage rates and payments	103
Investment experience	23
Retirement assets	13
Insurance claim history	11
Medical information	7
Purchase history	7
Risk tolerance	7
Credit-based insurance score	2
Medical-related debts	0

Table 10: Types of personal information financial institutions say they collect. We note that few of these types of personal information seem abnormal for a financial institution to collect, raising the question of what this particular disclosure communicates to users.

E. WHEN INFORMATION IS COLLECTED

As described in Section 4.1.5, institutions were required to list exactly five occasions on which they collect information. Table 11 shows the number of institutions listing different numbers of occasions. Of the 3,422 institutions, 85.0% listed five occasions when they collect consumers' information, as specified by the model privacy form [27]. Some institutions, however, listed up to 11 different occasions on which they collect information. While 61 institutions (1.8%) listed more occasions than required, we observed fewer than the required number for 13.2% of institutions.

# occasions	# institutions	
≥6	61	1.8%
5	2,908	85.0%
4	305	8.9%
3	83	2.4%
2	40	1.2%
1	12	0.4%
0	13	0.4%

Table 11: Number of occasions listed for when an institution collects personal information.

Occasion	# institutions
Open an account	3,280
Apply for a loan	3,094
Use your credit or debit card	1,846
Deposit money	1,555
Pay your bills	1,542
Make deposits or withdrawals from your account	1,039
Give us your contact information	701
Show your driver's license	623
Make a wire transfer	590
Provide account information	383
Give us your income information	285
Provide employment information	257
Show your government-issued ID	244
Pay us by check	145
Apply for financing	133
Provide your mortgage information	110
Seek advice about your investments	69
Apply for insurance	64
Give us your employment history	64
Give us your wage statements	59
Tell us about your investment or retirement portfolio	21
Enter into an investment advisory contract	17
Seek financial or tax advice	10
Tell us where to send the money	8
Tell us who receives the money	7
Pay insurance premiums	6
Direct us to buy securities	4
Direct us to sell your securities	4
File an insurance claim	3
Apply for a lease	3
Buy securities from us	2
Tell us about your investment or retirement earnings	1
Order a commodity futures or option trade	1
Sell securities to us	0

Table 12: 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.

F. SHARING PRACTICES OF CREDIT CARD COMPANIES AND LARGE BANKS

Institution name	Everyday business purposes	Marketing purposes	Joint marketing	Affiliates - Trans. & Exp.	Affiliates - Credit.	Affiliates' marketing	Non-affiliates' marketing
Capital One, Chase, Discover Bank, and HSBC	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Bank of America and Citi	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Missing	Share, opt-out
American Express	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Barclays Bank	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, no opt-out	Share, opt-out	Missing	Don't share
GE Capital	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Don't share	Missing	Don't share
U.S. Bank	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Share, opt-out	Missing	Don't share
Wells Fargo	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share

Table 13: Sharing practices of credit-card companies that appear on a J.D. Power & Associates list [17]. 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 the reasons for which they share data. For instance, GE Capital says that it shares data for only three of the seven purposes listed, whereas other institutions say they share for all seven purposes.

Institution name	Everyday business purposes	Marketing purposes	Joint marketing	Affiliates - Trans. & Exp.	Affiliates - Credit.	Affiliates' marketing	Non-affiliates' marketing
1st Source	Share, no opt-out	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share	Don't share
Associated Banc-Corp	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
BancFirst	Share, no opt-out	Don't share	Don't share	Don't share	Don't share	Missing	Don't share
BancorpSouth	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Bank of America	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Missing	Share, opt-out
Bank of Hawaii	Share, no opt-out	Share, opt-out	Share, opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Beneficial Bank	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
BOK Financial	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Don't share	Share, opt-out	Share, opt-out
Brookline Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share
Capital Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Capital One	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Chase	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Chemical Bank	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share	Missing	Don't share
Citi	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Missing	Share, opt-out
Cole Taylor Bank	Share, no opt-out	Share, no opt-out	Don't share	Share, opt-out	Share, opt-out	Share, opt-out	Don't share
Columbia State Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Don't share	Missing	Don't share
Comerica	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Commerce Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out	Don't share
Community Bank	Share, no opt-out	Don't share	Don't share	Don't share	Don't share	Missing	Don't share
Doral	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
East West Bank	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Don't share	Missing	Don't share
Farmers & Merchants Bank	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share	Don't share	Don't share
Fifth Third Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
First Bancorp	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
First Citizens Bancshares	Share, no opt-out	Share, opt-out	Share, opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
First Financial Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out	Don't share
First Horizon	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
First Interstate Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Don't share	Missing	Don't share
FirstMerit	Share, no opt-out	Share, opt-out	Share, opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
First Niagara	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
First Republic Bank	Share, no opt-out	Missing	Don't share	Missing	Missing	Missing	Don't share
Frost	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share

Continued from previous page

Institution name	Everyday business purposes	Marketing purposes	Joint marketing	Affiliates - Trans. & Exp.	Affiliates - Credit.	Affiliates' marketing	Non-affiliates' marketing
Glacier Bancorp	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Don't share	Missing	Don't share
Hancock Holding	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out	Don't share
Huntington	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Iberia Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Independent Bank	Share, no opt-out	Don't share	Don't share	Don't share	Share, opt-out	Missing	Don't share
Investors Bank	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Keycorp	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Missing	Don't share
M&T Bank Corporation	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
MB Financial	Share, no opt-out	Share, opt-out	Share, opt-out	Share, no opt-out	Don't share	Share, opt-out	Don't share
National Penn Bancshares	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
National Bank Holding	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share	Missing	Don't share
NBT Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out	Don't share
New York Community Bancorp	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Northern Trust	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, no opt-out
Old National	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out	Don't share
Pinnacle Bank	Share, no opt-out	Share, opt-out	Don't share	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
PNC Bank	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Popular	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Private Bancorp	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share
Regions Financial	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Signature Bank	Share, no opt-out	Don't share	Don't share	Don't share	Don't share	Missing	Don't share
State Street Bank	Share, no opt-out	Don't share	Don't share	Don't share	Don't share	Missing	Don't share
Sterling Bank	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share	Missing	Don't share
Suntrust	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Susquehanna Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Synovus Financial	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
TCF Financial	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Share, opt-out
Texas Capital Bank	Share, no opt-out	Don't share	Don't share	Don't share	Don't share	Missing	Don't share
West America	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Don't share	Missing	Don't share
Western Alliance Bancorp	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share	Don't share	Don't share
TFS	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Trustmark	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share

Continued from previous page

Institution name	Everyday business purposes	Marketing purposes	Joint marketing	Affiliates - Trans. & Exp.	Affiliates - Credit.	Affiliates' marketing	Non-affiliates' marketing
UMB Financial	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
United Community Bank	Share, no opt-out	Share, no opt-out	Don't share	Don't share	Don't share	Missing	Don't share
Valley National Bancorp	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Don't share	Missing	Don't share
Webster Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
Wells Fargo	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share
WesBanco	Share, no opt-out	Share, opt-out	Share, opt-out	Share, no opt-out	Don't share	Share, opt-out	Don't share
Valley National Bancorp	Share, no opt-out	Share, no opt-out	Don't share	Share, no opt-out	Don't share	Missing	Don't share
Wintrust Financial	Share, no opt-out	Share, no opt-out	Don't share	Share, opt-out	Share, opt-out	Share, opt-out	Don't share
Zions First National Bank	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, no opt-out	Share, opt-out	Share, opt-out	Don't share

Table 14: The sharing practices of the 73 financial institutions on Forbes' list of "100 best banks" [3] for which we found a privacy disclosure using the model privacy form.

G. LOGISTIC REGRESSION MODELS

The OCC districts as used in our logistic regression models:

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

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	Odds ratio	β	Z	P>|Z|	Odds ratio 95% CI
For our marketing purposes					
OCC District (Central)	0.60	-0.51	-2.97	0.003	[0.43, 0.84]
Offices	1.06	0.05	8.70	<0.001	[1.04, 1.07]
Bank Holding Company	2.13	0.75	6.21	<0.001	[1.67, 2.70]
Interstate Branches	1.36	0.30	2.02	0.040	[1.00, 1.83]
Metro Statistical Area	1.31	0.27	3.24	0.001	[1.11, 1.55]
Combined Statistical Area	1.24	0.21	2.34	0.019	[1.03, 1.50]
State Name	1.24	0.21	2.34	0.019	[1.03, 1.50]
Specialization (Agricultural)	0.59	-0.52	-4.39	<0.001	[0.47, 0.74]
Specialization (All other <1$B)	0.61	-0.49	-3.83	<0.001	[0.48, 0.79]
FDIC Region (Chicago)	1.84	0.61	2.68	0.007	[1.17, 2.88]
FDIC Region (Kansas City)	1.79	0.58	3.53	<0.001	[1.29, 2.47]
Bank Charter Class (N)	1.29	0.25	2.40	0.016	[1.04, 1.59]
For joint marketing with other financial companies					
OCC District (Central)	0.54	-0.61	-2.56	0.010	[0.34, 0.86]
Offices	1.00	0.00	1.95	0.050	[0.99, 1.00]
Bank Holding Company	1.76	0.56	4.77	<0.001	[1.39, 2.22]
Trust Powers	1.79	0.58	6.29	<0.001	[1.49, 2.15]
Interstate Branches	2.33	0.84	6.82	<0.001	[1.83, 2.98]
Combined Statistical Area	1.28	0.24	2.34	0.019	[1.04, 1.50]
State Name	0.45	-0.79	-2.42	0.015	[0.23, 0.85]
Specialization (Agricultural)	0.47	-0.75	-5.31	<0.001	[0.35, 0.62]
Specialization (All other <1$B)	0.47	-0.75	-4.56	<0.001	[0.34, 0.65]
Specialization (All other >1$B)	3.04	1.11	2.54	0.011	[1.29, 7.18]
FDIC Region (Chicago)	2.19	0.78	2.46	0.014	[1.17, 4.09]
For our affiliates' everyday business purposes– transactions and experiences					
OCC District (Northeastern)	1.84	0.60	4.08	<0.001	[1.37, 2.47]
OCC District (Central)	1.31	0.27	2.00	0.045	[1.01, 1.72]
Offices	1.01	0.01	2.26	0.024	[1.00, 1.01]
Bank Holding Company	5.37	1.68	14.14	<0.001	[4.26, 6.79]
Trust Powers	1.64	0.49	4.79	<0.001	[1.34, 2.01]
Interstate Branches	1.46	0.37	2.60	0.009	[1.09, 1.96]
Metro Statistical Area	1.35	0.30	2.33	0.020	[1.04, 1.74]
State Name	1.88	0.63	2.57	0.010	[1.16, 3.06]
For our affiliates' everyday business purposes– creditworthiness					
OCC District (Northeastern)	2.01	0.69	3.65	<0.001	[1.38, 2.94]
Offices	1.01	0.01	4.29	<0.001	[1.01, 1.01]
Bank Holding Company	3.64	1.29	8.17	<0.001	[2.67, 4.97]
Trust Powers	1.83	0.60	4.30	<0.001	[1.39, 2.42]
Interstate Branches	1.70	0.53	2.85	0.004	[1.18, 2.45]
Metro Statistical Area	1.92	0.65	3.18	0.001	[1.28, 2.88]
For our affiliates to market to you					
OCC District (Northeastern)	2.52	0.92	4.06	<0.001	[1.61, 3.94]
Offices	1.03	0.03	4.96	<0.001	[1.01, 1.04]
Bank Holding Company	2.52	0.92	4.89	<0.001	[1.74, 3.65]
Trust Powers	1.79	0.58	3.62	<0.001	[1.30, 2.46]
Metro Statistical Area	1.86	0.62	2.81	0.005	[1.20, 2.89]
Combined Statistical Area	1.86	0.62	2.38	0.017	[1.11, 3.10]
State Name	0.24	-1.42	-2.42	0.015	[0.08, 0.76]
For nonaffiliates to market to you					
Trust Powers	1.65	0.50	2.47	0.014	[1.10, 2.47]
Specialization (Agricultural)	0.55	-0.59	-1.96	0.050	[0.30, 1.00]
Specialization (All other <1$B)	0.39	-0.94	-1.99	0.047	[0.15, 0.98]

Table 15: Results from the logistic regression models corresponding to the different types of sharing practices. Only those variables significant at α=0.05 are shown.

H. DETAILED SHARING PRACTICES

Sharing practice	Southern		Central		Western		Northeastern	
Financial institutions' own marketing purposes								
Don't Share	446	48.3%	394	43.4%	338	37.1%	195	31.7%
Share & Opt-Out	21	2.3%	24	2.7%	16	1.8%	24	3.9%
Share & No Opt-Out	457	49.5%	489	54.0%	556	61.1%	396	64.4%
Joint marketing with other financial companies								
Don't Share	721	78.0%	702	77.7%	703	77.3%	392	63.8%
Share & Opt-Out	19	2.0%	23	2.5%	21	2.3%	23	3.8%
Share & No Opt-Out	185	20.0%	179	19.8%	185	20.3%	199	32.4%
For affiliates' everyday business purposes (transactions and experiences)								
Don't Share	760	82.6%	713	79.1%	704	78.6%	441	72.1%
Share & Opt-Out	11	1.2%	16	1.8%	9	1.0%	16	2.6%
Share & No Opt-Out	149	16.2%	172	19.1%	183	20.4%	155	25.3%
For affiliates' everyday business purposes (creditworthiness)								
Don't Share	850	92.3%	839	93.0%	822	91.2%	529	86.3%
Share & Opt-Out	68	7.4%	57	6.3%	66	7.4%	80	13.0%
Share & No Opt-Out	3	0.3%	6	0.7%	8	0.9%	4	0.7%
For affiliates to market to you								
Don't Share	202	71.6%	247	79.9%	257	75.8%	128	54.2%
Share & Opt-Out	80	28.4%	60	19.4%	82	24.2%	106	44.9%
Share & No Opt-Out	0	0.0%	2	0.7%	0	0.0%	2	0.9%

Table 16: Sharing practices by the OCC District where the institution is physically located. Overall, institutions in the Southern OCC Region shared for the fewest different reasons. Institutions in the Western and Northeastern OCC Regions shared for the largest number of reasons. Only those variables significant at α=0.05 are shown.

Sharing Practice	Commercial bank, FDIC		Commercial bank, Federal Reserve		Commercial bank, OCC		Savings association, OTS		Savings bank, FDIC	
Financial institutions' own marketing purposes										
Don't Share	867	44.5%	160	37.0%	197	37.0%	82	35.1%	67	32.2%
Share, Opt-Out	50	2.6%	14	3.2%	9	1.7%	4	1.7%	8	3.9%
Share, No Opt-Out	1,030	52.9%	259	59.8%	329	61.5%	147	63.1%	133	63.9%

Table 17: Sharing practices by bank charter class. Relative to other types of banks, commercial banks supervised by the FDIC most frequently did not share data. Only the single variable significant at α=0.05 is shown.

Sharing practice	Belong to a bank holding company?			
	No		Yes	
Financial institutions' own marketing purposes				
Don't Share	1,255	43.2%	118	26.3%
Share, Opt-Out	71	2.4%	14	3.1%
Share, No Opt-Out	1,581	54.4%	317	70.6%
Joint marketing with other financial institutions				
Don't Share	2,229	76.8%	289	64.5%
Share, Opt-Out	74	2.6%	12	2.7%
Share, No Opt-Out	601	20.7%	147	32.8%
For affiliates' everyday business purposes (transactions and experiences)				
Don't Share	2,396	83.2%	222	49.6%
Share, Opt-Out	49	1.7%	3	0.7%
Share, No Opt-Out	436	15.1%	223	49.8%
For affiliates' everyday business purposes (creditworthiness)				
Don't Share	2,692	93.3%	348	77.7%
Share, Opt-Out	177	6.1%	94	20.1%
Share, No Opt-Out	15	0.5%	6	1.3%
For affiliates to market to you				
Don't Share	718	76.0%	116	52.5%
Share, Opt-Out	223	23.6%	105	47.5%
Share, No Opt-Out	4	0.4%	0	0.0%

Table 18: Comparing sharing practices of institutions that belong to bank holding companies and those that do not. Overall, institutions that are part of bank holding companies share more than those that are not members. Only those variables significant at α=0.05 are shown.

Sharing practice	Have interstate branches?			
	No		Yes	
Financial institutions' own marketing purposes				
Don't Share	1,295	43.7%	78	19.9%
Share & Opt-Out	61	2.1%	24	6.1%
Share & No Opt-Out	1,608	54.3%	290	74.0%
Joint marketing with other financial institutions				
Don't Share	2,317	78.2%	201	51.7%
Share & Opt-Out	58	2.0%	28	7.2%
Share & No Opt-Out	588	19.8%	160	41.1%
For affiliates' everyday business purposes (transactions and experiences)				
Don't Share	2,393	81.5%	225	57.5%
Share & Opt-Out	34	1.2%	18	4.6%
Share & No Opt-Out	511	17.4%	148	37.9%
For affiliates' everyday business purposes (creditworthiness)				
Don't Share	2,738	93.1%	382	77.2%
Share & Opt-Out	185	6.3%	86	22.0%
Share & No Opt-Out	18	0.6%	3	0.8%

Table 19: Sharing practices of institutions with interstate branches. Overall, institutions with interstate branches share more than those without interstate branches. Only those variables significant at α=0.05 are shown.

Sharing practice	All other (<1$B)		Agricultural		Other specialized (<1$B)		Mortgage lending		Commercial lending		Consumer lending		All other (>1$B)		Credit card	
Financial institutions' own marketing purposes																
Don't Share	181	54.7%	314	53.0%	68	46.3%	120	41.0%	680	35.0%	7	33.0%	2	6.4%	0	0.0%
Share, Opt-Out	2	0.6%	9	1.5%	2	1.4%	7	2.4%	63	3.3%	0	0.0%	2	6.5%	0	0.0%
Share, No Opt-Out	148	44.7%	269	45.4%	77	52.4%	166	56.7%	1,191	61.5%	14	66.7%	27	87.1%	6	100.0%
Joint marketing with other financial institutions																
Don't Share	280	84.6%	509	85.1%	122	83.6%	222	75.5%	1,355	70.4%	18	85.7%	9	30.0%	2	33.3%
Share, Opt-Out	2	0.6%	9	1.5%	0	0.0%	6	2.0%	68	3.5%	0	0.0%	1	3.3%	0	0.0%
Share, No Opt-Out	49	14.8%	80	13.4%	24	16.4%	66	22.4%	502	26.1%	3	14.3%	20	66.7%	4	66.7%
For non-affiliates to market to you																
Don't Share	322	98.5%	582	97.8%	145	100.0%	276	95.8%	1,817	96.0%	20	100.0%	27	90.0%	2	40.0%
Share, Opt-Out	5	1.5%	12	2.0%	0	0.0%	11	3.8%	72	3.8%	0	0.0%	3	10.0%	3	60.0%
Share, No Opt-Out	0	0.0%	1	0.2%	0	0.0%	1	0.3%	3	0.2%	0	0.0%	0	0.0%	0	0.0%

Table 20: Sharing practices by primary specialization in terms of asset concentrations. Financial institutions with agricultural specializations share the least (47%). Consumer lending and commercial lending institutions share the most, with 67% and 65%, respectively.

I. MODEL PRIVACY FORM

This page and the one that follows contain a screenshot of the most comprehensive version of the model privacy form. Institutions that do not offer opt-outs may use a reduced version that omits the "mail-in form" and "to limit sharing" section [27]. Text in pink is meant to be replaced with information, and the cells of the disclosure table ("reasons we can share your personal information") must be populated with the institution's practices.

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]

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]