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

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

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

CCS Concepts: • **Information systems** → *Online banking*; • **Security and privacy** → *Economics of security and privacy*

Additional Key Words and Phrases: Privacy, financial industry, bank, WWW, web, disclosure, data sharing, large-scale comparison, standard format, opt-out

ACM Reference Format:
Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur. 2016. A large-scale evaluation of U.S. financial institutions' standardized privacy notices. ACM Trans. Web 10, 3, Article 17 (August 2016), 33 pages.
DOI: http://dx.doi.org/10.1145/2911988

1. INTRODUCTION

When the United States Congress was considering the Gramm-Leach-Bliley Act of 1999 (GLBA), allowing the consolidation of different types of financial institutions, privacy advocates argued that it was important to notify consumers about these institutions' data practices and allow consumers to limit the use and sharing of their data [Ireland

---

This article is an extended version of the following: Lorrie Faith Cranor, Kelly Idouchi, Pedro Giovanni Leon, Manya Sleeper, Blase Ur. Are They Actually Any Different? Comparing Thousands of Financial Institutions' Privacy Practices. In *Workshop on the Economics of Information Security* (WEIS'13), 2013.

This work was supported in part by the National Science Foundation under its Secure and Trustworthy Computing (SaTC) initiative grant 1330596 for "TWC SBE: Option: Frontier: Collaborative: Towards Effective Web Privacy Notice and Choice: A Multi-Disciplinary Prospective." This research was also conducted with government support under and awarded by the DoD, Air Force Office of Scientific Research, National Defense Science and Engineering Graduate (NDSEG) Fellowship, 32 CFR 168a.

Authors' addresses: L. F. Cranor (lorrie@cs.cmu.edu), P. G. Leon (pgl@andrew.cmu.edu), and B. Ur (blase@blaseur.com), Carnegie Mellon University, 5000 Forbes Ave., Pittsburgh, PA 15213, USA. Lorrie Faith Cranor (lorrie@cs.cmu.edu) is the contact author.

ACM 1559-1131/2016/08-ART17 $15.00
DOI: http://dx.doi.org/10.1145/2911988

and Howell 2003]. The act passed with a provision mandating annual privacy notices. In the years that followed, these disclosures were widely criticized for being difficult to read and understand [Nader et al. 2001]. In response, eight federal agencies jointly released a *model privacy form* in 2009 [U.S. Federal Register 2009]. This model privacy form, which combined boilerplate text with sections for institutions to fill in regarding their own practices, was designed to "make disclosure of institutions' information sharing practices and consumer choices more transparent" in an easy-to-read format [U.S. Federal Register 2009].

Besides making it easier for consumers to find privacy information, privacy notices that are provided in a standardized format also enable automated, large-scale comparisons of privacy practices. The idea of providing privacy notices in standardized formats has long held great potential for empowering consumers to compare companies' privacy practices. From standards for machine-readable privacy policies, such as the Platform for Privacy Preferences (P3P) [Cranor 2002], to recent attempts to have humans annotate websites' privacy policies and terms of service [Terms of Service; Didn't Read 2015], much time and energy have gone into attempts to provide privacy information in a standardized format. Unfortunately, these initiatives generally do not reach fruition. For instance, websites have been found to misuse machine-readable privacy disclosures [Leon et al. 2010; Reay et al. 2009], while attempts to have humans annotate privacy practices do not scale well.

Although financial institutions in the United States are not required to use the model privacy form to enumerate their privacy practices, the use of this form provides a safe harbor for privacy disclosures under GLBA [U.S. Federal Register 2009]. As a result, financial institutions have incentives to use this model privacy form to make their mandatory privacy disclosures. Throughout this article, we refer to an institution's privacy disclosure using the model privacy form as a *standardized notice*. We found thousands of financial institutions posting a standardized notice on the web, giving us the opportunity to analyze privacy practices across an entire industry.

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

We then compared these 6,191 institutions in terms of their data-sharing practices, consumers' ability to opt out of data sharing, and the personal information the policies state may be collected. To investigate how different factors affect institutions' sharing practices, we further conducted statistical analyses using additional information included in the FDIC list regarding various institutions' characteristics. For additional insight into how competitors compare, we also analyzed the policies of institutions on a Forbes list of the 100 largest banks [Badenhausen 2012] and a J.D. Power survey of credit card satisfaction [J.D. Power & Associates 2012].

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

website[1] for consumers to compare these institutions' privacy practices based on the information we extracted from the standardized notices.

Furthermore, we found that both large institutions and those headquartered in the northeastern region of the United States are more likely to share consumers' personal information for marketing purposes than all other institutions. Finally, we found deficiencies in both the specification and the use of the model privacy form that may counterintuitively limit consumers' access to information about financial institutions' privacy practices.

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

2. BACKGROUND AND RELATED WORK

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

2.1. Privacy Policies

Consumers value the privacy of their personal information [Carrascal et al. 2013], yet it can be difficult for consumers to control this information [Krishnamurthy and Wills 2009]. 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 [OECD 1980] and the U.S. Federal Trade Commission's Fair Information Practice Principles (FIPPs) [FTC 1998]. 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. [2008] found that the clarity and credibility of privacy notices were crucial for influencing consumer trust. When information about privacy is made accessible to consumers, Tsai et al. [2011] found that consumers will pay a premium price to make purchases from more privacy-protective businesses.

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. [2002] found the average privacy policy to require 2 years of college education to comprehend. Similarly, Jensen and Potts [2004] examined 64 privacy policies and found that many were difficult to find and read. The reading level of privacy policies is not the only barrier to comprehension; Ur et al. [2013] found instances of privacy policies being unavailable in a user's language, in contrast to the rest of a website. McDonald and Cranor [2008] 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 his or her browsing.

Well-designed, standardized formats for privacy notice can overcome many of these obstacles. Furthermore, privacy notices can be compared easily if they are presented in a standardized format. Researchers have examined methods for presenting privacy policies in a standardized, usable manner. For example, Kelley et al. [2009] found that displaying privacy policy information in a tabular "nutrition label" format

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

made it easier for users to find information. Even when companies don't provide standardized notice about their privacy practices or terms of use, projects like "Terms of Service; Didn't Read" have used crowdsourcing to put this information into a short, standardized format [Terms of Service; Didn't Read 2015].

Standardized privacy notices—whether human readable or machine readable—help facilitate large-scale comparison and evaluation [Cranor 2012]. 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 [Cranor 2002]. Cranor et al. [2008] 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. Unfortunately, P3P has not been widely adopted [Cranor 2012]. In a different study, Cranor et al. [2008] found high rates of syntax errors among the P3P policies they examined. Furthermore, Leon et al. [2010] 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. Similarly, Reay et al. [2009] found that websites often post P3P policies whose stated practices violate the mandates of their own legal jurisdiction.

2.2. Financial Federal Laws' Privacy Provisions

In this article, we examine financial institutions' annual privacy disclosures that are mandated by GLBA, which was signed into law on November 12, 1999 [Gramm-Leach-Bliley 1999]. GLBA's primary purpose was to encourage competition in the financial services industry by removing barriers that prevented common ownership (affiliation) between commercial banks, investment banks, and insurance businesses [White 2009; Shull 2002; Macey 1999].

Affiliation between different types of financial services companies presented an opportunity for newly affiliated companies to share information. In response to concerns about the privacy of consumer information, Congress included Title V, known as the Privacy Rule, in GLBA. This rule requires financial institutions to provide annual notices of their privacy policies and practices (15 U.S.C. Section 6802–6803). The rule also mandates that customers have the right to opt out of data sharing with nonaffiliated companies. However, the Privacy Rule provides a "joint marketing exception" to the opt-out requirements, allowing nonaffiliated financial companies to share information without offering an opt-out when there exists a formal agreement for marketing financial products or services to a consumer [FTC 2000].

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

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

The provisions of GLBA, the FCRA, and FACTA combine to establish three contexts in which financial institutions must provide notice and the opportunity to opt out. GLBA's Financial Privacy Rule applies to the sharing of consumer financial information with nonaffiliates, the FCRA restricts sharing consumer report information between affiliated companies, and FACTA limits when consumer report information shared between affiliates may be used for marketing [McCorkell and Smith 2009].

2.3. Criticisms of GLBA's Privacy Provisions

The privacy protections offered by GLBA have prompted a range of criticisms. Some critics feel that GLBA offers incomplete or too few privacy protections. For instance, in an examination of GLBA privacy provisions, Janger and Schwartz [2001] conclude that GLBA "leaves the burden of bargaining on the less informed party, the individual consumer". Schiller [2003] also argues that the notice provisions provided by GLBA do not go far enough toward providing privacy protections. She recommends that GLBA further restrict information sharing among affiliates. Freeman [2003] similarly concludes that GLBA was a good start, yet "need[s] further refinement", arguing that the "opt-out" provision has made it unlikely that many customers will take the active steps needed to protect their confidential data. Nojeim [2000] also argues that GLBA is incomplete because it does not prevent the flow of personal information among affiliates and uses an opt-out approach, failing to require consumers' active consent.

Other critics feel that the protections offered by GLBA are an impediment to the free market. Some economists have claimed that "efforts to protect privacy in the financial services industry (and elsewhere) are obstacles to the functioning of optimally efficient markets" [Swire 2003]. Lacker [2002], for example, argues that in a perfectly competitive market, financial privacy would be determined by economic forces regardless of the choice of mechanisms offered. Furletti and Smith [2003] claim that the open sharing of consumer information makes the market more efficient and benefits both financial institutions and consumers. They further claim that laws like the Fair Credit Reporting Act provide sufficient privacy protections for consumers. In counterpoint, Swire [2003] argues that inappropriate disclosure of personal information can easily lead to a "misallocation of resources".

Investigations conducted around the time GLBA came into effect studied the act's initial impact on financial institutions' privacy disclosures. Sheng and Cranor [2005] 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 GLBA, the amount of sharing among affiliates and nonaffiliates increased. Antón et al. [2004] examined privacy statements from nine financial institutions covered by GLBA and concluded that these statements did not comply with the GLBA requirements of conspicuousness and clarity. They suggested the use of a standardized vocabulary to improve the readability of financial institutions' privacy policies.

2.4. Development of the Model Privacy Form

A few years after GLBA was enacted, eight U.S. regulators[2] jointly noted wide variations in the privacy notices financial institutions were sending to consumers. They found these notices "difficult to compare, even among financial institutions with identical practices" and questioned "whether such notices comply with the requirement

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

that they be clear and conspicuous." As a result, regulators started a process to create a standard model for privacy notices that "consumers could more easily use and understand" [U.S. Federal Register 2009]. Financial institutions, researchers, and communications firms took part in this process.

The process of developing a standardized notice began in the summer of 2004. The regulators retained a communications firm, Kleimann Communication Group, to develop a prototype of a standardized notice. To this end, the firm conducted two 10-participant focus groups and 46 individual interviews, releasing a report of their findings in February 2006 [Kleimann Communication Group Inc. 2006]. Notably, the main goal of the prototype notice was to help consumers understand financial institutions' sharing practices, not necessarily to provide a comprehensive list of the types of personal information that financial institutions collect. In March 2007, the regulators issued the prototype for public comment [U.S. Federal Register 2009].

Following public comments on the proposed model form, the regulators commissioned a quantitative survey designed to evaluate the effectiveness of the revised model form. The survey, which was conducted in the spring of 2008, tested comprehension and usability of the model form as compared with three other styles of notice. Notices from three fictitious banks with different sharing practices were tested among 1,032 consumers recruited from five U.S. cities. The prototype outperformed the alternative styles tested [Macro International Inc. 2008].

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

The regulators again commissioned Kleimann Communication Group to conduct validation testing. The firm conducted a seven-participant study and concluded in its February 2009 report that the improvements suggested by Levy and Hastak improved the clarity of opt-out choices without affecting understanding of sharing practices [Kleimann Communication Group Inc. 2009]. Garrison et al. [2012] give a more detailed account of the user testing behind the model forms.

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

2.5. State Laws

U.S. states have enacted a number of laws limiting financial institutions' ability to share financial data. GLBA includes a provision providing that it does not preempt state laws that are consistent with it. State laws that are inconsistent are invalid only to the extent of the inconsistency (15 U.S.C. Section 6807) [Negroni and Kromer 2001; McMahon 2006]. A state law with stronger consumer protections is explicitly not inconsistent (and thus not preempted). Many states have laws that prohibit financial institutions from disclosing customer information unless that disclosure is authorized or required by law or court order (see Proskauer Section 5:6.2 [Mathews 2013] for examples).

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]

Fig. 1. The first page of the model privacy form [U.S. Federal Register 2009]. We extracted and analyzed what information is collected; how information is shared, including whether consumers can limit any type of sharing; and how consumers may limit sharing. The sharing table and text in pink need to be filled in by the financial institution.

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of financial institution] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of financial institution] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account—unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

Fig. 2. The second page of the model privacy form [U.S. Federal Register 2009]. We extracted and analyzed how information is collected, as well as the list of affiliates, nonaffiliates, and joint marketing partners.

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

information to be shared between most types of affiliates only after notice and the opportunity to opt out.

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

3. METHODOLOGY

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

3.1. Obtaining Lists of Financial Institutions

As the first step in searching for U.S. financial institutions' standardized notices based on the model privacy form, we needed a list of these institutions. Having a list of the names and geographic locations of these institutions enabled us to collect standardized notices in a systematic way and minimize confusion between banks with similar names (e.g., multiple, seemingly independent banks were called "First National Bank," "Liberty Bank," "Pinnacle Bank," etc.). To this end, in March 2014, we compiled two complementary lists encompassing a total of 19,329 financial institutions. The first list comprised a number of different types of financial institutions. The second list comprised only federal credit unions, which were absent from the first list.

We created our first list of 12,511 distinct financial institutions by merging lists from the Fed and the FDIC, two of the largest U.S. government agencies related to the financial industry. To obtain the Federal Reserve list of 6,588 financial institutions, we made a Freedom of Information Act (FOIA) request. The list of 6,781 financial institutions insured by the Federal Deposit Insurance Corporation is available online.[3] The FDIC list also includes an institution's characteristics, location, assets, and contact information [FDIC 2014]. We merged these two lists based on each institution's "Research, Statistics, Supervision and Regulation, and Discount and Credit" (RSSD) ID number, removing duplicate entries. The RSSD ID uniquely identifies all institutions that have reporting obligations to the Federal Reserve. Although these two lists overlapped to an extent, we found that many institutions were present on only one of these lists. Following the merging process, our list contained 12,511 financial institutions.

We also made FOIA requests to obtain lists of financial institutions from the other main U.S. government agencies that regulate financial institutions, notably the Consumer Financial Protection Bureau (CFPB) and the Office of the Comptroller of the Currency (OCC). Although these lists together included 101 institutions absent from

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

both the Federal Reserve and FDIC lists, they had much less metadata about the institutions' characteristics. We thus chose to exclude these additional institutions.

Our second list comprised 6,818 credit unions supervised by the National Credit Union Administration (NCUA).[4] The NCUA regulates federal credit unions in the United States. In addition to the name of each credit union, the list contained each institution's full mailing address, as well as information on its peer group.

3.2. Determining an Institution's Web Domain

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

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

3.3. Retrieving Standardized Notices

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

We retrieved the first 10 webpages returned as a result of that Google query for each company and selected the one with the largest number of hallmark elements of a standardized notice for further analysis, setting a minimum threshold of elements included to consider it valid. Appendix A details this process.

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

For additional insight into the practices of institutions consumers may be most familiar with, we manually collected notices from the 86 financial institutions on a Forbes list of the 100 largest banks [Badenhausen 2012] for which we could find these notices. Similarly, to understand consumers' privacy options for credit cards, we collected standardized notices from all 11 credit card companies included in a J.D. Power survey of credit card satisfaction [J.D. Power & Associates 2012].

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

3.4. Parsing Standardized Notices

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

During the development of our parsing program, we repeatedly tested our parser on small groups of standardized notices and manually checked for instances that were not matched. Based on these manual checks, we iteratively improved our parser to capture rewordings we commonly observed. For instance, we observed "use your credit or debit card" being replaced by the similar statements "use your credit/debit card," "use your credit card," "use your debit card," and "use your ATM card." We adjusted the parser to recognize all of these variants. Similarly, as we detail in Appendix B, we iteratively updated our parser to recognize many variants of revision dates.

We paid particular attention to parsing the *disclosure table* (Figure 1), which states an institution's data-sharing and opt-out practices across seven purposes. We initially searched for "Yes," "No," and "We don't share," the values permitted in the specification of the model privacy form [U.S. Federal Register 2009]. Based on our iterative verification process, we supported six additional case-insensitive variants: "we do not share"; "we don't collect"; "we do not collect"; "we have no affiliates"; "Y"; and "N."

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

3.5. Analysis

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

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

Finally, using the subset of institutions for which we had additional information regarding institutions' characteristics, we investigated which of those characteristics were correlated with their sharing practices. We joined the data we parsed automatically from standardized notices with each institution's characteristics, as reported in the FDIC Institution Directory [FDIC 2014] and list of institutions from the Federal Reserve. In the FDIC list, these characteristics included an institution's geographic region, assets, and type of institution. We used these characteristics as independent variables and the binary indicator "shares"/"does not share" as the dependent variable to build logistic regression models. We built a regression model for six of the seven sharing practices in the disclosure table. We excluded the "for our everyday business purposes" row because nearly all institutions had identical practices. We built our

models incrementally, aiming for the parsimonious model with the best fit, as indicated by having the lowest Bayesian information criterion (BIC) and Akaike information criterion (AIC), along with the highest adjusted R^2 value.

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

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

To encourage further analysis of our data, we have released a spreadsheet of our parsed data at the following location: https://cups.cs.cmu.edu/bankprivacy/data.htm.

4. RESULTS

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

4.1. Data Practices

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

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

Table I. The Data-Sharing Practices of the Institutions in Our Primary Dataset

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

Blank indicates that the institution defined the term, yet provided no information about its own practices. We did not observe this section for 53 of the 6,191 institutions.

4.1.1. With Whom Data Is Shared. Standardized notices present consumers with information about how a financial institution shares their data with other companies. These disclosures discuss *affiliates*, which are financial or nonfinancial companies that are "related by common ownership or control" to the institution making the disclosure. The disclosures also discuss *nonaffiliates*, which are third parties that are not affiliates, and *joint marketers*, which can be affiliates and nonaffiliates. In the "Definitions" section of the model privacy form (Figure 2), institutions must indicate whether or not they share customers' information with affiliates, nonaffiliates, and joint marketing partners. If they share with any of these entities, they must also list illustrative examples of such entities [U.S. Federal Register 2009].

Institutions varied starkly in their practices, as shown in Table I. On the question of sharing with affiliates, 28% of institutions said they have affiliates and share with them, 25% said that they do not share with their affiliates, and 43% said that they do not have any affiliates. The remaining 4% of institutions, labeled *blank* in Table I, did not provide any information about whether they have affiliates. In contrast, 12% of institutions said they share with nonaffiliates, 66% said they do not, and only 18% said they do not have nonaffiliates. Joint marketing practices also differed; 42% of institutions said they engage in joint marketing, whereas 55% said they do not. This section of the model privacy form was missing entirely for 0.9% of institutions, and the remaining institutions defined the terms without providing information about their own practices. The differences we noted suggest that financial institutions follow considerably different practices. Note, however, that an institution stating on its notice that it shares data is not an affirmation that it currently does share data. In some cases, an institution that does not currently share data might state in its standardized notice that it does share to ease a potential transition to sharing in the future.

4.1.2. Reasons Data Is Shared. The model privacy form's disclosure table lists seven reasons for which an institution might share data, along with the institution's own practices for each of these reasons. For each of these reasons, institutions can disclose that they do not share data at all, share data but offer an opt-out, or share data without offering an opt-out. Notably, as we discuss further in Section 4.4, some institutions'

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

The disclosure table comprises seven rows, each representing a reason an institution might share data, such as the institution's everyday business purposes or joint marketing purposes. One row, "for our affiliates to market to you," is optional for institutions that do not have affiliates, whose affiliates do not use personal information, or whose affiliates have a separate notice [U.S. Federal Register 2009]. Of the 6,191 institutions in our dataset, 3,754 institutions (61%) omitted this row. Note that we did not check for consistency between the disclosure table and the definitions section of the model privacy form.

We grouped institutions' practices into three primary categories based on their responses to the questions "Does [institution name] share?" and "Can you limit this sharing?" We labeled institutions that answered "no" to the first question as *does not share*. Institutions that responded "yes" to the first question and "yes" to the second question provide an opt-out for this sharing, so we labeled those institutions *share, opt-out*. We assigned the label *share, no opt-out* to institutions that answered "yes" and "no," respectively. When a particular row of the table was not parsed, we labeled that value *missing*. As we discuss further in Section 4.5.1, a handful of institutions provided contradictory answers to these two questions. For example, some institutions said in the first column that they share data for the purpose represented by that row, yet said in the second column that they do not share data for that reason. Between 13 and 42 institutions (0.2%–0.7%) per row make contradictory disclosures.

Companies are required to provide opt-outs for some types of data sharing but are not required to do so in other cases. As we discussed in Section 2.2, institutions that share information about creditworthiness with affiliates, or that share with either affiliates or nonaffiliates for marketing purposes, must provide an opt-out. Institutions that share for "our marketing purposes," that share "for joint marketing," or that share information about transactions and experiences with affiliates "may choose to provide an opt-out" but are not required to do so [U.S. Federal Register 2009].

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

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

4.1.3. Opt-Out Mechanisms. The mechanism for opting out of data sharing could impact consumers' likelihood to opt out. We parsed the contents of the "to limit our sharing" section of the model privacy form, searching for instructions on opting out via mail, email, web, and telephone. Table III shows the opt-outs offered. Overall, 20.5% of institutions offer at least one opt-out mechanism. We observed 627 institutions that provided exactly one mechanism, 491 institutions that provided two different mechanisms, and 152 institutions that provided at least three different mechanisms.

Non-computer-based opt-out mechanisms were more prevalent than computer-based methods. Of the institutions offering an opt-out, 28.2% let consumers opt out via email or a website. In contrast, 59.9% of institutions allowed consumers to opt out over the

Table II. A Summary of 6,191 Financial Institutions' Practices for Sharing Consumers' Personal Information

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

Institutions self-reported these practices in the model privacy form's disclosure table. Values that are missing could be caused by an institution omitting that row of the table, or by an error in our parser. An additional 0.2%–0.7% of institutions in each row made disclosures that were contradictory; these are excluded from the table.

Table III. Institutions' Opt-Out Mechanisms

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

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

phone, via postal mail, or using either mechanism. We counted institutions as providing a postal mail opt-out if they either instructed consumers to send mail to a particular address or, more popularly, provided a detachable, mail-in form to fill out. For 48.1% of institutions, we automatically observed such a detachable mail-in form.

4.1.4. What Information Is Collected. The first section of the model privacy form discloses "the types of personal information that the institution collects and shares" based on a predefined list of 24 types of information financial institutions commonly collect. The model privacy form specifies that the term "Social Security number" must be the first bullet, followed by exactly five of the following 23 terms: "income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions" [U.S. Federal Register 2009]. In total, exactly six terms should be arranged in three bullet points, as shown in Figure 1 in the background section of the article.

The main design objective of this section of the model privacy form was to familiarize customers with the concept of personal information, but not necessarily to provide a comprehensive list of the types of personal information that institutions collect [Kleimann Communication Group Inc. 2006]. Unfortunately for consumer understanding of privacy practices, given that institutions are told to include exactly six out of 24 data types, the omission of a data type does not provide any meaningful information about whether or not the institution collects that type of data.

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

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

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

4.1.5. How Information Is Collected. On the second page of the model privacy form, financial institutions are required to say how they collect consumers' information, again using phrases from a predefined list. The specification of the model privacy notice states that "institutions must use five (5) of the following terms to complete the bulleted list for this question," followed by a list of 34 occasions [U.S. Federal Register 2009]. We present a detailed count of these disclosures in Appendix G.

As with the types of information collected, the five most frequent terms for how information is collected were simply the five listed in pink as examples in the model privacy form [U.S. Federal Register 2009]: "open an account," "apply for a loan," "use your credit or debit card," "deposit money," and "pay your bills." On the opposite end of the spectrum, only one institution noted collecting information when consumers tell them about investment or retirement earnings, while no institutions specified collecting information when consumers sell securities to them.

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

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

The model privacy form also contains disclosures about other sources that provide data to an institution. Under the section titled, "How does *name* collect my personal information?" institutions must include either of the following statements if they apply to their practices: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies," or "We also collect your personal information from other companies" [U.S. Federal Register 2009]. We observed that 82.9% of institutions collect additional information from credit bureaus, 83.4% do so from "other companies," and 73.2% collect data from affiliates.

4.2. Comparing Similar Institutions

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

4.2.1. Practices Within a Specialization. We first compare the practices of similar institutions based on their specialization. First, we split the institutions using categories provided by the Federal Reserve. We also added all federal credit unions from the NCUA list as an additional type of financial institution. We eliminated categories for which we obtained fewer than 10 institutions' standardized notices, and the nine categories of institutions we compared are shown in Table IV.

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

In addition to widespread data sharing for "everyday business purposes" by all types of institutions, between 53.4% and 79.2% of institutions of each type shared data for their own marketing purposes without offering an opt-out. On the other end of the spectrum, whereas only 9.4% of credit unions chose not to share data for their own marketing purposes, 44.0% of state commercial banks supervised by the FDIC did not share data for this purpose. Between 1.2% and 16.3% of institutions in each specialization shared data for their own marketing purposes, yet offered an opt-out.

Table IV. The Nine Institution Types That We Analyzed and Compared

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

With the exception of credit unions, this classification is provided by the Federal Reserve [Federal Reserve 2014].

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

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

4.2.2. Practices Among the Largest Banks and Credit Card Companies. We also examined even more directly whether consumers might be able to exercise privacy choice among some of the most well-known competitors. To this end, we compared the institutions on a list compiled by Forbes [Badenhausen 2012] of the 100 largest banks, as well as the institutions on a list compiled by J.D. Power & Associates of consumer satisfaction with credit card companies [J.D. Power & Associates 2012]. Even among companies in these lists, we found differences in privacy practices, suggesting that making privacy practices more salient could empower consumers to choose more privacy-protective

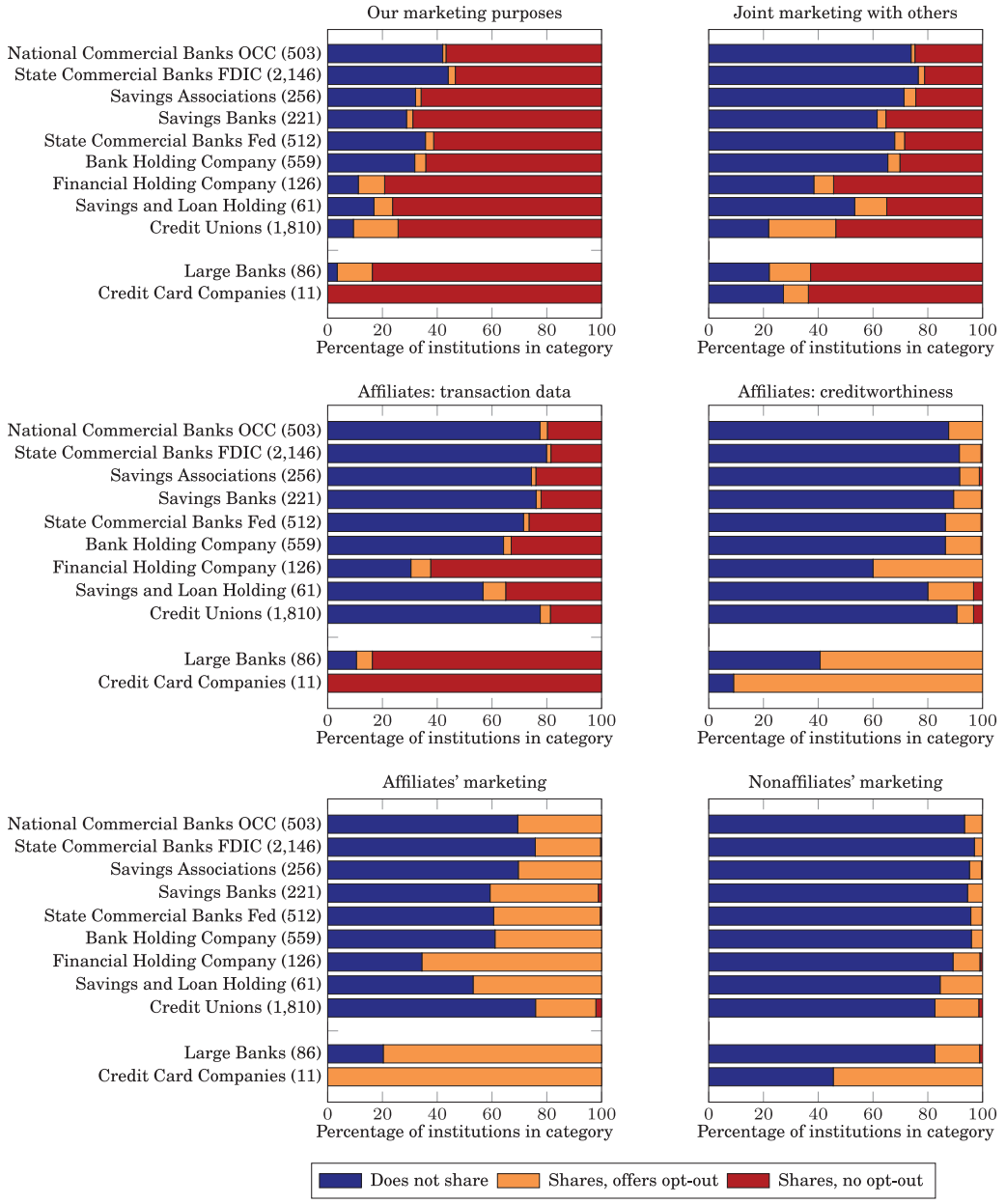


Fig. 3. The prevalence of sharing practices from the disclosure table. We exclude missing data. In particular, only 2,418 institutions disclosed their practices for the optional "for our affiliates to market to you" category.

institutions. In addition to the aforementioned categories of primary specialization, Figure 3 includes bars visualizing the practices of the *large banks* and *credit card companies* we discuss in this section.

In November 2014, we manually searched the websites of all banks in a Forbes list of the 100 largest banks in the United States [Badenhausen 2012] for standardized notices. We found standardized notices for 86 of these banks. Since a consumer might

choose from among these large banks, we investigated how their privacy practices compare. Table VIII in the appendix summarizes large banks' practices in aggregate.

Relative to financial institutions overall, the large banks tended to be less privacy protective. The proportion of large banks that shared data was larger than the proportion of institutions in each of the nine primary specializations that did the same for five of the six types of sharing shown in Figure 3. For example, 79.7% of large banks shared data for affiliates' marketing purposes (with or without offering an opt-out), whereas only between 24.1% (credit unions) and 65.6% (financial holding companies) of institutions in each of the nine specializations did the same.

We also analyzed the sharing practices of the 11 credit card companies listed in a consumer satisfaction survey conducted by J.D. Power and Associates [J.D. Power & Associates 2012]. Most of these companies shared data for many reasons, yet a few had more privacy-protective practices for certain types of sharing. However, for the company's own marketing and for providing affiliates information about transactions and experiences, all 11 credit card companies shared data without offering an opt-out. Similarly, for affiliates' marketing purposes, all 11 credit card companies shared data, though all did offer the required opt-out.

Eight of the 11 credit card companies said they share consumers' personal information without offering an opt-out for "our marketing purposes," "joint marketing," and "affiliates' everyday business purposes - transactions and experiences." Only GE Capital, U.S. Bank, and Wells Fargo said they do not share for joint marketing. Similarly, more than half of the companies said they share for "nonaffiliates to market to you." Table IX in the appendix lists the practices of each credit card company.

4.3. Factors Correlated with Privacy Practices

Using metadata provided as part of the FDIC directory [FDIC 2014], we investigated how different institutional characteristics correlated with those institutions' privacy practices. Because the other lists of institutions did not include such rich metadata, we limited this analysis to institutions on the FDIC list. The factors we investigated included the institution's size in terms of assets, the type of institution according to the Fed classification, the geographic region where the institutions' headquarters were located, whether the institution had been granted any trust powers to conduct fiduciary activities [FDIC 2013], and whether the institution was owned by shareholders. We list these factors alongside additional details in Table V. We selected this subset of characteristics from a larger set in the FDIC directory to account for what we found in pilot studies [Cranor et al. 2013] to be the most relevant characteristics.

A number of variables in the FDIC directory all could serve as proxies for the size of an institution, including equity, income, number of offices, and whether the company is a bank holding company. While we had used an institution's number of offices and interstate branches as the proxy for size in our prior work [Cranor et al. 2013], in this article we instead use the institution's total assets because we subsequently learned that researchers at the CFPB use that metric as a proxy for size. In any case, we found both measures to be highly correlated. Similarly, various variables potentially indicate an institution's location. We decided to use the four geographic districts defined by the OCC to categorize institutions into four general regions. Using only four OCC districts, as opposed to individual states, allowed us to make more meaningful statistical comparisons across regions. Statistical analysis across states would be problematic because only a handful of institutions are headquartered in certain states.

To evaluate the impact of these factors on institutions' sharing practices, we built logistic regression models. While we chose not to build a model for sharing related to an institution's everyday business purposes because that practice varied minimally, we built six regression models corresponding to the other six practices listed in the

Table V. Independent Variables Considered in Our Logistic Regression Models

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

disclosure table. We gradually increased the number of variables in our models, always starting with assets, which was a strong predictor in our proportionality χ^2 tests. Next, we added location, institution type, and additional indicator variables. We also switched the order in which variables were added and looked at the residual errors of each model. In the end, we selected the parsimonious model with the best fit, as indicated by having the lowest Bayesian information criterion (BIC) and Akaike information criterion (AIC), along with the highest adjusted R^2 value.

When an institution did not share consumers' personal information for a particular purpose, we assigned the binary outcome variable the value 0. When an institution shared information, regardless of whether it offered an opt-out, we assigned the outcome variable the value 1. We also tested ordinal models where the outcome variable had three levels: not sharing, sharing with an opt-out, and sharing without an opt-out. The results of these models were similar to the binary models. We report results from the binary model in this article as they are easier to interpret.

As shown in Table VI, our logistic regression models revealed a number of factors to be significantly correlated with institutions' privacy practices. Chief among these factors were the institution size (measured in terms of assets) and the OCC district where the institution was geographically headquartered. The type of institution was a significant factor for the marketing purposes of the institution itself and its nonaffiliates. We discuss the impact of each of these characteristics in the following section and present detailed results for each regression model in Section XIII of the appendix.

4.3.1. Institution Size. We found that the larger the institution, the more likely it was to share consumers' data across all six sharing purposes we investigated. Table XII in the appendix shows the fraction of institutions in each asset bracket that do not share, share yet offer an opt-out, and share without offering an opt-out. For example, only 10.5% of institutions below the 25th percentile of assets shared for joint marketing purposes without offering an opt-out, whereas 54.4% of institutions above the 90th percentile did so. Similarly, only 1.4% of institutions below the 25th percentile in

Table VI. Summary of Characteristics That Significantly Correlate with Sharing Practices

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

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

terms of assets shared with nonaffiliates to market to consumers, whereas 9.1% of institutions above the 90th percentile did so. Our regression models shown in Table XIII in the appendix detail the sharing behaviors of institutions in each asset bracket. For example, when compared with a small institution, the odds that a very large institution would share for joint marketing purposes are over 10 times higher, and the odds that a very large institution would share with nonaffiliates to market to consumers are over 6 times higher. Note that the principal reason GLBA included an exception to permit joint marketing with nonaffiliates without requiring an opt-out was to allow small institutions to compete with large ones [Swire 2001]. Instead, we found large companies were more likely than small companies to share for this purpose.

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

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

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

Table VII. Sharing Practices of the State in Each Region with the Most Institutions

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

Institutions in California shared less than institutions from the other three states, and institutions in New York shared more than institutions from the other three states. Differences were statistically significant at $\alpha = 0.05$ using a χ^2 proportionality test.

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

We looked closer at differences across states in each of the four OCC regions. In each region, we selected the state with the largest number of institutions. Table VII shows the practices of institutions in these states regarding sharing for joint marketing and for affiliates to market to consumers. The per-state results were consistent with the OCC-region results. In particular, institutions in New York (northeastern region) shared more than institutions in the other three states for both joint marketing without offering opt-out choices (30.9%) and affiliate marketing (47.6%). Institutions in California (western region) shared less than institutions in the other three states for both joint marketing and affiliate marketing. It is also important to note, as discussed in Section 2, that California's Financial Information Privacy Act (CalFIPA) mandates that consumers opt in before a financial institution may share "nonpublic personal information" with a nonaffiliated third party.

4.3.3. Institution Type. The type of institution was significantly correlated with two of the six sharing practices we studied. Table XV in the appendix shows that, in comparison to other types of institutions, commercial banks supervised by the FDIC most frequently did not share data for their own marketing purposes, or for affiliates and nonaffiliates to market to consumers. Our models also show that savings associations are significantly more likely to share than commercial banks supervised by the FDIC ($p = 0.03$). Other commercial banks also share at a higher rate than FDIC commercial banks for both affiliates and nonaffiliates to market to consumers ($p < 0.05$).

4.3.4. Other Factors. Banks with granted trust powers shared at a significantly higher rate for joint marketing, affiliates' marketing, and affiliates' everyday business purposes (transactions and experiences). Trust powers are granted at the state level under criteria that vary by state [FDIC 2013] and are correlated with the institution's size. The larger the institution, the more likely it will have trust powers. Nevertheless, even when controlling for an institution's assets, institutions with trust powers were more likely to share data.

We found that institutions located in a Metro Statistical Area were more likely to share data for their own marketing purposes than those not located in such an area. We also found that companies owned by shareholders were more likely to share

creditworthiness information for their affiliates' everyday business practices than institutions not owned by shareholders.

4.4. Compliance with the FCRA and GLBA

As discussed in Section 2.2, GLBA prohibits financial institutions from sharing nonpublic personal information with nonaffiliated third parties unless the institution offers consumers the opportunity to opt out. Similarly, the FCRA mandates the provision of an opt-out before information about consumers' creditworthiness may be shared with affiliates and, as amended by FACTA, mandates the provision of an opt-out before consumer report information may be shared with affiliates for marketing purposes.

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

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

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

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

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

4.5. Misuse of the Model Privacy Form

During our manual analyses of standardized notices during the development and verification of our parser (described in Appendix B), we noticed deviations from both the letter and the goal of the model privacy form. In this section, we discuss ways in which financial institutions deviated from the specification of the model privacy form [U.S. Federal Register 2009].

Reasons we can share your personal information	Does Bendena State Bank/Bank of Highland share?	Can you limit this sharing?
For our everyday business purposes- such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes- to offer our products and services to you	Yes	We don't share

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

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

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

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

Many institutions invented their own wording. For instance, Fisco (fisco.com) said that they collect information when customers "complete subscription documents" and "submit contributions or redemption requests," neither of which was among the 34 standardized terms. Similarly, Monitor Bank (monitorbank.com) said it collects "deposit account number(s)," "phone number," "address," "date of birth," and "loan number(s)." While it was not surprising that a financial institution might collect these data, none was listed in the specification [U.S. Federal Register 2009]. Arguably, these institutions' more detailed disclosures might actually be more useful to consumers.

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

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

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

5. DISCUSSION

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

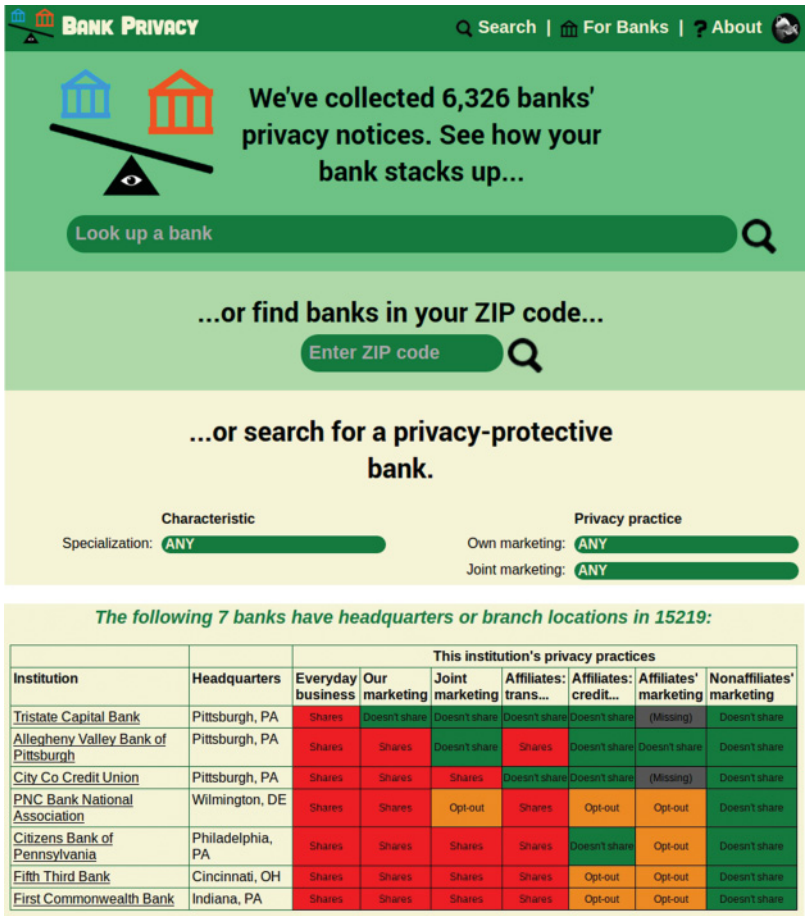
5.1. Users' Choices

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

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

While the possibility of consumers choosing financial institutions based in part on privacy practices seems promising, the lack of a simple mechanism for a consumer to make large-scale privacy comparisons or perform open-ended searches has been a major barrier. During the course of this project, we felt it would be helpful if a consumer could go to a website and have the ability to say, "I currently bank at Company X. Please tell me about competing banks in the same geographic area that are more privacy protective." To this end, we built such an interactive website (https://cups.cs.cmu.edu/bankprivacy) to help consumers search for or compare financial institutions. Figure 5 shows the front page of the website.

In addition to helping consumers, our Bank Privacy website can assist regulators in taking stock of the prevalence of different practices across the financial industry. Similarly, regulators can use our online database to uncover idiosyncratic behaviors



		This institution's privacy practices						
Institution	Headquarters	Everyday business	Our marketing	Joint marketing	Affiliates: trans...	Affiliates: credit...	Affiliates' marketing	Nonaffiliates' marketing
Tristate Capital Bank	Pittsburgh, PA	Shares	Doesn't share	Doesn't share	Doesn't share	Doesn't share	(Missing)	Doesn't share
Allegheny Valley Bank of Pittsburgh	Pittsburgh, PA	Shares	Shares	Doesn't share	Shares	Doesn't share	Doesn't share	Doesn't share
City Co Credit Union	Pittsburgh, PA	Shares	Shares	Shares	Doesn't share	Doesn't share	(Missing)	Doesn't share
PNC Bank National Association	Wilmington, DE	Shares	Shares	Opt-out	Shares	Opt-out	Opt-out	Doesn't share
Citizens Bank of Pennsylvania	Philadelphia, PA	Shares	Shares	Shares	Shares	Doesn't share	Opt-out	Doesn't share
Fifth Third Bank	Cincinnati, OH	Shares	Shares	Shares	Shares	Opt-out	Opt-out	Doesn't share
First Commonwealth Bank	Indiana, PA	Shares	Shares	Shares	Shares	Opt-out	Opt-out	Doesn't share

Fig. 5. The Bank Privacy website: https://cups.cs.cmu.edu/bankprivacy/.

by particular institutions, as well as to examine practices by institutions in different regions of the country or institutions that meet particular criteria. Over the course of this project, we were surprised to learn that regulators do not appear to have previously examined the privacy practices stated in institutions' standardized notices on any sort of large scale, in part due to lacking an easy mechanism to make such comparisons.

With information about institutions' privacy practices in a more accessible, standardized format, one can imagine financial institutions with consumer-friendly privacy practices using these practices as a competitive advantage. In past studies, consumers have even paid a premium price to purchase items from companies with more consumer-friendly privacy practices [Tsai et al. 2011], and it stands to reason that they might similarly favor financial institutions with exemplary privacy practices. Both industry and policymakers could benefit from future research investigating consumers' privacy preferences in the financial domain. Results from such research can assist the shaping of companies' practices and mandated requirements.

While consumers armed with sufficient information do appear to have privacy choices for many types of financial institutions, there are some types of institutions for which institutions consistently share data without offering an opt-out. For example, consumers looking for a credit card company would have very limited options since all credit card

companies in our study share data for their own marketing purposes and share data on transactions and experiences with affiliates without offering opt-out choices. Most of these companies also share data for joint marketing without opt-outs.

5.2. The Role of Regulators

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

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

Short, standardized notices have been suggested as the top layer in a "layered" privacy notice, which has been championed by both industry groups and regulators [Center for Information Policy Leadership 2007]. 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.

This issue is compounded by the manner in which institutions use the model privacy form. Rather than using the model privacy form as a supplement highlighting important points of a full-length privacy policy, the model privacy form replaced the full-length policies on the websites of many institutions we examined. Even though full-length privacy policies are too long for average consumers to read [McDonald and Cranor 2008], the 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 [U.S. Federal Register 2009] notes that "financial institutions may rely on [the model privacy form] as a safe harbor to provide disclosures." It is possible that this safe-harbor provision substantially reduces consumer awareness of privacy practices since institutions are required only to disclose some, rather than all, of their privacy practices on this short-form notice. While we believe the availability of short-form notices to be a good thing for consumers, we also believe that traditional privacy policies should still be made available.

Compliance and Oversight. Standardized notices can also make oversight of privacy disclosures more efficient. Because the standardized notices provided under the Gramm-Leach-Bliley Act are now posted online by many financial institutions, we were able to automate the process of collecting and evaluating them. We detected

notices with stated sharing practices in apparent violation of U.S. law. For three of these data-sharing purposes listed in the disclosure table, institutions were required to provide consumers a way to limit sharing [U.S. Federal Register 2009]. In violation of the law, more than 100 institutions said they shared data for these purposes, yet reported that consumers could not limit sharing. When we contacted institutions for which this was the case, some of them explained that the sharing practices they were disclosing annually to their customers were not their actual practices. Although they amended their standardized notices accordingly, these cases make us question to what extent consumers could rely on privacy notices to evaluate companies' actual practices, and to what extent stricter regulations and enforcement are necessary. These results also call into question current oversight mechanisms for financial institutions' privacy practices. We suggest that oversight institutions like the Consumer Financial Protection Bureau (CFPB) use tools similar to those we developed.

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

5.3. Online Notices and Implementation Issues

Currently, the standardized notice tends to be delivered as a static PDF, static HTML page, or static printout mailed to consumers. We believe there are a number of opportunities being missed for making online standardized notices interactive. In addition to the benefits mentioned earlier, online notices can be personalized, enable online opt-out methods, and provide links to additional information. For example, users may be able to see a notice that applies to their particular state of residence. We have found that institutions often use the "Other Important Information" section in the model privacy form to specify exceptions to sharing practices for residents of different states. An online notice can easily provide a drop-down menu allowing customers to select their state of residence to view the applicable privacy notice. Furthermore, an online privacy notice can show whether the consumer's opt-out right is currently being exercised.

We believe that customers' privacy can further be improved if, in addition to traditional offline methods such as mail and phone, online opt-out methods were offered widely. Companies may be incentivized, however, to make opting out difficult for consumers to avoid any overhead and costs associated with processing the opt-out request. Furthermore, due to space limitations, the paper-based standardized format does not allow companies to list all the data types that they collect, all the methods that they use to collect information, and the names of the entities with whom they share customers' personal information. In an online notice, this additional and relevant information can be available just one click away from the baseline notice.

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

We believe that many of these problems and inconsistencies related to institutions generating their standardized notice could be mitigated if a government agency provided an interactive tool that companies could use to generate standardized notices for online posting. The PDF form builder currently available does not prevent these problems. We hypothesize that the small and often understaffed structure of credit unions may have contributed to their high rate, relative to larger institutions, of posting standardized notices that violate the FCRA or GLBA opt-out requirements. A more guided process for building a standardized notice could help to mitigate these problems. Therefore, we developed a tool to help banks build their privacy notices. This tool is accessible at https://cups.cs.cmu.edu/bankprivacy/forbanks.htm.

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

5.4. Study Limitations

The automatic retrieval and parsing of standardized notices allowed us to perform a large-scale analysis of financial institutions' privacy notices, yet introduced some limitations. As we did not have access to the domain names of most of the financial institutions in our original list, we used the conservative heuristics described in Section A.1 to first find institutions' domain names and then retrieve their corresponding notices if they had one. We were able to retrieve notices from about one-third of companies in the original set. We randomly selected 100 companies from the set of those from which we could not automatically retrieve a standardized notice and manually attempted to retrieve domain names and notices from them. We manually found notices from 40 of those 100 companies, suggesting that our heuristics could be improved. However, finding those notices was a time-consuming task and required several steps that may not be possible to fully automate. Crowdsourcing could be an alternative, but likely an expensive one as it is time consuming to find notices. We also found that small companies (e.g., credit unions) were less likely to have an Internet presence and use standardized notices and that large companies (e.g., BHC) often have multiple subsidiaries with different domains that we were unable to find automatically. However, most of these subsidiaries are not consumer facing and tend to have the same privacy policy as the parent company. We also may have missed very large companies that

use different domain names for subsidiaries. Nevertheless, our sample of notices was heterogeneous enough to allow us to compare institutions of different types.

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

ACKNOWLEDGMENTS

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

REFERENCES

Annie I. Antón, Julia B. Earp, Qingfeng He, William Stufflebeam, Davide Bolchini, and Carlos Jensen. 2004. Financial privacy policies and the need for standardization. *IEEE Security & Privacy* 2, 2 (2004), 36–45.

Kurt Badenhausen. 2012. America's Best and Worst Banks 2012. Forbes. http://www.forbes.com/sites/kurtbadenhausen/2012/12/18/full-list-americ as-best-and-worst-banks-2012/. (December 2012).

Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira. 2013. Your browsing behavior for a big M: Economics of personal information online. In *Proceedings of the 22nd International Conference on World Wide Web (WWW'13)*. 189–200.

Center for Information Policy Leadership. 2007. Ten steps to develop a multilayered privacy notice. (2007).

Lorrie Faith Cranor. 2002. *Web Privacy with P3P*. O'Reilly.

Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law* 10 (2012), 273–307.

Lorrie Faith Cranor, Serge Egelman, Steve Sheng, Aleecia M. McDonald, and Abdur Chowdhury. 2008. P3P deployment on websites. *Electronic Commerce Research and Applications* 7, 3 (2008), 274–293.

Lorrie Faith Cranor, Kelly Idouchi, Pedro Giovanni Leon, Manya Sleeper, and Blase Ur. 2013. Are they actually any different? Comparing thousands of financial institutions' privacy practices. In *Workshop on the Economics of Information Security (WEIS'13)*.

FACTA. 2003. Fair and Accurate Credit Transactions Act. Pub. L. No. 108-159, 117 Stat. 1952. (2003).

FDIC. 2013. Trust Examination Manual. http://www.fdic.gov/regulations/examinations/trustmanual/section_10/sec tion_x.html. (Accessed June 1, 2013).

FDIC. 2014. Institution Directory. http://www2.fdic.gov/IDASP/. (Accessed July 26, 2014).

Federal Reserve. 2014. Federal Reserve's Financial Institution Types. http://www.ffiec.gov/nicpubweb/content/help/LinkAdvancedSearchAllinstitutions.htm. (Accessed July 26, 2014).

Edward H. Freeman. 2003. Privacy notices under the Gramm-Leach-Bliley act. *Information Systems Security* 12, 2 (2003), 5–9.

FTC. 1998. Privacy online: A report to Congress. (June 1998).

FTC. 2000. Privacy of Consumer Financial Information; Final Rule. Federal Register. (May 2000).

Mark Furletti and Stephen Smith. 2003. Financial privacy: Perspectives from the payment cards industry. *Payment Cards Center Discussion Paper* (2003).

Loretta Garrison, Manoj Hastak, Jeanne M. Hogarth, Susan Kleimann, and Alan S. Levy. 2012. Designing evidence-based disclosures: A case study of financial privacy notices. *Journal of Consumer Affairs* 46, 2 (2012), 204–234.

Mark A. Graber, Donna M. D'Alessandro, and Jill Johnson-West. 2002. Reading level of privacy policies on internet health web sites. *Journal of Family Practice* 51, 7 (2002), 642–645.

Gramm-Leach-Bliley 1999. Gramm-Leach-Bliley Act. Pub. L. No. 106-102, 113 Stat. 1338. (1999).

Oliver Ireland and Rachel Howell. 2003. The fear factor: Privacy, fear, and the changing hegemony of the American people and the right to privacy. *North Carolina Journal of International Law and Commercial Regulation* 29 (2003), 671.

Edward J. Janger and Paul M. Schwartz. 2001. The Gramm-Leach-Bliley act, information privacy, and the limits of default rules. *Minnesota Law Review* 86 (2001), 1219–1262.

J. D. Power & Associates. 2012. 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).

Carlos Jensen and Colin Potts. 2004. 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'04)*. 471–478.

Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS'09)*.

Kleimann Communication Group Inc. 2006. Evolution of a Prototype Financial Privacy Notice. http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf. (February 2006).

Kleimann Communication Group Inc. 2009. A Report on Validation Testing Results. http://www.ftc.gov/reports/financial-privacy-notice-report-validation-t esting-results-kleimann-validation-report. (2009).

Balachander Krishnamurthy and Craig E. Wills. 2009. Privacy diffusion on the web: A longitudinal perspective. In *Proceedings of the 18th International Conference on World Wide Web (WWW'09)*. 541–550.

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

Pedro Giovanni Leon, Lorrie Faith Cranor, Aleecia M. McDonald, and Robert McGuire. 2010. 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'10)*. 93–104.

Alan Levy and Manoj Hastak. 2008. Consumer Comprehension of Financial Privacy Notices. Interagency Notice Project. http://ftc.gov/privacy/privacyinitiatives/Levy-Hastak-Report.pdf. (December 2008).

Jonathan R. Macey. 1999. The business of banking: Before and after Gramm-Leach-Bliley. *Journal of Corporation Law* 25 (1999), 691.

Macro International Inc. 2008. Mall Intercept Study of Consumer Understanding of Financial Privacy Notices: Methodological Report. http://www.ftc.gov/reports/quantitative-research-macro-international-report. (September 2008).

Kristen J. Mathews. 2013. *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*. Practicing Law Institute.

Peter L. McCorkell and Andrew M. Smith. 2009. Fair credit reporting act. Update—2008. *Business Lawyer* 64, 2 (2009), 579–591.

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

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

Ralph Nader and others. 2001. Joint Petition for Rulemaking on Privacy Notices. http://www.ftc.gov/bcp/workshops/glb/comments/. (July 2001).

Andrea Lee Negroni and John P. Kromer. 2001. Gramm-Leach-Bliley: Tip of the privacy iceberg. *Banking Law Journal* 118, 10 (2001), 958–969.

Gregory T. Nojeim. 2000. Financial privacy. *New York Law School Journal of Human Rights* 17 (2000), 81.

OECD. 1980. Guidelines on the protection of privacy and transborder flows of personal data. (1980).

Ian Reay, Scott Dick, and James Miller. 2009. A large-scale empirical study of P3P privacy policies: Stated actions vs. legal obligations. *ACM Transactions on the Web (TWEB)* 3, 2 (April 2009), 6:1–6:34.

Julia C. Schiller. 2003. Informational privacy v. the commercial speech doctrine: Can the Gramm-Leach-Bliley act provide adequate privacy protection. *Commlaw Conspectus* 11 (2003), 349.

Xinguang Sheng and Lorrie Faith Cranor. 2005. An evaluation of the effect of US financial privacy legislation through the analysis of privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 2 (2005), 943.

Bernard Shull. 2002. Banking, commerce and competition under the Gramm-Leach-Bliley act. *Antitrust Bulletin* 47 (2002), 25.

Peter P. Swire. 2001. The surprising virtues of the new financial privacy law. *Minnesota Law Review* 86 (2001), 1263.

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

Zhulei Tang, Yu (Jeffrey) Hu, and Michael D. Smith. 2008. Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems* 24, 4 (2008), 153–173.

Terms of Service; Didn't Read. 2015. http://tosdr.org/. (2015).

Janice Y. Tsai, Serge Egelman, Lorrie F. Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* 22, 2 (June 2011), 254–268.

Blase Ur, Manya Sleeper, and Lorrie Faith Cranor. 2013. {Privacy, Privacidad, Приватност} Policies in social media: Providing translated privacy notice. *I/S: A Journal of Law and Policy for the Information Society* 9, 2 (2013), 201–243.

U.S. Federal Register. 2009. Final model privacy form under the Gramm-Leach-Bliley act. *Federal Register* 74 (December 1, 2009), 62890–62994.

Lawrence J. White. 2009. The Gramm-Leach-Bliley act of 1999: A bridge too far—Or not far enough. *Suffolk University Law Review* 43 (2009), 937.

Received September 2015; accepted April 2016