Carnegie Mellon University
Research Showcase @ CMU

Institute for Software Research | School of Computer Science

2006

An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies

Steve Sheng
Carnegie Mellon University

Lorrie Faith Cranor
Carnegie Mellon University

Follow this and additional works at: http://repository.cmu.edu/isr

Recommended Citation
.

This Article is brought to you for free and open access by the School of Computer Science at Research Showcase @ CMU. It has been accepted for inclusion in Institute for Software Research by an authorized administrator of Research Showcase @ CMU. For more information, please contact research-showcase@andrew.cmu.edu.

An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies

Steve Sheng (shengx@cmu.edu) and Lorrie Faith Cranor (lorrie@cmu.edu)

Abstract

Little research exists measuring the effectiveness of privacy legislation as compared to self-regulation. As policy makers, advocates and industry groups debate new privacy legislation, empirical research on the effectiveness of existing privacy legislation is needed to help inform the debate.

We conducted a longitudinal study of the privacy policies posted online between 1999 and 2005 for 50 companies in the US financial industry. We analyzed these policies to determine how they changed over this time period and what changes were likely prompted by compliance requirements of the Gramm-Leach-Bliley Act (GLB) privacy rule. We also conducted a similar analysis of the privacy policies from 10 retailers over the same time period. The retailers were not subject to US privacy regulation and thus serve as a control group.

Our research shows that since the GLB Act has gone into effect, financial privacy notices are more complete, however we have not found a significant change in the privacy choices offered to consumers. We observed that large banks and credit card companies minimally comply with GLB. While complying with the regulation, they are still able to collect large amounts of information about customers and share the information extensively with affiliates. They also take advantage of the exceptions provided by the law to share with third parties without giving consumers choices. Finally, we observe that choices about third party sharing offered by financial institutions tend not be as good as those available from retailers.

1. Introduction

Privacy is a major concern for American Internet users, as indicated by numerous surveys over the past several years.[1] Over the past decade the US congress has enacted several privacy-related bills, including Health Insurance Portability and Accountability Act (HIPAA 1996), Children's Online Privacy Protection Act (COPPA 1998), and Title V of the Gramm-Leach-Bliley Act (GLB 1999). In addition, over thirty privacy-related bills have been proposed and debated by the 108th and 109th Congress.[2]

Some privacy activists argue for EU-style[3] privacy laws, while others push for more limited legislation supplemented by self-regulation. Industry groups oppose most privacy regulations, although recently some companies have started supporting privacy legislation.[4] Recent security breaches[5] at major financial institutions have left millions of customers susceptible to identity theft.[6] As a result both state and federal legislatures have proposed a host of new bills aimed at increasing the security and confidentiality of customer data.[7]

As debate continues on new privacy proposals, it is useful to have data about the effectiveness of existing privacy regulations and self-regulatory programs to help inform the debate. Often, the only data available comes in the form of anecdotes. However, as organizations and companies are increasingly publishing privacy policies, their data practices are becoming more transparent.

We conducted a longitudinal study of financial institutions privacy policies. By collecting these policies over a period of 6 years, beginning prior to the enactment of the GLB, we were able to study the impacts of GLB on privacy policies and corporate data practices. In this paper we present our findings, which indicate that GLB has had only a modest impact on the privacy policies and practices of financial institutions. We found that financial privacy notices are more complete since the enactment of the GLB; however we have not found a significant change in the privacy choices

---

[1] Lorrie Faith Cranor, Joseph Reagle and Mark S. Ackerman, Beyond Concern: Understanding Net Users' Attitudes About Online Privacy (AT&T Labs-Research, 1999); Privacy Leadership Initiative, Consumer Privacy Attitudes and Behaviors Survey (New York City: 2001); Privacy Leadership Initiative, A Survey of Consumer Privacy Attitudes and Behavior Conducted by Harris Interactive (2000); Inc Louis Harris and Associates and Alan F. Westin, E-Commerce Privacy Survey (Privacy & American Business and Price Waterhouse, Inc., 1998); Joseph Turow, Americans and Online Privacy: The System Is Broken (Philadelphia: Annenberg Public Policy Center, University of Pennsylvania, 2003).

[2] EPIC Bill Track, http://www.epic.org/privacy/bill_track.html, last visited March 10, 2006

[3] The European Union Directive on Data Protection provides a framework for privacy regulations in EU countries. These laws provide for consistent privacy rules across all industry sectors, requiring that data subjects be given notice about data practice and that consent be provided for secondary data uses. Data protection commissioners in each country play a role in enforcing these laws.

[4] For example, Microsoft recently began advocating comprehensive Federal Privacy Legislation. See http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx

[5] Some notable examples: CitiFinancial on June 6, 2005 announced that it has lost 3.9 million customer data records in transit; Choiepoint on February 15, 2005 announced that thieves posing as legitimate customers had downloaded 145,000 consumer data records and at least 750 fraud cases were known. DSW shoe Warehouse announced on March 8, 2005 that hackers stole 1.4 million credit card and drivers license numbers.

[6] WSJ Staff Writer, "Without a Trace," Wall Street Journal Online June 6, 2005.

[7] Tom Zeller Jr, "Data Security Laws Seem Likely, So Consumers and Businesses Vie to Shape Them," The New York Times November 1, 2005.

offered to consumers. We observed that large banks and credit card companies minimally comply with GLB: they collect considerable amounts of customer information and share the information extensively with affiliates, and they take advantage of the exceptions provided by the law to share with third parties without giving consumers choices. Finally, we observe that choices about third party sharing offered by financial institutions tend not be as good as those available from the unregulated retail industry.

2. Background and Related Work

We begin by introducing the relevant financial privacy legislation, discuss the role of privacy self regulation, and describe other studies that have conducted privacy policy surveys. At the end of this section we distinguish our study from the previous work and discuss the goals of our study.

2.1 Gramm-Leach-Bliley Act

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" (GLB Act) was signed into law on November 12, 1999 and became effective on July 1, 2001. The law modified previous federal laws[8] and "allows for the creation of a financial holding company. Such companies may include a commercial bank and subsidiaries that conduct financial activities or activities incidental to financial activities."[9] In other words, GLB enables banks to engage in a whole line of financial activities. Late in the legislative process, legislators were concerned at the prospect that the consolidation of the financial industry would lead to privacy invasions. As a result of this concern, Title V was added to the GLB Act.[10] Title V of the GLB Act requires financial institutions to provide an initial "clear and conspicuous" notice of privacy policies and practices to all customers, an annual notice of privacy policies, and an opportunity for consumers to opt out of disclosing protected financial information to nonaffiliated third parties.[11] The FTC's final rule[12] specifies what information should be minimally included in the privacy notices and provides examples of GLB-compliant privacy policies.

However, the GLB has two very important exceptions[13]: first it allows for disclosure to an "affiliate"[14] of the financial institutions without providing notice of the disclosure and opportunity to

---

[8] The Glass-Steagall Act constrained the ability of FDIC member banks to affiliate with insurance or securities companies; The Bank Holdings Company Act prohibited banks from controlling companies unless they performed banking related services.

[9] Richard C. Turkington and Anita L. Allen, Privacy Law: Cases and Materials, American Casebook Series, 2nd ed. (2002).

[10] For a more thorough treatment of the legislative process of the GLB, please refer to Peter Swire's article "The Surprising Virtues of the New Financial Privacy Law," Minnesota Law Review 86.

[11] Turkington and Allen, Privacy Law: Cases and Materials.

[12] The FTC and eight other federal agencies, charged to implement the GLB privacy rule, came up with a set of guidelines to implement the GLB (16 CFR Part 313).

[13] Other exceptions that allow for data disclosure without notice and choice include: (1) dislcores in response to consumer requests for specified financial services, (2) when necessary to protect the financial institution's records and to prevent actual or potential fraud, (3) disclosures to insurance rate advisory organizations, (4) disclosures to law enforcement agencies, (5) disclosures in connection with proposed sales or mergers, (6) disclosures to the financial institution's lawyers and accountants and (7) in compliance with Federal, State or local legal requirements. These

opt out. Thus personal information may flow freely between affiliated financial institutions; second, it permits disclosure of nonpublic personal financial information to nonaffiliated third parties that jointly offer marketing with the original institution.

GLB does not preempt other state laws that offer stronger privacy controls. As a result a number of states have taken advantage of this and have enacted their own privacy laws that are stronger than the GLB.[15] For example, the California legislature deemed the GLB protection insufficient and enacted a financial privacy law (California SB 1) that requires companies to give consumers an "opt in" choice before sharing with unaffiliated third parties, and an "opt out" choices before sharing with affiliates. Vermont's Department of Banking, Insurance, Securities, and Health Care Administration also adopted opt-in provisions for information sharing.

Responses to the GLB Act privacy rule have been mixed. Many privacy law scholars were critical of exceptions and the choices offered in the law. For example Pandozzi concluded that "Title V (GLB Privacy Section) is riddled with loopholes and exceptions that severely weaken, if not paralyze, the consumers' power to opt out of information sharing between financial institutions and nonaffiliated third parties."[16] Paul M. Schwartz argues that the GLB's promise falls short because the opt-out requirement burdens the consumer. He wrote, "The opt-out rule fails to impose any penalty on the party with superior knowledge — the financial entity — should negotiations over further use and transfer of data fail to occur. … the GLB Act places the burden of bargaining on the less-informed party, the individual consumer."[17]

Peter Swire has criticized some aspects of the GLB, but argued in an article titled "The Surprising Virtues of the New Financial Privacy Law," that the law has some "surprising merits." For example, the broad definition of "financial institutions" in the law makes it applicable to many institutions, and the level of detail required by the GLB notice requirement requires financial institutions to examine their data practices and creates more possibilities for accountability.[18]

2.2 Self Regulation

In the absence of legislation, industries or companies sometimes voluntarily adopt a set of principles or practices to protect consumer privacy, functioning as self-regulation. Generally speaking,

---

exceptions are arguably in alignment with customer expectations of privacy. Thus, in this paper, we will not address these exceptions.

[14] "Affiliate is defined as any company that controls, is controlled by or under the common control with another company." (16 CFR 313.3 a) As an illustration, Citigroup owns Citibank, Dinner Club Card, and Smith Barney Investment. These companies can be considered affiliates. (Source: http://www.citigroup.com/citigroup/business/brands.htm)

[15] Virginia Boyd, "Financial Privacy in the United States and the European Union:A Path to Trans-Atlantic Regulatory Harmonization," (Harvard Law School, 2005).

[16] Neal R. Pandozzi, "Be Ware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation," Miami Law Review 163 (2001).

[17] Paul M. Schwartz, "Property, Privacy, and Personal Data," Harvard Law Review 117 Harv. L. Rev. 2055 (2004).

[18] Peter P. Swire, "The Surprising Virtues of the New Financial Privacy Law," Minnesota Law Review 86.Minnesota Law Review.

industries seek to self regulate to avoid legislation, or to anticipate legislation, although self regulation can also be used to implement legislation, and to supplement legislation.[19]

The US Federal Trade Commission's online privacy activities in the mid 1990s led to several self-regulatory initiatives to improve data privacy practices, including the BBBOnLine and TRUSTe privacy seal programs. Each of these initiatives requires participating entities to post privacy notices that conform to guidelines based on the Fair Information Practice Principles. TRUSTe was founded in 1997 by the Electronic Frontier Foundation and the CommerceNet Consortium. The TRUSTe program evolved over time, going through a number of major revisions. TRUSTe awards a "trustmark" to web sites that agree to adhere to a set of privacy principles and agree to comply with ongoing TRUSTe oversight and consumer complaint resolution procedures. About 2000 web sites had TRUSTe seals in 2005. The BBBOnLine privacy program is operated by the Council of Better Business Bureaus and is similar to the TRUSTe program. As of January 2005, 630 web sites had BBBOnLine privacy seals.

Previous research on privacy seals has been limited. Moores and Dhillon surveyed the performance of Web seals and gave them a mixed review, citing mostly anecdotal evidence.[20] More recently, Moores surveyed 143 students about privacy seals and concluded that most did not understand their meaning and could not recognize them.[21] These studies suggest that privacy seals may not be succeeding as mechanisms for engendering consumer trust. However, questions remain about whether they are playing a role in improving privacy practices. There is some evidence that privacy policies on web sites with privacy seals are more readable than policies on sites without privacy seals,[22] but it is not clear what substantive differences there are between sites with privacy seals and those without privacy seals.

In *The Governance of Privacy*, Bennet and Raab describe four general ways companies self regulate: privacy commitments, privacy codes of practice, privacy standards, and privacy seals.[23] Privacy commitments are brief statements of commitment to the set of privacy principles that companies abide by. An example of privacy commitment is that private sector companies are encouraged to adopt the 1981 OECD Guidelines. Privacy codes of practice refers to a set of rules for employees, members or member organizations to follow. They provide more than a simple claim. Privacy standards harmonize the existing codes. One example is the Canadian Standards Association Model Code for the Protection of Personal Information. As already discussed, examples of privacy seals includes TRUSTe and BBBOnline.

---

[19] Peter Hustinx, "The Role of Self-Regulation in the Scheme of Data Protection," the 13th Conference of Data Protection Commissioners (Strasbourg: 1991).

[20] Moores, T. and Dhillon, G. (2003) "Do privacy seals in e-commerce really work?" Communications of the ACM. Vol 46, No. 12.

[21] Moores, T.T. (2005) "Do consumers understand the role of privacy seals in e-commerce?." *Communications of the ACM*, **48**(3), Mar., pp. 86-91.

[22] Milne, G.R., Culnan, M.J., and Greene, H. 2005. A Longitudinal Assessment of Online Privacy Notice Readability: Implications for Developing a Short Notice Format. *Journal of Public Policy and Marketing*.

[23] Colin J. Bennett and Charles D. Raab, "Self Regulatory Instruments," The Governance of Privacy: Policy Instruments in Global Perspective (Burlington: Ashgate Publishing Company, 2002).

The banking industry adopted privacy self-regulatory measures prior to the enactment of the GLB Act. In late 1997 several banking industry associations[24] agreed on a set of privacy principles to respond to rising privacy concerns (and perhaps to avoid legislation).[25] The privacy principles cover eight separate areas: recognition of a customer's expectation of privacy; use, collection and retention of customer information; maintenance of accurate information; limiting employee access to information; protection of information via established security procedures; restriction on the disclosure of account information; maintaining customer privacy in business relationships with third parties; and making an institution's privacy principles known to the customer.

2.3 Related Work

Economists, legal scholars and policy makers have researched and debated the best way to protect personal privacy. Varian and Acquisti studied economic aspects of privacy such as transaction costs and asymmetric information.[26] Tang et al treated the matter analytically using formal economic models. Their analysis suggests that "government regulation using multiple privacy protection regimes for different market types will generate more social surplus than overarching approaches based on mandatory standards, consumer awareness, or self-regulation."[27]

Surveys have been an important tool to inform public policy debates on protecting privacy. For example, the FTC surveyed privacy policies posted online in 1998 and 2000.[28] Based on these surveys, it recommended industry self-regulation in 1998, but later resolved to recommend legislation to complement industry self-regulatory programs in 2000. Besides the FTC's privacy policy surveys, Atkinson surveyed privacy policies online in 2002,[29] and Milne and Culnan compared the previous surveys.[30] These surveys did not look specifically at financial institutions' privacy policies, however. The FDIC surveyed privacy practices posted by financial institutions in 1999,[31]

---

[24] The American Bankers Association (ABA), The Bankers Roundtable (Roundtable),the Banking Industry Technology Secretariat (BITS), the Consumer Banks Association (CBA) and the Independent Bankers Association of America (IBAA) announced on September 18th, 1997 that they had endorsed a common set of privacy principles.

[25] See Press Release, "Banking Industry Unites On Customer Privacy," September 18, 1997, available at http://www.ftc.gov/reports/privacy3/comments/016.pdf, last accessed March 29, 2006

[26] Hal Varian, Economic Aspects of Personal Privacy (National Telecommunications and Information Administration, 1996); Alessandro Acquisti, "Privacy and Security of Personal Information: Economic Incentives and Technological Solutions," The Economics of Information Security, eds. Jean Camp and Stephen Lewis (2004); Alessandro Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification," ACM Electronic Commerce Conference (New York, NY: ACM Press, 2004); Alessandro Acquisti and J Grossklags, "Privacy and Rationality in Decision Making," IEEE Security & Privacy 2005.

[27] Zhulei Tang, Yu (Jeffrey) Hu and Michael D. Smith, "Protecting Online Privacy: Self-Regulation, Mandatory Standards, or Caveat Emptor," 2005 Workshop on the Economics of Information Security (Boston: 2005).

[28] Federal Trade Commission, Privacy Online: A Report to Congress (Federal Trade Commission, 1998); Federal Trade Commission, Privacy Online: Fair Information Practices in the Marketplace: A Report to Congress (Washington DC: Federal Trade Commission, 2000).

[29] Jr. William F. Adkinson, Jeffrey A. Eisenach and Thomas M. Lenard, Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites (The Progress and Freedom Foundation, 2002).

[30] George R. Milne and Mary J Culnan, "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S Web Surveys," The Information Society 18 (2002).

but there has not previously been a longitudinal study that tracks the changes in financial institution privacy policies before and after GLB went into effect.

One study analyzed the privacy policies of nine US healthcare web sites before and after HIPAA went into effect and concluded that federal health privacy regulations have not improved the level of privacy protections at these sites.[32]

Anton et. al analyzed financial privacy policies after the law was enacted and observed that "financial privacy statements lack clarity and are full of statements that regular consumer cannot understand."[33] The Center for Democracy and Technology studied the opt-out choices financial institutions offer to consumers and concluded that the GLB is off to "a slow, confusing start to giving customers control."[34]

Current literature on evaluating the effectiveness of the privacy law is based on cross sectional data in which the state of privacy is evaluated at a single point in time and is not compared over time. This literature sheds some light on the effectiveness of the GLB Act. However a few important questions have yet to be addressed.

What effect has the GLB Act had on financial institution privacy policies and practices? This is the overarching question that our research seeks to address. There is an implicit assumption that the GLB privacy rule required regulated institutions to change their policies and practices. However, there has been little empirical data collected on the types of changes that were made to comply with the law, the extent of these changes, and the number of institutions impacted.

Did the GLB Act have an impact on the readability of financial privacy notices? Some regulations may require disclosures that are so complicated that it is almost impossible to comply without producing notices that are difficult to read. Other regulations may be accompanied by guidance that results in more readable notices. A number of studies have demonstrated that financial privacy notices are difficult to read and understand. Are the current readability problems with GLB notices likely caused by the regulation, or have the notices actually improved (or remained unchanged) as a result of the regulation?

Have regulated companies adopted policies that minimally comply with the GLB Act, or have they adopt policies that exceed the mandated requirements? In the absence of regulation, companies respond to market incentives or other pressures to determine what level of privacy to offer in their policies. They may adopt

---

[31] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and Office of Thrift Supervision, Interagency Financial Institution Web Site Privacy Survey Report (Washington DC: 1999).

[32] Antón, A., Earp, Vail, M., Jain, N., Gheen, C., and Frink, J. 2004. *An Analysis of Web Site Privacy Policy Evolution in the Presence of HIPAA*. North Carolina State University Computer Science Technical Report # TR-2004-21. http://www.theprivacyplace.org/papers/hipaa_7_24_submit.pdf

[33] Annie I. Anton, Julia B. Earp, David Bolchini, Qingfeng He, Carlos Jensen and William Stufflebeam, "The Lack of Clarity in Financial Privacy Policies and the Need for Standardization," IEEE Security & Privacy 2004; Mark Hochhauser, Lost in the Fine Print: Readability of Financial Privacy Notices (Privacy Rights Clearinghouse, 2001).

[34] Center for Democracy and Technology, "Online Banking Privacy: A Slow, Confusing Start to Giving Customers Control over Their Information," (2001).

privacy-friendly policies in an attempt to prevent the enactment of new privacy regulation. As there is often some uncertainty as to what level of privacy will be sufficient to satisfy regulators or consumers, companies may make different decisions about the level of privacy to offer. Once privacy regulation has been adopted, there is no longer uncertainty about what is necessary to satisfy regulators, and companies that comply with the regulation are able to advertise that they offer the privacy protections required by law. Nonetheless, some companies may still have incentives to provide additional protections that exceed the mandated requirements. Empirical data is needed to determine the extent to which companies create policies that exceed the mandated requirements. This is especially important in the case of the GLB Act, as the mandated privacy requirements are often criticized as being fairly minimal. [35]

How does the level of privacy offered by companies regulated by the GLB Act compare with the level of privacy offered by companies in unregulated industries? If a privacy regulation raises the level of privacy offered by companies in an industry, we might expect to find lower levels of privacy offered by companies in similar, but unregulated, industries. If, on the other hand, the regulation reduces the incentives companies have to offer privacy levels above the mandated requirements, we may find higher levels of privacy offered by companies in unregulated industries.

Our research aims to shed light on these four questions through the collection and analysis of empirical data. Although more data would be needed to answer all of these questions conclusively, we believe the data we have collected provide important insights into the answers to these questions.

3. Data Collection and Analysis

If companies provided full disclosure of their privacy practices on a regular basis, the impact of privacy regulation could be measured through an analysis of these disclosures. However, unregulated companies are not obligated by law to offer any privacy disclosures, and regulated companies are required only to make certain types of privacy disclosures. In the US, there is no governmental entity responsible for collecting or maintaining an archive of these disclosures. Thus it has been difficult to track privacy practices over time.

The advent of web site privacy policies has made it much easier to conduct research on privacy policies. As discussed earlier, a number of surveys of web site privacy policies have been performed. Because web sites are frequently archived by Internet search engines and companies attempting to provide archives of the entire Web, it is now possible to retrieve not only a company's current online privacy policy, but also privacy policies previously posted on their web site. Thus a rich set of data on privacy practices is now available going back several years. Unfortunately, this data is not 100 percent complete, and the analysis of this data remains time consuming as it cannot be completely automated.

Not all companies have web sites, not all companies have privacy policies, and not all companies that have both web sites and privacy policies post their privacy policies on their web sites. One limitation of our approach is that we make the simplifying assumption that the privacy policies we collect online are somewhat representative of the privacy policies across an entire industry sector.

---

[35] For example, Anita Allen asserted that the GLB only provided a floor for privacy protection. Turkington and Allen, Privacy Law: Cases and Materials.

However, we have not collected privacy policies from companies that provide them only offline in order to verify that this assumption is reasonable. Collecting offline privacy policies requires contacting each company individually in person, by telephone, or by postal mail, and requesting their policies. In our experience, finding the correct point of contact within a financial institution to request a privacy policy is difficult, and some companies are reluctant to send policies to people who are not already their customers.[36]

3.1 Research Data

We collected privacy policies from 60 US companies with significant online presence — 50 financial institutions and a control group of 10 retailers — as shown in **Table** 1. By "significant online presence," we mean an institution posted privacy policies online before 2000, and the policies posted were substantial in content. A policy is "substantial in content" if it addresses aspects of the information practice regarding data collection and data sharing. Thus, an online policy that addresses only web cookie usage is not considered to be substantial in content. The 50 financial institutions whose policies we collected included the top 10 U.S. banks with significant online presence (**Table** 2), the top 10 credit card issuers (Table 3),[37] and 30 banks selected randomly from the top 500 banks by asset (**Table** 4).[38] We also collected the privacy policies of the top ten retailers with significant online presence (Table 5).[39] We sampled randomly from the top 500 list until we had collected 30 banks. We found that 25.9% of the institutions posted policies online before the GLB that are significant in content.

For each company, we collected their privacy policies once a year from 1999 to 2005. Current policies were collected from the companies' website directly. Policies from 1999 to 2004 were collected from the Internet Archive.[40]

Table 1: Research Data

Type	Number of Companies	Total Number of Policies Collected (1999-2005)
Banks	Top 10	45
	Random 30	168
Credit Card Issuers	Top 10	56
Retailers	Top 10	45

Table 2: Top 10 Banks with significant online presence

[36] Some of our undergraduate students visited several local bank branch offices to request privacy policies as part of a class project. At some of these banks the tellers refused to give them a copy of the privacy policy unless they opened an account.

[37] WSJ Staff Writer, "Largest Credit Card Issuers, 2004," Wall Street Journal April 8, 2005.

[38] The data is provided by KPMG.

[39] David P. Schulz, The Nation's Retail Power Players 2005 (2005).

[40] The Internet Archive is a service that allows people to visit archived versions of Websites from 1996 to the present time. See http://www.archive.org/ , last accessed March 12, 2006

RANK	BANKNAME
1	Citigroup Inc.
2	JPMorgan Chase & Co.
3	Bank of America Corporation
4	Wachovia Corporation
5	Wells Fargo & Company
6	U.S. Bancorp
9	BB&T Corporation
13	KeyCorp
14	Regions Financial Corp.
16	MBNA Corporation

Table 3: Largest 10 personal credit issuers with significant online presence

RANK	Institution Name
1	JPMorgan Chase & Co.
2	Citigroup, Inc.
3	MBNA Corporation
4	American Express Credit Corporation
5	Bank of America Corporation
6	Capital One Financial Corporation
7	Discover
8	HSBC USA
9	Providian Financial Corporation
10	Wells Fargo & Company

Table 4: the Random 30 Banks with significant online presence

RANK	BANKNAME
20	AmSouth Bancorporation
23	Marshall & Ilsley Corporation
24	Huntington Bancshares Incorporated
41	First Citizens BancShares, Inc.
54	Trustmark Corporation
55	UMB Financial Corporation
69	Pacific Capital Bancorp
70	Texas Regional Bancshares, Inc.
84	CVB Financial Corp.
134	Financial Institutions, Inc.
154	CoBiz Inc.
161	Seacoast Banking Corporation of Florida
178	Arrow Financial Corporation
179	Merchants and Manufacturers Bancorporation, Inc.
212	Bank of Granite Corporation
221	German American Bancorp
239	QCR Holdings, Inc.
246	Farmers National Banc Corporation

RANK	BANKNAME
282	Washington Banking Company
283	Princeton National Bancorp, Inc.
298	MidSouth Bancorp, Inc.
314	Penns Woods Bancorp, Inc.
315	Guaranty Bancshares, Inc.
322	LCNB Corporation
337	James Monroe Bancorp, Inc.
340	Bank of Commerce Holdings
354	Mid Penn Bancorp, Inc.
410	Northern Trust Corporation
472	Pulaski Bank
490	Jones National Bank & Trust

Table 5: Largest 10 retailers with significant online presence

RANK	Institution Name
3	Kroger
5	Target
7	Walgreen
8	Lowes
10	Safeway
11	CVS
13	Bestbuy
18	Gap
22	Staples
24	Office Depot

We collected both the top 10 and a random set of 30 banks because these groups have differing characteristics. Top 10 banks have a large customer base and thus have a larger impact on consumers than the average bank. In our study, we also wanted to compare the relative impact of the law on the largest institutions and average institutions. We selected the top five hundred banks as a sampling frame instead of all the FDIC insured banks because the top 500 banks accounts for most of the banking industry's total asset.[41]

We collected privacy policies from an unregulated industry for two reasons. First, it is difficult to determine whether observed privacy policy changes are caused by the GLB privacy rule or other factors that may also be in play during this time period, such as increasing use of the Internet and ecommerce, and a rising awareness of data privacy issues. By comparing financial privacy policies with policies from an unregulated industry we hope to gain a better understanding of which changes were caused by GLB. A second and perhaps more important reason is that a non-regulated industry has different incentives to protect privacy, comparing the privacy they offer with the regulated industry provides data on the effectiveness of the legislation. Of course, as no industry operates in a

[41] See National Commercial Banks, Encyclopedia of American Industries. Online Edition, 2006, Thomson Gale.

vacuum, regulation in one industry may also prompt changes in other industries, for example, adopting self-regulatory initiatives in an attempt to avoid similar regulation.

The ideal control group would be an industry sector similar to the structure of the US financial industry that does not have privacy regulation. We first considered Canadian banks, however we found they are subject to privacy regulation passed in 2000. We chose the US retail industry as a control group because retailers, like financial institutions, closely interact with consumers and they collect large amounts of data. However, we do acknowledge important differences between retailers and banks: retailers do not typically collect as much personal information as banks; second, they do not have the same type of affiliate structures as banks.

Finally, it is worth noting that due to technical limitations, such as robot exclusion,[42] the Internet Archive did not archive the policies of all of the institutions we studied every year. Thus, we were not able to collect all of the policies that companies posted. In total, we have collected 314 of the 360 privacy policies we attempted to collect.

3.2 Research Methods

We began by collecting 314 privacy policies, as described in the previous section. All policies were stored in our database. We then performed an automated analysis to gather basic statistics on each policy. Finally, one pre-GLB policy and one post-GLB policy for each company were reviewed by a privacy expert and coded into a format suitable for statistical analysis.

Our automated analysis captured textual statistics on each policy, including the number of words and sentences in each policy and readability scores.[43] Various readability measurements exist; many calculate a score that is equivalent to a grade level in U.S schools. We used the Flesh-Kincaid readability score, which is the most commonly used method for evaluating the readability of technical documents.[44]

Our coding process was facilitated by the use of software we developed that presents the coder with a privacy policy, a coding form, and a code book, side-by-side on a computer screen. The coding form asks the coder to identify the types of data collected, the uses of that data, the data retention policy, access policy, and other key points. When information was unclear or missing from a privacy policy, coders also spent some time reviewing the associated web site to see whether any of the missing information was provided elsewhere. Any remaining unclear or missing information was coded as "unknown." After a coder completed coding a privacy policy, the software saved the coded

---

[42] A site may post a file (robot.txt) on their web server, specifying the directories that are to be excluded from archiving by automated robots (computer programs).

[43] We automated this process by writing customized computer programs. The "style" command in Unix provided most of the textual statistics. We also used tools in Microsoft Word to gather some statistics.

[44] The Flesh-Kincaid readability score is calculated in the following way: FKL = 11.8*syllables/wds+0.39*wds/sentences-15.59. The result corresponds to an equivalent grade level in U.S schools. We used the "style" command in UNIX to gather this statistic. We also computed other readability statistics such as Automated Readability Index, Gunning-Fog indices, Coleman-Liau index. However, the choice of readability statistics did not significantly impact our results.

information in a computer-readable format for later statistical analysis.[45] To ensure that we did not suffer from coding bias, a second expert coded 15% of the policies on key variables. We found that the coders agreed 95% of the time.

4. Research Results

We analyzed the data we collected to answer our four research questions:

- What effect has the GLB Act had on financial institution privacy policies and practices?
- Did the GLB Act have an impact on the readability of financial privacy notices?
- Have regulated companies adopted policies that minimally comply with the GLB Act, or have they adopted policies that exceed the mandated requirements?
- How does the level of privacy offered by companies regulated by the GLB Act compare with the level of privacy offered by companies in unregulated industries?

In order to measure the effect of GLB on financial institution privacy policies we examined the quality of the privacy notices themselves as well as the level of privacy offered both before and after GLB went into effect. The quality of privacy notices is generally measured by their completeness and comprehensibility. The more complete and comprehensible a policy is, the better consumers will understand a company's practices. Completeness of privacy policies is often measured against the US FTC's fair information practices, which has five essential components: notice, choice/consent, access, security, enforcement and remedies.[46] We discuss our findings on completeness in Section 4.1. Measuring comprehensibility requires determining whether people understand what the policy says. Performing a readability analysis of the text is usually the first step in measuring comprehensibility. We discuss our findings on comprehensibility in Section 4.2. Many factors go into determining the level of privacy offered. In this study we focused on information sharing, as this is the focus of the GLB privacy rule. We discuss our findings on information sharing in Section 4.3. Finally we compare our data on financial institutions with our data on retailers in section 4.4.

Overall, we found only modest impacts of GLB on financial institution privacy policies. We found that post-GLB privacy policies are longer, more complete, and more standardized than pre-GLB policies. They are also slightly easier to read, but still require college-level reading skills to comprehend. Most companies we surveyed have adopted policies that do not exceed the mandated requirements and provide a level of privacy lower than that provided by the top retailers we surveyed.

[45] The coded information about each privacy policy was stored as a computer readable privacy policy using an extended version of the Platform for Privacy Preferences (P3P) we created that included the ability to mark data practices as "unknown." A second coder coded 15% of our policies. We found that the second coder agreed 95% of the time with the original coder.

[46] See http://www.ftc.gov/reports/privacy3/fairinfo.htm. It is worth noting that the FTC's version of fair information practices is a watered down version of the OECD Guidelines, which contains eight principles.

4.1 Post GLB privacy policies are more substantial in content, more complete and more standardized

The privacy policies we examined became longer, more complete, and more standardized after the GLB Act took effect.

We observe that the length of the policies among the random 30 banks increased rapidly from 1999 to 2002, and then leveled off. These changes started before the legislation went to effect (the GLB was passed in November 1999 but did not actually take effect until July 2001), probably due to companies revising their privacy policies so that they would be in compliance by the time the law took effect. It is also possible that due to the increasing attention that data privacy was receiving during that period, companies expanded their privacy policies to promote consumer confidence.

The top 10 banks' policies became more substantial over time, but do not exhibit the same pattern as the random banks' policies. The difference we observe between the two group is that pre-GLB, the top ten banks privacy policies were already more substantial than the random 30 banks (average of 1504 words as compared to 508 words). Thus, less change was necessary to comply with the law. Interestingly, some top banks with longer policies before GLB shortened their policies after the GLB was enacted. We observed a similar trend in the random group. We discuss this finding and its implications in more detail in Section 4.3.

Credit card companies' policies also shown improvement, post-GLB policy increased from 900 words to 1600 words.

Figure 1 shows the length of policies (measured by the number of words) for the top 10 and random 30 groups of banks from 1999 to 2005.

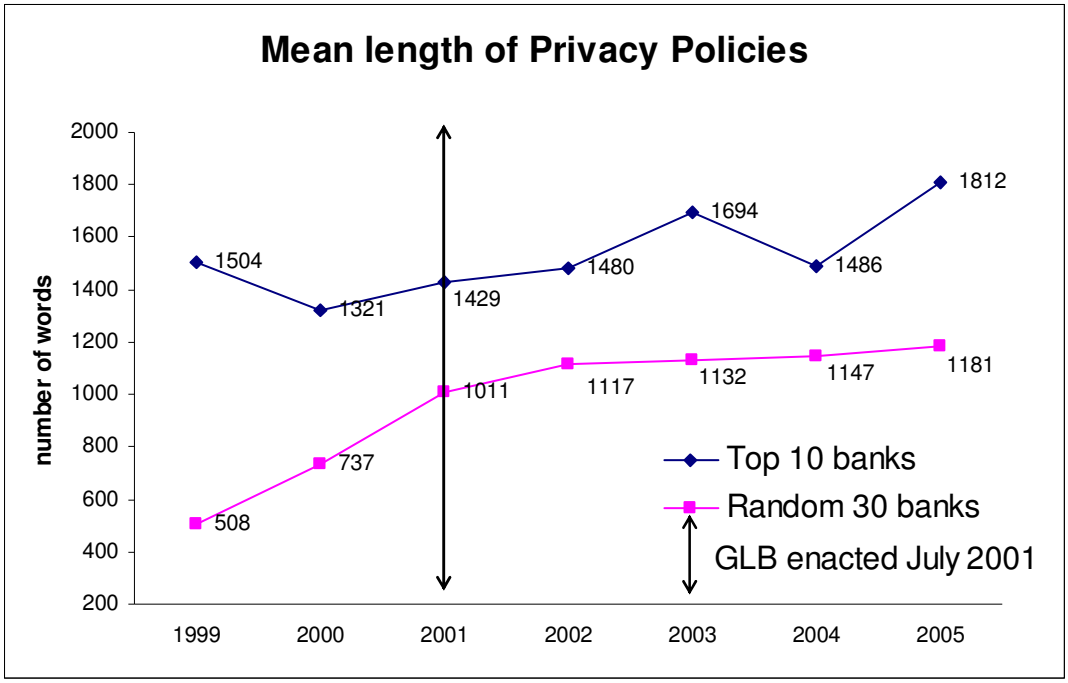

Figure 1: Mean length of privacy policies measured by the number of words for the top 10 and random 30 banks from 1999 to 2005. The number of data points from 1999 to 2005 for the random 30 banks are: 7, 29, 27, 26, 25, 24, and 30; for the top 10 banks are 5,8,8,5,6,5,10. the GLB privacy rule went into effect on July 1, 2001.

We observed that post-GLB policies are also more complete than pre-GLB policies. To measure completeness we looked at whether the coder was able to determine the following information for each privacy policy: what information the company collects, whether it shares with affiliates, what information it shares with affiliates, what choice it gives to consumers for affiliate sharing, and similar questions for sharing with non-affiliated third parties. We found that pre-GLB policies had a high percentage of unknowns[47], but post-GLB policies are more complete. The result for the random 30 group is presented in Figure 2. Data from the top 10 group exhibits a similar pattern; however, top-10 banks had fewer unknowns prior to GLB than the random 30 banks.[48]

[47] As part of the coding process, the coders read each privacy policy carefully to determine if the policy mentioned anything about whether the company shares information with affiliates or third parties, and if so what information is shared, and what choice is given to consumers. If after reading the privacy policy, the coders could not determine the answers to these questions, they coded it as "unknown."

[48] Data for the top 10 group: affiliate sharing unknown: pre-GLB, 20%, post-GLB 0%; affiliate disclosure: pre-GLB, 30%, post-GLB 0%; affiliate choice: pre-GLB, 30%, post-GLB 0%; Third party sharing unknown: pre-GLB, 10%, post-GLB 0%; third party choice unknown: pre-GLB, 40%, post GLB 0%.

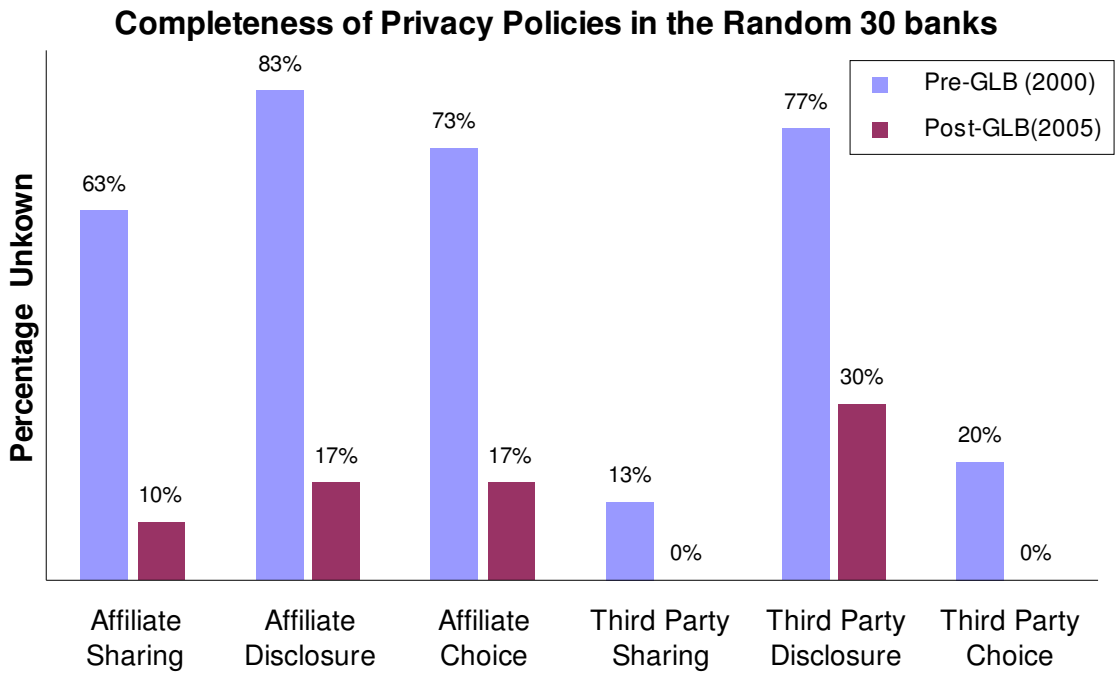

Figure 2: Percentage of privacy polices coded as "unknown" for the random 30 group. Unknown means that after reading the policy; we are unable to decide the company's practices regarding such sharing. Affiliate and Third party disclosure refers to the types of information to be disclosed to affiliates and third parties respectively.

From reading the privacy policies, we observed that before GLB, many financial institutions posted privacy policies that modeled the American Bankers Association's privacy principle.[49] The principle, announced in 1997, was an industry wide initiative to promote privacy protection.[50] Pre-GLB, many banks—especially those in the random 30 group—based their privacy policies closely on the principle, making few modifications. The FTC, in its final rule for GLB privacy in 2000, included GLB compliant privacy policy examples. Post-GLB, most banks use the FTC's template with little modification.

We verified our observation using a textual similarity measure.[51] Our measure gauges the similarity between the two policies by the number of overlapped words and the frequency of their usage. If two documents use the same set of vocabularies and the frequency of their usage is similar, then our measure would be close to 1.

---

[49] Available at http://www.aba.com/About+ABA/ABA_privprinpublic.htm.

[50] Boyd, "Financial Privacy in the United States and the European Union:A Path to Trans-Atlantic Regulatory Harmonization."

[51]

Our analysis of shows that there is a significant change in the content of the privacy policies from 2000 to 2001 as they use a different set of vocabularies. This is indicated by the fact that the similarity score for policies from 2000 to 2001 is much lower than in the other years we examined. The results are shown in Figure 3.

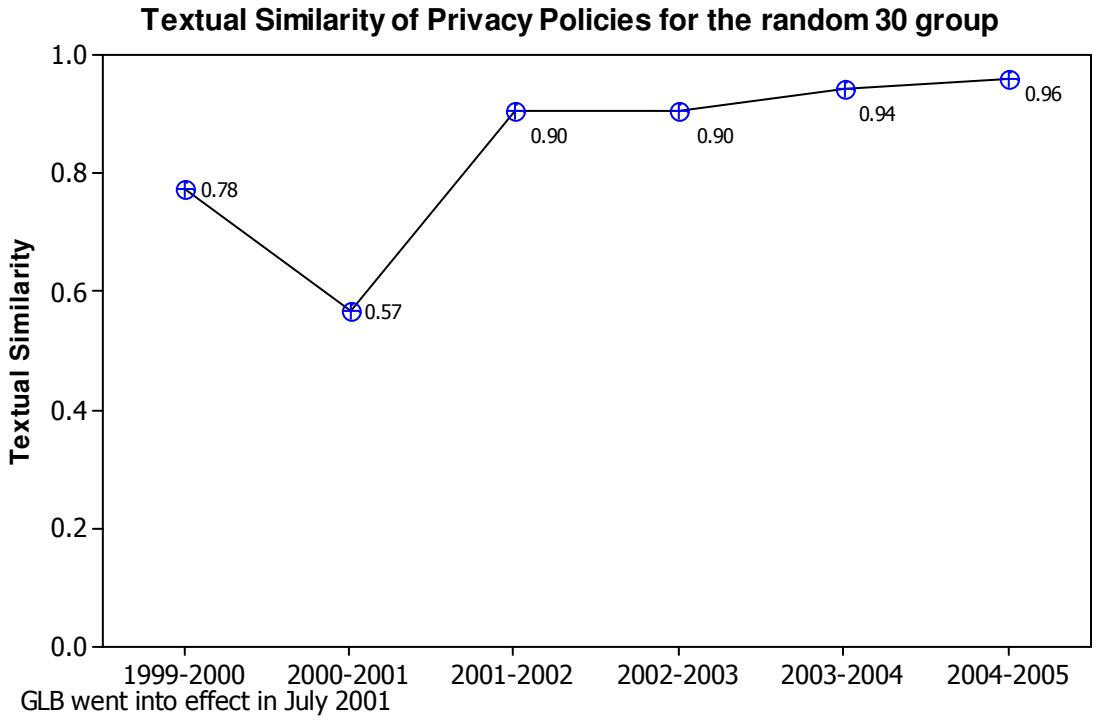

Figure 3: Mean textual Similarity of privacy policies for the random 30 group. Policies from the same institution in adjacent years are compared (for example 99 with 2000, 2000 with 2001)

4.2 The readability of policies has improved gradually but not significantly

The readability of financial privacy policies continually improved during the time period examined, with the largest changes observed between 1999 and 2002. In 1999, policies had an average Kincaid readability score of 14.5. This dropped to 13.0 in 2002. Figure 1 shows this improvement for the top10 and random 30 group of banks.

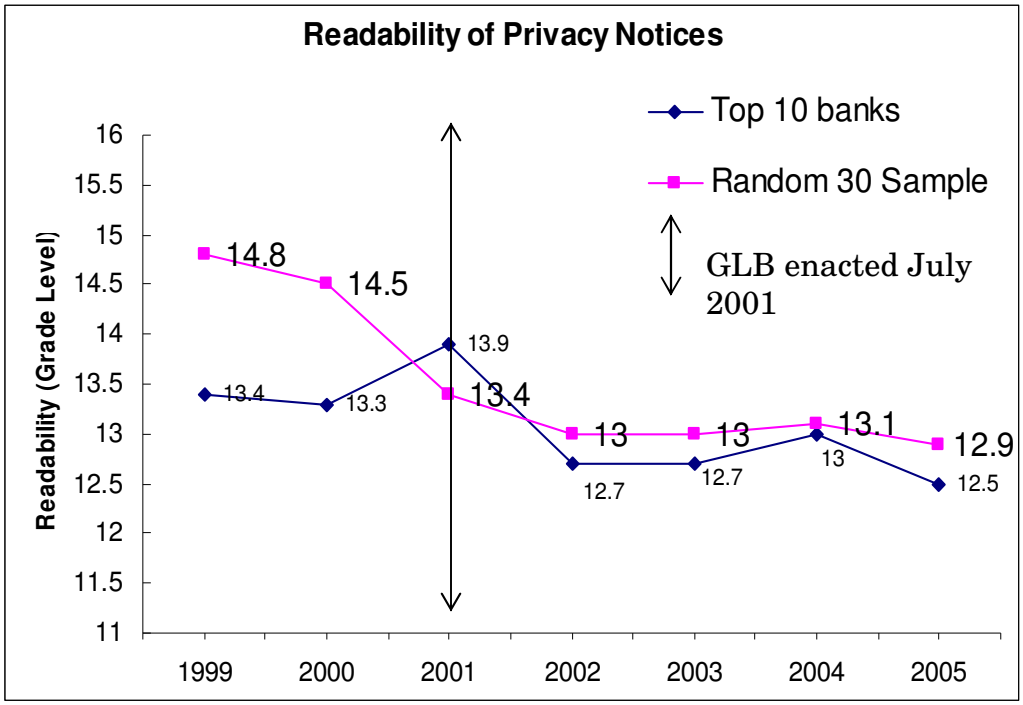

Figure 4: Mean readability of privacy policies measured by the kincaid score for the top 10 and random 30 banks group from 1999 to 2005. The number of data points for the random 30 banks from 1999 to 2005 is: 7, 29, 27, 26, 25, 24, and 30; for the top 10 banks are 5,8,8,5,6,5,10. GLB went into effect on July 1, 2001. The kincaid score corresponds to the equivalent years of education needed to understand the text.

The average kincaid score after 2002 leveled off at about 13.0, which roughly is equivalent to the U.S college freshman reading level.[52] In light of the fact that in 2005, 48% of the population over 15 has a high school or less education,[53] and comparing the common readability scores for other materials, the readability improvement we observed probably has not had much real impact. In addition, it is important to keep in mind that readability scores are calculated based on the length of words, sentences, and paragraphs, only. They do not take into account use of jargon or unfamiliar words, vague language, complicated sentence structure, or references to laws with which most people are unlikely to be familiar.

For example, although the following two statements have similar readability scores, the second makes a much more direct statement than the first:

> Bank A: "We do not share information about you with third parties outside of … , except as permitted by law."

[52] We have calculated various other readability measures such as ARI, and Gunning Fog index, and found similar trends.

[53] U.S Census Bereau, Educational Attainment in the United States: 2004 , Table 1. available at http://www.census.gov/population/www/socdemo/education/cps2004.html, accessed March 26, 2006

> Bank B: "We may share all the information we collect with our affiliates, and we may also share your information with companies we have joint marketing agreements with."

Arguably Bank A's statement is likely to mislead most consumers into thinking that Bank A engages in little sharing of personal information. In fact, Bank A and Bank B have virtually the same data sharing practices. This reason for this misunderstanding is that consumers may not know that the law actually contains only very limited restrictions on data sharing.

4.3 Banks and credit card companies minimally comply with GLB. Sharing with affiliates and third parties increased post-GLB.

Top 10 banks and credit card companies surveyed appear to only minimally comply with GLB, offering few if any privacy protections that go beyond what the law requires. These companies collect large amounts of information from consumers, and share information extensively with affiliates and third parties.

Typical information that banks collect include:

- application information such as personal information, assets, income and debts;
- transaction information such as account balances, types of account, payment history, credit card usage;
- consumer report information such as creditworthiness or credit history;
- information from outside sources such as employment verification, information about credit and other relationships, verification of information such as property insurance coverage; and
- information from online interactions with the company's websites.

As shown in Figure 5, all of the top 10 banks and 90% of the top 10 credit issuers had policies in 2005 indicating that they may share *all* information they collect with the affiliates. Only 10% of the banks in the random 30 group do not share with affiliates.

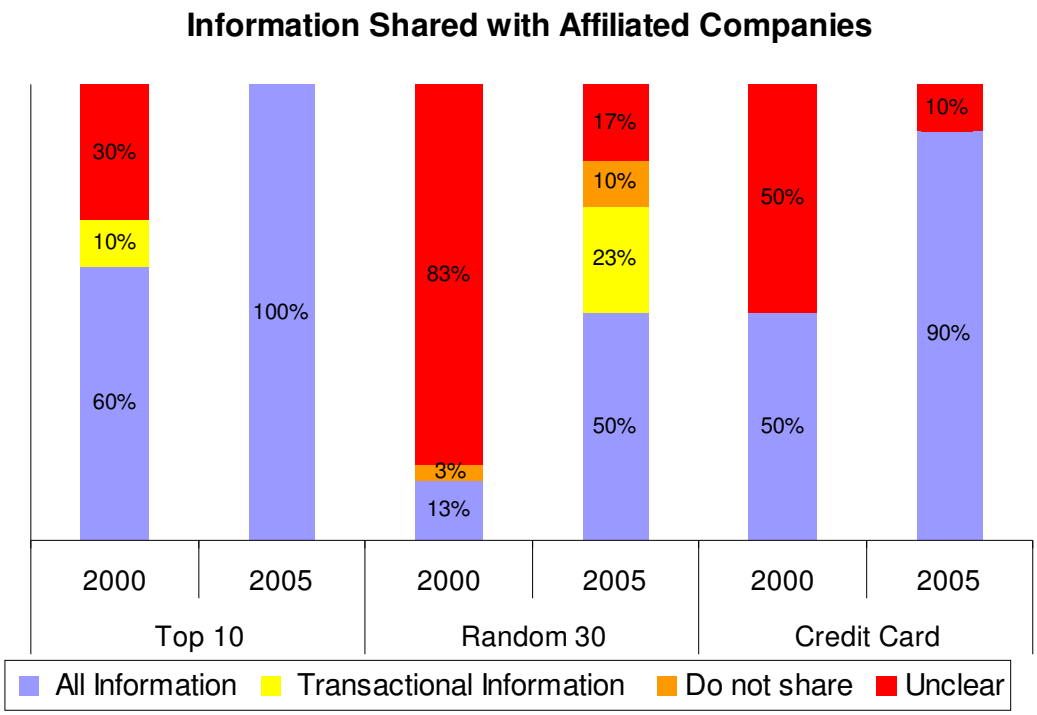

Figure 5: Affiliate sharing in 2000 and 2005 for the top 10 banks, random 30 banks and the top 10 personal credit issuers

Prior to the enactment of GLB, many bank privacy policies did not state clearly whether or not they shared information with affiliates or third parties. However, based on the high rate of affiliate sharing observed in 2005 it appears that this sharing has either increased or remained essentially unchanged. In addition, because GLB relaxes restrictions on the acquisition of affiliates, banks are acquiring an increasing number of affiliates and engaging in mergers. When banks merge, a large amount of customer information is consolidated. Since GLB places no limits on affiliate sharing, and few banks have voluntarily adopted policies that restrict their own affiliate sharing, individuals' financial data is now being shared more extensively than it was before GLB was enacted. We will address this in more detail in the policy implications section.

We also examined third party sharing (including joint marketing) before and after GLB. As shown in

Figure 6, third party sharing also appears to have increased after GLB was enacted.

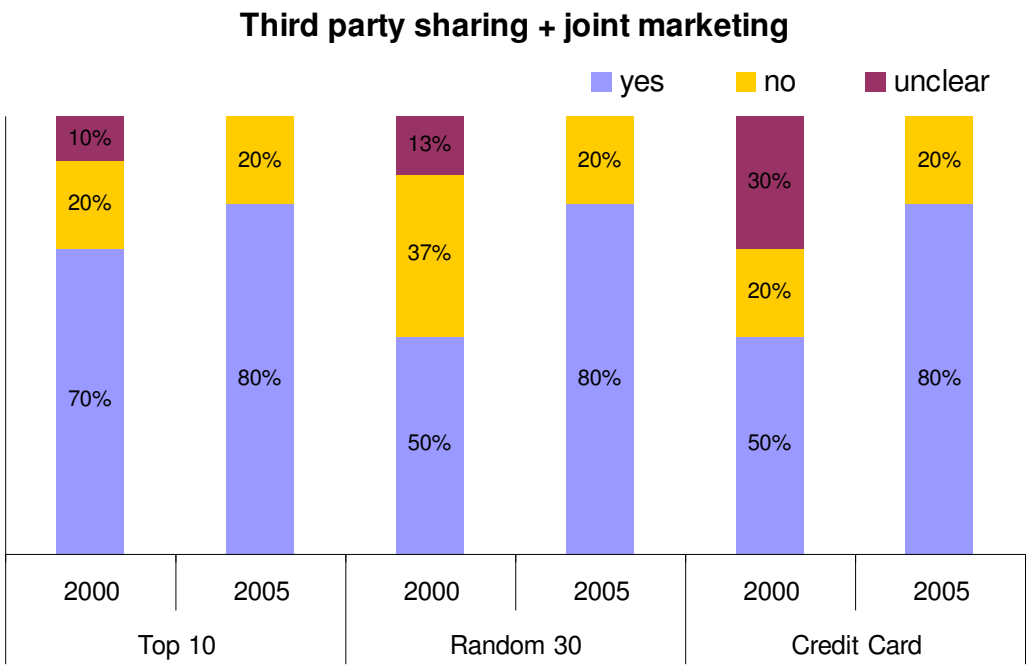

Figure 6: Third party sharing including joint marketing in 2000 and 2005 for each of the groups.

Although privacy policies often discuss third-party sharing and joint marketing agreements separately, we combine them here as We categorize joint marketing sharing as sharing with third parties, because in essence joint marketers are third parties. GLB does not require companies to offer consumers the ability to opt-out of joint marketing as long as they disclose in their privacy policies that they may engage in join marketing. However, if an opt-out is offered, then joint marketers can be treated as ordinary third parties, who may be permitted to further share the information with other companies. We find that the number of institutions sharing with third parties actual increases from 2000 to 2005.

4.4 Top retailers' privacy policies evolves more gradually, are less standardized, but offer better choices than top banks

We find that the top retailers' privacy policies exhibit a similar pattern of change as we observed in the policies of top financial institutions during the period examined. Figure 7 shows that the average length of the retail privacy policies increases at about the same pace as those of financial institutions, lending further support to the idea that GLB did not significantly change the policies of top financial institutions. It would be useful to compare a sample of random retailers similar to our random 30 banks to see whether random retailers' policies showed a sharp increase during the same time period that we observed a sharp increase in the length of random 30 bank policies. This would provide additional insights into whether changes in bank policies were directly caused by the GLB Act. We did observe that privacy policies in the retail sector evolved more gradually than they did in the financial sector. The median textual similarity between 2000 and 2001 is 0.89 for the retail sector, compared with 0.54 for the top-10 banks.

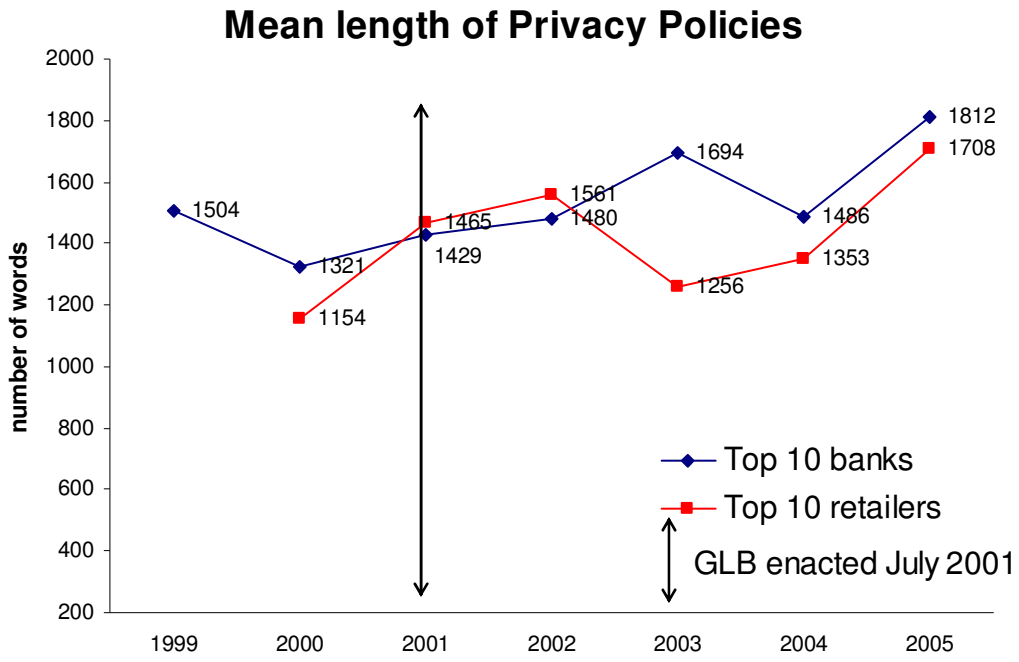

Figure 7: Length of Privacy Notices between retailer and banks

Overall privacy policies in the retail sector are more readable than in the financial sector, As shown in **Figure** 8, the readability of policies changed little for top-10 institutions during the period we studied.

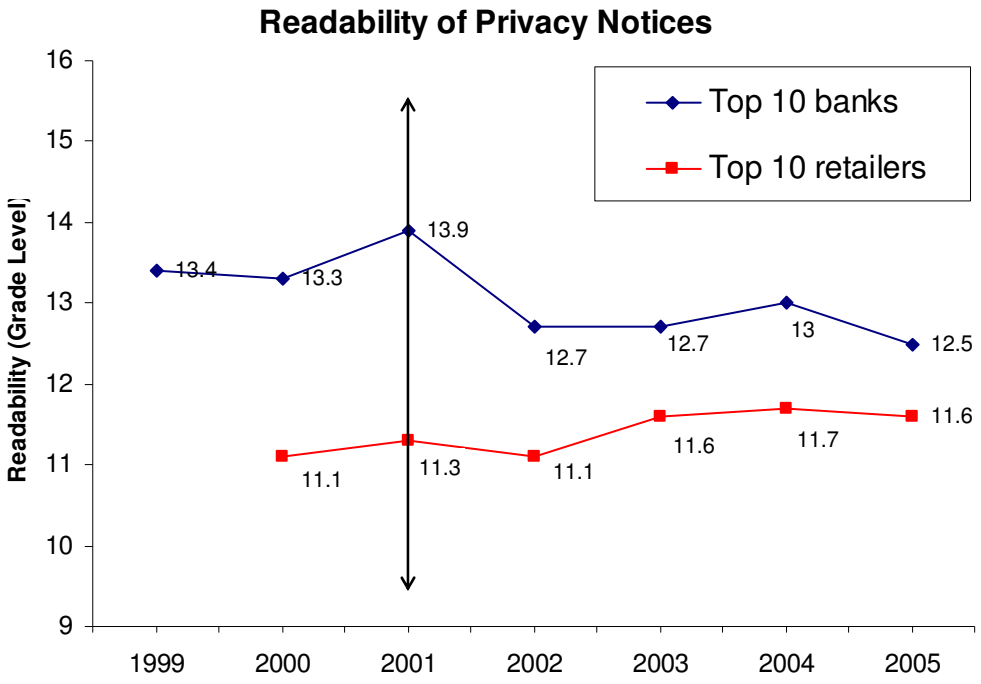

Figure 8: Readability of Policies between retailer and banks

Although the privacy policies of retailers are more readable, they are less standardized than the policies of financial institutions. For example, there is no standard definition as what exactly constitutes an "affiliate" in the retail sector. Some policies refer to "partners" and others use the term "subsidiaries."

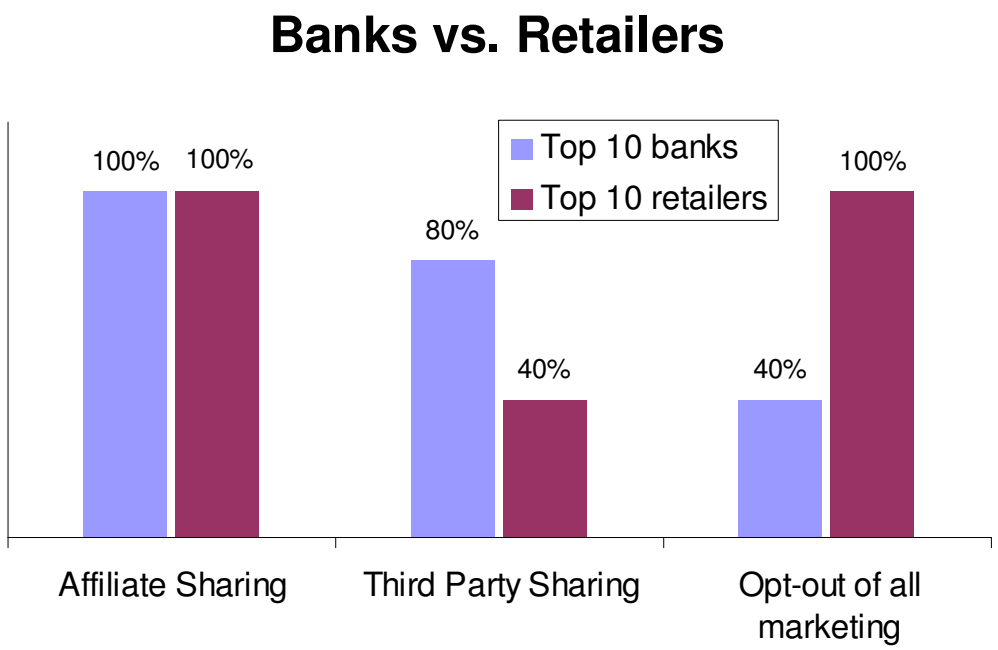

Figure 9: Top banks versus top retailers

All of the retailers surveyed shared personal information with affiliates, and none of them offer opt-out choices. This is very similar to what we observed in the banking industry. With regards to third party sharing for marketing, only four out of ten retailers share their information with third parties, and all of them offer opt-out choices. All of the retailers surveyed offer consumers opt-out choices for marketing, both internal and external, while only 4 of the top 10 banks offer similar choices. These results are shown in Figure 9.

Our comparison between the top-10 banks and top-10 retailers gives us some insights into the impacts of the GLB Act as compared with other influences, but it does not give us complete picture for two reasons. First, our sample size is small as we only include the top 10 retailers with significant online presence. Second, the retail industry has a very different structure from the financial industry. For example, retailers typically do not have as extensive affiliate networks as we see in the financial industry. Nevertheless, both industries are similarly influenced by other factors such as competition, increasing Internet adoption, rising privacy concerns, and increasing growth of e-commerce.

5. Policy Implication

Our research shows that the GLB Act serves some public policy objectives by making privacy policies more complete. The standard format and common vocabulary enables comparison amongst financial institutions. However, the readability of privacy policies has not improved significantly; such notices do not result in the majority of the population being better informed. Content analysis of the privacy policies shows that top banks and personal credit issuers minimally comply with GLB and there is little difference in terms of affiliate and third party data sharing among banks before and after GLB went into effect. This result has several policy implications that we will address in this section.

5.1 Impacts of increased affiliate and third party sharing

The fact that banks share extensively with affiliates without giving consumers choice has troubling implications. First, the GLB Act removes restrictions on banks acquiring affiliates. As shown in Figure 10, between 1999 and 2004 there have 1216 acquisitions of non-banks by banks. This is broken down by sector in Table 6. When banks merge, usually customer information databases are consolidated. In many circumstances, affiliate information sharing has little to do with the original purpose for which information was collected. For example, under the law, it is entirely plausible that a travel company owned by a bank could go through a customer's transaction data (for example, credit card charges) to find their favorite destinations and mail solicitations for travel deals.

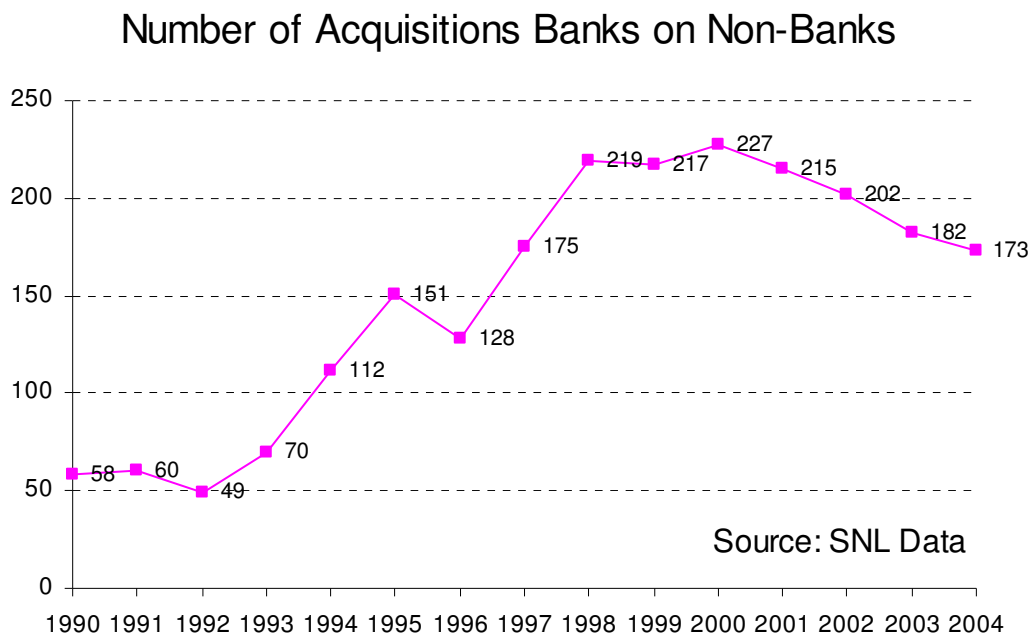

Figure 10: Number of Acquisitions banks on non-banks

Table 6: Acquisitions by sector since GLB enacted

Non-Bank Sectors	Total Transactions (1999-2004)
Insurance	405
Securities & Investments	317
Mortgage Production/Servicing Ops	121
Specialty Finance	124
Credit Card	76
Trust	60

5.2 Would the short notice approach work?

To improve the readability of financial privacy notices, the Federal government as well as industry groups have proposed short notices that summarize the complete legal notice.[54] Although we believe this approach can better inform consumers, we argue that this direction has its inherent limitations. Current research on disclosure system argues that a disclosure system would not achieve its goal if consumers have few real choices or do not believe there is anything more they need to know.[55] For example, they found that the restaurant rating systems in the Los Angeles County makes it easy for

[54] See http://www.ftc.gov/os/2003/12/031223anprfinalglbnotices.pdf

[55] Archon Fung, David Weil, Mary Graham and Elena Fagotto, The Political Economy of Transparency: What Makes Disclosure Policies Effective? (Boston: Ash Institute for Democratic Governance and Innovation, 2004).

consumers to compare restaurants hygiene ratings, giving the restaurant owners a strong incentive to improve their hygiene. However, other transparency system have not worked very well. For example, federal and state laws require employers label hazardous substances in their workplaces. This seems to have little impact in part because workers have very constrained choices about where to work and/or limited ability to change workplace conditions.

In the case for financial privacy notice, will a short notice serve a similar function as a restaurant rating system that could change consumer banking behaviors? Currently banks and credit card companies minimally comply with GLB, so the practices and choices they offer are very similar to each other and consumers' options with regards to privacy are limited. Perhaps short notices would provide additional incentives for some banks to adopt better practices so as to differentiate themselves.

5.3 Impacts of various state laws

The GLB privacy rule does not preempt other state laws that offer stronger privacy controls. As a result a number of states have taken advantage of this and have enacted their own privacy laws that are stronger than the GLB. For example, the California state legislature concluded that "the GLB Act increases the likelihood that the personal financial information of California residents will be widely shared among, between, and within companies. …. The policies intended to protect financial privacy imposed by the Gramm-Leach-Bliley Act are inadequate to meet the privacy concerns of California residents." As a result, they have enacted the financial privacy law for California (California SB 1).

Other states like Vermont and North Dakota have taken advantages of the no preemption clause in the GLB privacy rule and enacted tougher privacy laws. Increasing state laws and interstate commerce poses a compliance nightmare for banks, banks have to comply with differing state laws. If more states adopt supplemental privacy laws, a point would be reached when it is too costly for financial institutions to comply with every state law. This might actually clear the way for a more stringent, uniform national privacy law. This is certainly one of the reasons Microsoft is proposing comprehensive federal data privacy legislation that seeks to preempt state laws.[56]

6. Discussion and Future Work

This research provides some preliminary insights into the effects of the GLB Act privacy rule. However it also raises many additional questions and suggests other research areas to explore.

In order to better understand the trends we observed and to draw stronger statistically significant results, future work should sample a larger set of institutions, as well as draw comparisons with other industry sectors within the US and other countries.

---

[56] Brad Smith, general council for Microsoft, explained that "[t]he growing focus on privacy at both state and federal levels has resulted in an increasingly rapid adoption of well-intended privacy laws that are at times overlapping, inconsistent and often incomplete. This is not only confusing for businesses, but it also leaves consumers unprotected. A single federal approach will create a common standard for protection that consumers and businesses can understand and count on." http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx, last accessed, March 11, 2006

While the majority of the banks share extensively, a few *do* have policies that offer privacy protections beyond what is required by law. For example, in the top 10 group, bank of America and Wellsfargo do not share with non-affiliated third parties. A few banks in the random 30 group do not share with third parties as well. Why have these banks chosen not to share with affiliates, contrary to common industry practice? They may see privacy as an important issue to promote consumer trust, and therefore it is in their best interest not to share. For example, the Bank of America privacy policy says, "the law gives you protections, but we give you more." An alternative hypothesis is simply that they do not share with third parties because they have so many affiliates that they have no need to share with non-affiliated third parties.

When banks with different privacy practices merge or banks acquire credit card companies, what kind of policies do they adopt? Do they tend to adopt the more or less privacy protective policies? What are the factors that determine their decision?

Legislation generally not only affects the regulated industry, it can have some ripple effects in other industries as well. Could the enactment of financial privacy legislation be causing voluntary improvements in policy practices in other industries that are hoping to avoid similar legislation? This is an interesting and important question to explore further.

Although privacy policies are gradually becoming more readable, it is still not clear whether consumers can actually comprehend these policies? Can consumers understand the meaning and implications of their data sharing? Studies are needed in which privacy policies are read and interpreted by average consumers.[57]

In the absence of privacy regulation, some companies have voluntarily enrolled self-regulatory programs such as TRUSTe, and BBBOnline. Do companies that enroll in these programs have better policies than companies that do not enroll? How do the policies of companies enrolled in these programs compare with the policies of companies subject to privacy legislation?

Finally, our research looked at how the law affects external-facing privacy policies. How does the law affect the internal policies and practices of companies, for example resource allocation, internal data practices, policy enforcement, and communications with employees about privacy policies? An examination of internal privacy practices in regulated and unregulated companies would provide additional insights into the impacts of privacy laws.

7. Acknowledgements

The author gratefully acknowledges Ronnie Liu from KMPG for providing a dataset of the top 500 financial institutions; Mike Dekay and Judy Xi for many help on the statistics; Ponnurangam

[57] Cranor et al compared the comprehensibility of three natural language privacy policies with natural language interpretations of computer-readable privacy policies created by two P3P user agents. College-educated participants were asked to answer four questions about each policy they read and then to rate the ease with which they were able to perform each task. Although participants were able to answer the questions using the natural language and computer generated policies almost equally well, they reported that they found the computer-generated policies much easier to understand. L. Cranor, P. Guduru, and M. Arjula. User Interfaces for Privacy Agents. To appear in *ACM Transactions on Computer-Human Interaction*, 2006.

Kumaraguru for double coding 15% of the policies; and Paul Hines is to be thanked for helpful editorial comments.