A Large-Scale Evaluation of U.S. Financial Institutions’ Standardized Privacy Notices
Lorrie Faith Cranor, James T. Graves, Pedro Giovanni Leon, and Blase Ur
Carnegie Mellon University

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 and Howell 2003]. The act then 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. This standardized format for enumerating privacy practices was designed to “make disclosure of institutions’ information sharing practices and consumer choices more transparent” in an easy-to-read format [Federal Register, December 2009].

Although financial institutions in the United States are not required to use the model privacy form to disclose their privacy practices, the use of this form provides a safe harbor for privacy disclosures under GLBA [Federal Register, December 2009]. As a result, many financial institutions have used this model privacy form to make their mandatory privacy disclosures; hereafter referred as standardized notices. This fact provides a rare opportunity for analyzing privacy practices at large scale across an entire industry.

To this end, we collected lists of financial institutions in the United States and wrote a computer program that automatically queries Google in search of these companies’ standardized notices. Upon finding a standardized notice, the program automatically parses it 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, the Federal Deposit Insurance Corporation, and the National Credit Union Administration, 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 say may be collected. For additional insight into how practices compare within a given type of institution and across different types of institutions, we used the Federal Reserve definitions of types of financial institutions1 to cluster and analyze similar types of institutions. We also analyzed the policies of institutions on a Forbes list of the 100 largest banks2 and a J.D. Power survey of credit card satisfaction.3

---

1 http://www.ffiec.gov/nicpubweb/content/help/institution%20type%20description.htm
3 http://www.jdpower.com/content/press-release/xdTqU1T/2012-u-s-credit-card-satisfaction-study.htm (Visited last time in May 2014)
We found differences in stated data-sharing practices across financial institutions, even within a particular type and among companies on the same consumer-advice lists. Some institutions disclosed more privacy-protective practices stating that they did not share consumers’ personal information for purposes like marketing even when they were permitted to do so. Other institutions stated that they shared consumers’ personal information, yet allowed consumers to opt out of this data sharing even when they were not required to offer an opt-out.

Overall, our results showed that consumers do have the option to do business with more privacy-protective financial institutions, for some categories of financial services, if they so choose. An important consideration, however, is how an average consumer might identify institutions with better privacy practices. For small-scale comparisons, the standardized layout of the model privacy form has huge advantages over traditional, non-standardized privacy policies. Because the same information is located in the same place on each standardized notice, consumers can directly compare two or more institutions’ privacy practices by placing these institutions’ standardized notices next to each other. A particular strength of the model privacy form is the disclosure table. We found substantial differences in stated privacy practices across institutions simply by examining this table, suggesting that consumers can similarly be empowered to compare institutions’ privacy practices.

While the possibility of consumers choosing financial institutions based in part on privacy practices seems promising, the lack of a simple mechanism for a consumer to make these comparisons on any sort of large scale is unfortunate. For instance, it would be nice 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 are currently building a website to help consumers search for and compare financial institutions’ stated practices. This service will be publicly available in June 2014 at http://cups.cs.cmu.edu/bankprivacy

One can imagine financial institutions using more protective privacy practices as a competitive advantage. Research has shown that users are willing to pay 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.

Furthermore, our large-scale analysis enabled us to observe how government regulation impacts 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 by law to offer an opt-out. In these three cases, between 158 (2.6%) and 563 (9.1%) institutions stated that consumers could opt-out of data sharing, providing choice to consumers even when not required. Between 1,808 (29.2%) and 4,492 (72.6%) institutions stated that did not share consumer data at all for each of these three purposes. In contrast, between 1,331 (21.5%) and 3,832 (61.9%) institutions stated that they share data for these purposes without offering an opt-out. These practices are permitted by United States financial laws, but they are less privacy protective.
A large-scale, automated analysis also has the potential to detect problematic privacy practices. We identified financial institutions whose stated sharing practices violate United States law. For three data-sharing purposes considered in the privacy model, institutions were required to provide consumers a way to limit sharing [Federal Register, December 2009]. In violation of the law, about 100 (2%) of institutions said they shared data for these purposes, yet reported that consumers could not limit sharing. In a preliminary evaluation with a smaller number of analyzed institutions conducted last year, we found 24 institutions with notices that were not compliant with the law [Cranor et al. 2013]. When we contacted those institutions, some of them explained that the stated sharing practices on those notices were erroneous and that their actual practices were different. Although they amended their standardized notices accordingly, these cases suggest the need for stronger enforcement mechanisms.

However, previous research investigating compliance with the Platform for Privacy Preferences (P3P), a standard for machine-readable privacy policies proposed by industry organizations, found a much larger rate (more than 30%) of non-compliance [Leon et al. 2010]. Comparing levels of compliance with P3P and the model privacy form, we can conclude that companies feel more compelled to comply with standards when those standards are mandated by the government.

A limitation of the model privacy form is that it does not require institutions to disclose all types of information that they collect. In fact, it requires to only list “Social Security Number” and exactly 5 other types of information chosen from a list of 23 possibilities. The main purpose of the model privacy form was to help consumers understand financial institutions’ sharing practices, and not necessarily to provide a comprehensive list of the types of personal information that is collected [Kleimann Report 2006]. However, this requirement limits transparency and reduces consumers’ ability to compare institutions’ practices since a large fraction of companies end up listing exactly the same types of data.

Furthermore, we found that the data types that institutions tend to disclose are often obvious. Hence, less obvious (and potentially more sensitive) data types that institutions may collect and share can remain undisclosed. Since many of these standardized notices are already online, the use of layered notices could help to achieve both clarity and transparency by bringing 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. Requiring financial institutions to have notices that comprehensively disclose their collection practices is essential as many of these companies are taking advantage of the safe harbor provisions presenting the model privacy form as a supplement highlighting important points of a full-length privacy policies. While we believe the availability of short-form notices to be good for consumers, we also believe that traditional privacy policies should still be made available.

Finally, apart from the benefits that standardized notices can provide to consumers, regulators can leverage them to verify compliance with the law, the same way we did. Although, notices might not reflect actual practices, non-complaint notices can trigger further oversight.
References:


