LAYERED, OVERLAPPING, AND INCONSISTENT: A LARGE-SCALE ANALYSIS OF THE MULTIPLE PRIVACY POLICIES AND CONTROLS OF U.S. BANKS

Lu Xian[1], *Van Hong Tran*[2], *Lauren Lee*[1], *Meera Kumar*[1], *Yichen Zhang*[3], *Florian Schaub*[1]

[1]University of Michigan, [2]University of Chicago, [3]University of Wisconsin-Madison

Privacy policies are often complex. An exception is the two-page standardized notice that U.S. financial institutions must provide under the Gramm-Leach-Bliley Act (GLBA). However, banks now operate websites, mobile apps, and other services that involve complex data sharing practices that require additional privacy notices and do-not-sell opt-outs. We conducted a large-scale analysis of 2,073 U.S. banks, which collectively hold 97% of all FDIC-insured assets, examining how banks provide privacy disclosures in response to layered disclosure requirements, including the Gramm-Leach-Bliley Act (GLBA), other federal guidelines, and the California Consumer Privacy Act (CCPA), a key example of U.S. state privacy laws. We examined whether a given bank provides multiple privacy policies (GLBA, general, mobile, cookie, and CCPA policies) and controls (GLBA, cookie, and CCPA opt-outs), and whether inconsistencies exist across these policies that could mislead or confuse consumers (see Figure 1 for data collection pipeline). We focused specifically on *third-party data sharing for marketing*, which we considered to include both marketing/advertising and analytics/research purposes more broadly, along with the related opt-outs, because people often find these practices concerning, as they constitute violations of contextual integrity.

Summary of findings.

(1) Across banks, privacy policies are both numerous and difficult to understand for consumers. 45.2% of the banks provided multiple policies, typically a GLBA notice combined with general, mobile, CCPA, or cookie policy, which requires consumers to navigate heterogeneous formats, overlapping scopes, and divergent definitions of "personal information." Combined policy text for a single institution often reaches college-level readability, far exceeding average U.S. adult reading levels. Larger banks, which reach the greatest number of consumers, provide the most complex and voluminous disclosures (see Figure 2).

(2) Despite legal mandates intended to guarantee transparency and the central role privacy policies play in helping consumers understand how their data is used, our study reveals widespread inconsistencies across the notices issued by the same bank. We noted two prevalent yet nuanced inconsistency types: (a) 492 banks (53.8% of those with both a GLBA and other policies) said "no" under GLBA while saying "yes" elsewhere for related sharing. This highlights that GLBA "no" statements alone are insufficient for understanding banks' data practices, especially when online and mobile services are involved. A consumer reviewing only a GLBA notice may infer protections that do not extend to website tracking, analytics, or mobile-app data flows. Such inconsistencies undermine consumer comprehension and the transparency goals of the very laws that require privacy notices. (b) In contrast, 337 banks (36.8% of those with both a GLBA and other policies) disclosed sharing under GLBA and yet restricted such practices specifically for California residents. This pattern of discrepancy between GLBA and CCPA-related disclosures may indicate that banks specifically restrict their third-party sharing practices for their Californian customers while sharing their other customers' data more freely. Additionally, although not contributing to the inconsistency types identified above, many "we don't share" statements involved broad legal qualifiers like "except as permitted by law," which complicates the interpretation of such no-sharing disclosures and may mislead consumers.

(3) Our measurement of third-party tracking further shows that firms' data practices frequently diverge from their stated disclosures. Although banks mostly implemented the required opt-outs for GLBA, half of the banks that disclosed the sale/sharing of personal information under CCPA failed to implement the required opt-outs. 60% of banks allowed marketing third-party cookies on their websites, and yet only 15% of them disclosed this in their privacy policies. When opt-out tools are offered, they are often burdensome, with GLBA opt-outs commonly limited to telephone calls or postal mail rather than the more frictionless digital interfaces recommended by modern privacy guidelines. We also found that the naming of cookie controls and the labeling of different cookie types were both

highly varied, which may confuse consumers and prevent them from effectively opting out.

Our findings call into question whether current policy requirements, such as the GLBA notice, are achieving their intended goals in today's online banking landscape. Our findings highlight that the narrowly-scoped GLBA notice may mislead consumers, and that the layering of different disclosure requirements can undermine the transparency goals of the very laws that require them. Based on our findings, we provide recommendations and discuss concrete opportunities for regulatory reform that could reduce duplication, resolve inconsistencies across notices, and ultimately make privacy information more accessible and actionable for consumers.

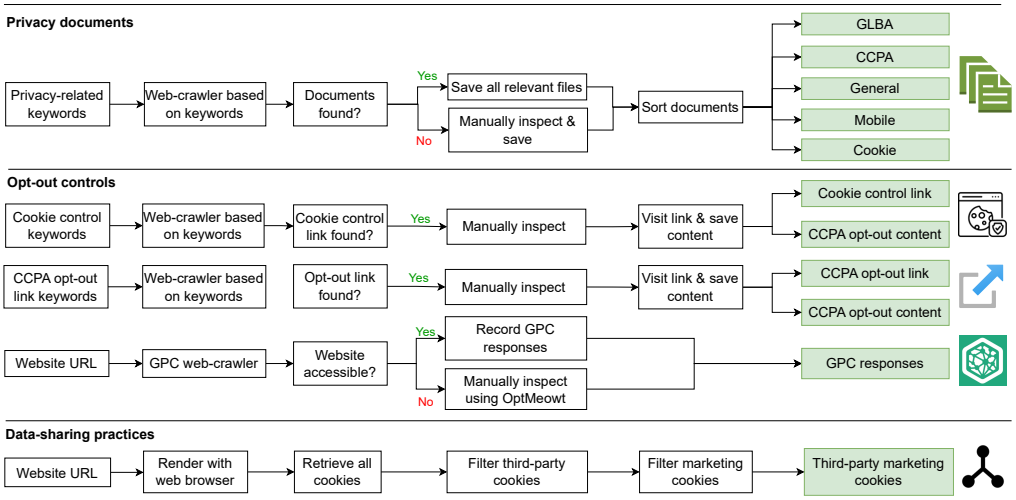

Figure 1. We collected the different privacy policies and third-party sharing opt-outs of the 2,073 largest U.S. banks.

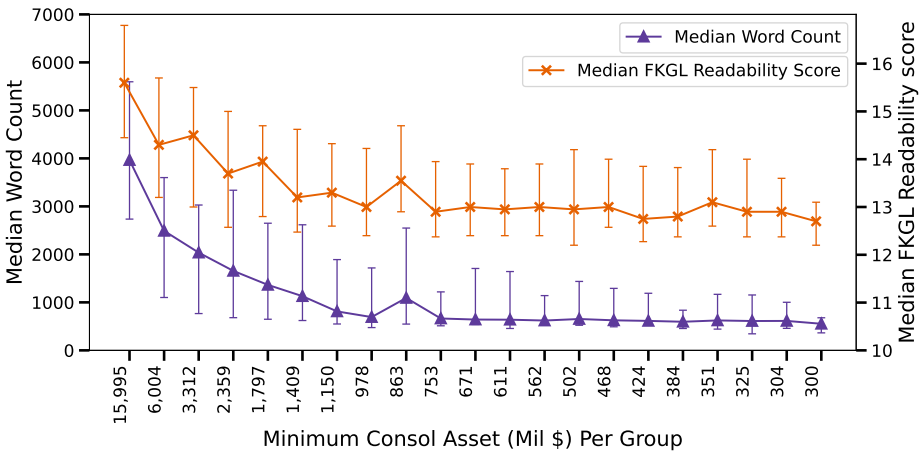

Figure 2. Word count and readability of all policies combined per bank. Banks are ranked by consolidated assets, a proxy for their sizes, and are then grouped into sets of 100 by rank for visualization purposes. Larger banks tend to provide more privacy policy content, but their policies are less readable.