



Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services

Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor,
and Kevin Butler, *University of Florida*

<https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bowers>

**This paper is included in the Proceedings of the
Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).**

July 12–14, 2017 • Santa Clara, CA, USA

ISBN 978-1-931971-39-3

**Open access to the Proceedings of the
Thirteenth Symposium
on Usable Privacy and Security
is sponsored by USENIX.**

Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services

Jasmine Bowers, Bradley Reaves, Imani Sherman, Patrick Traynor and Kevin Butler
{jdbowers, reaves, shermani, traynor, butler}@ufl.edu
Florida Institute for Cybersecurity (FICS) Research
University of Florida
Gainesville, Florida

ABSTRACT

Emerging digital financial services use mobile phones to provide access to populations traditionally excluded from the global economy. These “mobile money” services have proven extremely successful in their first ten years of deployment, and provide a powerful means of raising people out of poverty. Such services have access to a wealth of customer information, potentially including entire purchase histories, geolocation, and social network information. In this paper, we perform the first study of privacy policies in mobile money services, evaluating policies from 54 services and comparing them to 50 policies from traditional financial institutions. Because mobile money services are developed under a wide range of regulatory environments, we compare policies to the industry standard (the GSMA’s Mobile Privacy Principles) and to a traditional national standard (the FDIC’s Privacy Rule Handbook). Our analysis shows that almost half (44%) of these mobile money services do not have *any* privacy policy whatsoever. Of the services that do have privacy policies, roughly one-third (33%) fail to provide them in either of the two most common languages of their market. Furthermore, 50% of these policies do not ever identify to the user what data is actually being collected and stored. Finally, we find that where policies do exist, they are often incomplete and difficult to read by their target customers. These findings show that more work is needed to protect consumer privacy within these mobile money services.

1. INTRODUCTION

Cashless systems underpin our modern economy and the developed world now relies heavily on a massive digital infrastructure capable of moving money across the globe without delay. However, many parts of the world remain unable to easily access these traditional financial

networks, often limiting economic expansion and burdening the majority of people around the world with the physical risks and challenges associated with managing currency (e.g., theft, difficulty performing transactions, etc).

“Mobile money” services attempt to address this problem by making phones into payment platforms. Two arbitrary parties, whether in person or at a great distance, can easily transfer money between each other instantaneously. Technologically, this is implemented by various means: built-in “apps” for feature phones, simple text messages exchanged with the mobile money system, and in some limited cases smart phone apps. While conceptually simple, this technology has proven transformative. First, citizens incapable of visiting traditional banking services or maintaining relatively high minimum balances can participate in such services and pay only minimal transaction fees. Second, because virtually anyone with a phone can participate, it is simple for nearly every person and vendor in a country to be enrolled in the service. Finally, many such services are using information gathered on transactions to generate non-traditional creditworthiness measurements and insurance profiles, further enabling those in developing economies to gain access to investments that have proven essential for raising people out of poverty [39].

The implications of collecting and managing customer data in this environment are more risky than in traditional financial services. Specifically, because true peer-to-peer payment is enabled by mobile money services, they learn both their customers’ entire financial history and their social network. Moreover, many services also collect supplementary information including geographic location and the names of other applications installed on a device. The need for strong, clearly written privacy policies is therefore evident, and has been strongly supported by the industry group (i.e., the GSMA) since 2011 [43]. However, how the industry has adopted such regulation has not previously been explored.

In this paper, we perform the first independent analysis of privacy policies for the mobile money industry. While work has been done to evaluate privacy policies of traditional financial services in the past [13, 19, 37], our work is different for a number of reasons. First,

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12–14, 2017, Santa Clara, California.

ours is the first work to evaluate mobile money services, which are generally run by non-traditional financial entities (e.g., telecommunications providers) and are therefore not subject to the same kinds of regulations as the conventional banking industry. Second, we are not attempting to measure the “goodness” of the standards for the industry; rather, our work seeks to measure mobile money services against standards that are already in place. We believe this is critical as it measures the health of consumer privacy within the industry as expectations are currently set. Arguments for greater protections beyond what is suggested can always be made. Finally, mobile money services served approximately 411 million customers in 2015, and recent moves including demonetization in India put the industry’s population base in the billions [38]. As these customers often represent many of the world’s most financially vulnerable, it is critical for the privacy community to ensure that they are adequately protected.

We make the following contributions:

Compare Policies Against GSMA and FDIC Recommendations: Given that mobile money services are deployed across a wide range of regulatory environments, performance against a single national standard for privacy policies would be incomplete. Accordingly, we determine how these services conform to the mobile money industry (i.e., the GSMA) and widely used government (i.e., the US Federal Deposit Insurance Corporation (FDIC)) recommendations for communicating privacy policies. Our analysis shows that mobile money services lag significantly behind traditional financial institutions, with 44% having no available policy. Moreover, where policies are available, their coverage of critical topics is often limited. All but one service fail to meet either standard.

Measure Readability: Literacy rates are often lower in the developing world. To measure whether or not privacy policies adjust for this difference, we use multiple tests of readability from the linguistics community to compare traditional financial and mobile money offerings. We show that, on average, privacy policies for mobile money services have a higher grade-level readability score than traditional banks (12.1 vs 10.8), meaning that such policies are in general harder to understand.

Measure Availability in Official Languages: Given that mobile money services are available in a wide array of countries, we would expect that we would see privacy policies available in a wide array of languages. Unfortunately, our study shows of the mobile money services that have a privacy policy, 33% of them do not have a version written in the first or second official language of their country of operation.

We believe that our results point to a critical problem for mobile money services: privacy policies are not widely available, and where they are, the majority of them suffer from low readability and coverage issues. By providing the first such study of these policies, we believe that government and industry regulators can (and must) better address this problem.

The remainder of the paper is organized as follows: Section 2 discusses related research; Section 3 provides background on mobile money; Section 4 describes our methodology; Section 5 provides our results; Section 6 further discusses the implications of these results, and Section 7 provides concluding remarks.

2. RELATED WORK

Mobile money services have had enormous positive impact in enabling financial inclusion in the developing world. However, the security provided by such services has recently come into question. First generation services, which rely on SMS or USSD channels in 2G networks, are inherently insecure due to the use of weak (or no) ciphers on the air interface and the lack of strong end-to-end encryption [10,28]. Unfortunately, Reaves et al. [31] demonstrated systemic problems in smart phone apps throughout the ecosystem, including poor configuration, failure to properly authenticate certificates and in some cases, a complete lack of any protections. Moreover, most developers failed to improve the security of their applications over a year later in spite of receiving detailed vulnerability reports [30]. Castle et al. interviewed developers to understand the cause of such weaknesses, learning that many developers had difficulty properly using security libraries [11].

Creating “good” privacy policies is a challenge in and of itself. Entities handling user data must strike a careful balance between both comprehension and comprehensiveness. A number of researchers [21, 32, 36] provide guidelines for policy creation. McDonald and Cranor [25] argued that a singular focus on coverage represents a significant expense to users and determined that it would take users over 200 hours per year to read the policy of each website visited. Other researchers have attempted to achieve such balance, using techniques such as bulleted lists [17], privacy “nutrition labels” [22], and natural language processing for minimization [46]. Unfortunately, while such techniques appear to improve readability, only one (Federal Reserve privacy notice template) has been adopted at large scale [4]. Our work is able to bypass this challenge to some extent, as it seeks to measure adherence to widely known standards.

While Reaves et al. [31] did evaluate the terms of service for mobile money services they studied, the state of privacy policies in the mobile money environment has not previously been examined. Academic analysis of privacy policies in financial services dates back to at least 2001, with Hochhauser’s study demonstrating that understanding the privacy policies of the top 60 US-based financial institutions required an average reading level of 15.6 (i.e., the reading level of a 3rd year college student) [19]. Jensen and Potts [20] measured readability and accessibility in the privacy policies of well-known websites, similarly finding a great need for improved readability. More recently, Cranor et al. [13] conducted a large-scale study of 6,191 US-based financial institutions and focused on their policies for third parties, reasons for data sharing, and opt-out. Closest to our work is that of Sheng et al., [37] which found a lack of significant improvements to privacy policies

after the passage of the Gramm-Leach-Bliley (GLBA) Act [45], which mandated that banks make clear how they handle private customer data.

3. MOBILE MONEY

Billions throughout the developing world lack access to even the most basic financial services, and this especially includes many of the world’s poor [7]. Financial exclusion result in difficulty receiving wages, government transfers, remittances, making payments, and transferring money to local friends or relatives. This is to say nothing of the lack of simple conveniences provided by the modern financial services. There are a number of reasons why the poor are excluded from traditional financial services, including account fees, difficulty conducting business during relatively limited banking hours, and simple lack of available services (especially in rural areas).

In recognition of this problem, governments and development agencies are embarking upon programs to improve financial inclusion. These efforts are worthwhile because making saving and transferring money easier gives participants the ability to better support themselves as well as provide a safety net for family and friends. In many cases, such safety nets prevent minor financial setbacks from becoming personal crises.

One of the barriers to financial inclusion is that traditional brick-and-mortar banking comes at a high overhead, and it is simply not economical to provide services to customers with low transaction volume or balances. As a result, governments and NGOs are turning to a new model for financial inclusion: digital financial services served through ubiquitous mobile devices.

Services that provide the ability to store value and make payments through mobile phones are often called “mobile money services.” The first such service, M-Pesa, was deployed by SafariCom in 2007. M-Pesa pioneered a model where users could send and receive payments directly from their mobile phone, as well as deposit and withdraw funds from an account at any local airtime vendor. This model quickly achieved enormous success, and by 2013 M-Pesa supported payments amounting to a third of Kenyan GDP [26]. Other carriers and third party providers have taken notice, and supported by development organizations like the Gates Foundation and the World Bank, industry consortia like the GSMA, as well as motivated by their own commercial interest, mobile money services have been deployed in developing countries worldwide. Mobile money services have been augmented by other financial services – notably micro-finance (small loans) and even life insurance. Figure 10 in Appendix 7 shows the EcoCash mobile app payment interface.

Mobile money services are distinct from both traditional mobile banking (i.e., phone-based access to traditional banking accounts) and many popular mobile payment services in developed countries (e.g., PayPal, Venmo). Figure 1 highlights the most important differentiators.

First and foremost, mobile money is distinct because



	Mobile Money	Mobile Banking & Mobile Payments
		
Target Audience	Unbanked consumers	Existing customers
Financial System	Non-interoperable, closed-loop	Global interoperable financial network
Regulators	Financial, Telecom, or other agencies	Financial regulators only
Technology	SMS, USSD, Mobile Internet	Mobile Internet Only

Figure 1: Mobile money services are distinct from traditional mobile banking and mobile payments in several important ways.

of the market it serves. Mobile money services primarily target unbanked customers new to financial services, while traditional mobile banking and payment services focus on providing new features to existing customers. Second, mobile money is neither based on nor is currently interoperable with the existing traditional banking service. In fact, mobile money services are only rarely interoperable with one another, even within the same market. By contrast, both traditional mobile banking and mobile payment services like Apple Pay interact with the global banking network.

Mobile money services are also technologically unique. Some services are available exclusively through mechanisms compatible with feature phones like SMS or Universal Supplementary Services Data (USSD) in the cellular network. As smartphones increase in popularity in developing countries, more mobile money services are deploying smartphone apps. Many of these services, regardless of whether they operate using legacy channels, smartphone apps, or both, often expose their users to avoidable security vulnerabilities that place their users at risk of loss of funds or disclosure of personal information [11, 31]. This is particularly troubling because the terms of service of most of these services hold users accountable for losses due to fraud, in contrast to regulations and policies like those in the United States, which limit the consumers’ exposure to and liability for loss.

In fact, regulatory structures are another area where mobile money is distinctive compared to traditional banking. Many governments are enabling and encouraging mobile money growth by significantly relaxing the regulatory requirements for mobile money services. For example, many “Know Your Customer (KYC)” and anti-money laundering and countering financing of terrorism (AML/CFT) regulations are significantly relaxed to enable simple and practical enrollment of mobile money users. These regulation relaxations are necessary for



Figure 2: Countries represented in our selection of all mobile money services known to have Android apps.

mobile money to be successful, and AML/CFT goals are typically addressed by simply limiting the balances users are allowed to accumulate. However, the need for relaxed regulations in registration does not mean that regulations in other areas – particularly for data security, fraud liability, and data privacy – are unnecessary. Many mobile money services use transaction data to generate non-traditional creditworthiness measurements for users in developing economies.

4. METHODOLOGY

Our research seeks to address three main questions. First, *do mobile money applications have privacy policies and, if so, what do they cover?* Second, *are these policies written such that they are understandable by their target audience?* Finally, *are these policies written in the most commonly spoken languages in the country in which the application is deployed?*

To answer these questions, we began by collecting privacy policies of the top US banks by assets to serve as a reference group. We chose these banks because they have a well-understood regulatory structure. Because a similar set was studied in prior work [19], we argue that our observations in this space serve as a comparison point for emerging digital financial services. We then collect all available privacy policies for all 54 mobile money applications known to have an Android app in 2016. We focus on services with Android apps because smartphone applications have the ability to collect extremely fine-grained data about their users’ behavior, in contrast with the limited data collection made possible with feature-phone based services.

We then manually code these policies to investigate compliance with the industry-wide guidance provided by the GSMA as well as the guidance provided by the FDIC. The GSMA Mobile Privacy Principles represent an international accord on privacy policies agreed to by the industry trade group. The GSMA principles have been publicly available since 2011 [43], thereby allowing sufficient time for mobile money services to incorporate its requirements. We note that the GSMA has also released a Code of Conduct specifically for mobile money

providers [42]. This document directly addresses issues of user privacy, and explicitly calls on mobile money services to ensure the following principles: “Governance”, “Transparency and Notice”, “User Choice and Control” and “Minimization of Data Collection and Retention”. We decided to use the more complete set of Mobile Privacy Principles [43] for three reasons. First, the Code of Conduct has only been publicly available since 2014, three years fewer than the Mobile Privacy Principles document. Second, with the exception of “Governance”, each of the practices in the Code of Conduct maps directly to a principle in the Mobile Privacy Principles. “Governance” most readily maps to “Accountability and Enforcement”. Third, because mobile money services comprise mobile applications, the more explicit Mobile Privacy Principles apply to them as well.

Why use the FDIC principles: The FDIC principles [16] provide a more comprehensive standard by which to evaluate privacy statements than the GSMA standards. It was simply not practical to judge each policy based on the standards of the 32 different countries for which we collected mobile money apps. Accordingly, to have an objective basis of comparison, we chose to standardize our analysis on the FDIC standards and the GSMA standards. Including the FDIC principles allowed us to compare the policy coverage of US banks and mobile money applications to both US and international standards, although we understand that there are many confounds that will affect this comparison. We do not claim that the FDIC principles are an ideal standard, but an objective one that has been widely examined. It is also one we believe to be reasonably comprehensive. We readily admit that existing mobile money policies may not have been written with FDIC standards in mind; at the same time, the FDIC principles are general enough that we believe that the content they cover should be in any good privacy policy.

We conclude with an analysis of readability of policies and an analysis of availability of mobile money policies in dominant languages in their respective countries.

4.1 FDIC and GSMA Regulations

The GSMA and FDIC identify key principles that all privacy policies should adhere to and include. Below are the 11 principles used in our privacy policy analysis:

GSMA

Purpose of Data Collection: Policies should disclose the purpose of collecting, accessing, and sharing user data and ensure that each purpose is for legitimate business operations.

Children and Adolescents: If applicable to children, the service should guarantee that the child’s personal information is properly collected and should abide by all laws related to children’s privacy.

Accountability and Enforcement: Employees are held accountable for proper use and protection of user data.

FDIC

Collection Process: Notices should list the types of personal information that is collected.

Definitions: Notices should terms concerning collection process, information disclosure, etc.

Examples: Notices should include examples of the collection process, information disclosure, etc.

Third Parties: Notices should disclose affiliates that the bank shares nonpublic personal information with.

FDIC & GSMA

User Choice and Control: Notices should disclose the user's right to opt-out and how users can control the use of their personal information.

Security: Notices should disclose how personal information of users will be protected and safeguarded.

Sharing Process: Notices should include the personal information of users that may be disclosed.

Data Minimization/Retention: Information sharing practices of personal information of former customers should be disclosed and only the minimum amount of user information should be collected, accessed, and used at all times.

4.2 Selection and Collection Process

We compiled a list of the top 50 U.S. banks (by assets) based on the Federal Reserves Statistical Release of Large Commercial Banks [5]. We used the GSMA Mobile Money Tracker [18] to identify mobile money services, then manually searched the Google Play market and mobile money provider websites to locate those with smartphone applications. While a large number of applications exist, we carefully inspected each candidate application to ensure that it actually provides payment functionality. We identified 54 such services from 32 countries, as shown in Figure 2.

We located and downloaded privacy policies for all of the banks and mobile money services studied. Our search process was systematic and exhaustive, and is described below.

For a mobile money service, we first visit the app's Google Play Store profile to determine if a privacy policy link exists. If yes, we downloaded the policy from the Play Store. Otherwise we visit the website link in the Play Store (if present) or search Google for the website. If a website was not found after the Google search, the app was marked as not having a policy.

On the website for a mobile money service or bank, we first search for app's privacy policy on the main page. If not found, we searched the website to locate a policy. As a last resort, we examined the "About" pages of the website, then directly searched Google for a policy. Finally, if no policy had been found, we mark the bank or service as not having a policy.

We gathered every privacy notice/policy available on each bank or service's website, including documents termed "privacy policy," "privacy notice," "consumer privacy pol-

icy," "cookie policies," "online privacy policies," and "mobile privacy policies". Where applicable, we also investigated "terms of service" documents. We collect and analyze all privacy related documents, because some of the banks used the terms "privacy notice" and "privacy policy" interchangeably.

4.3 Coding Process

We conducted a manual coding analysis to determine which principles our collected policies adhered to.

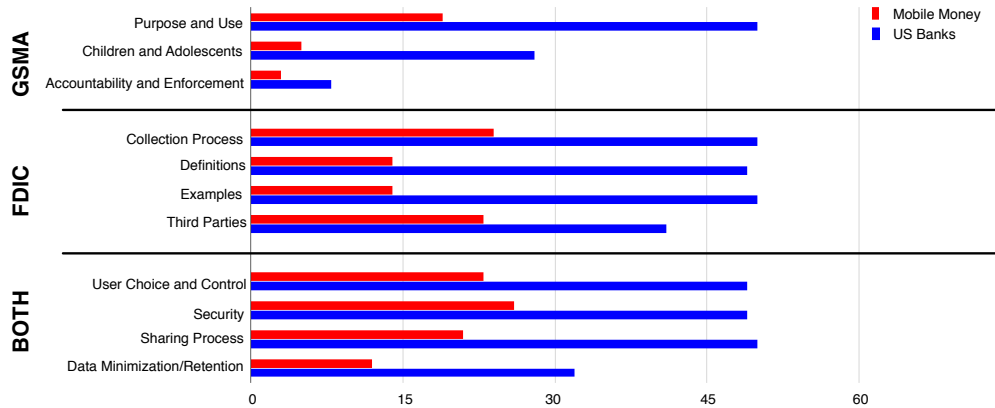
Our coding analysis consisted of two key phases: an initial key word search and subsequent manual analysis. Before coding, we generated a codebook that directly correlated to our policy principles. For example keywords for the **user options** principle included *disable*, *edit*, *user can request*, *user can edit*, *user can change*. We show our codebook in Appendix 7 in Table 3.

We note that a document only needed to *simply mention* the principle to receive credit for covering that principle. We do not otherwise evaluate the extent to which we believe the policy adheres to the letter or spirit of the recommendations. Because our work primarily is concerned with whether policies cover the requisite data *at all*, the absence of a principle in our reports is a strong indicator important privacy issues are being ignored by a particular policy. Thus, the keyword analysis was sufficient to show that most of the mobile money policies failed to mention why data was collected.

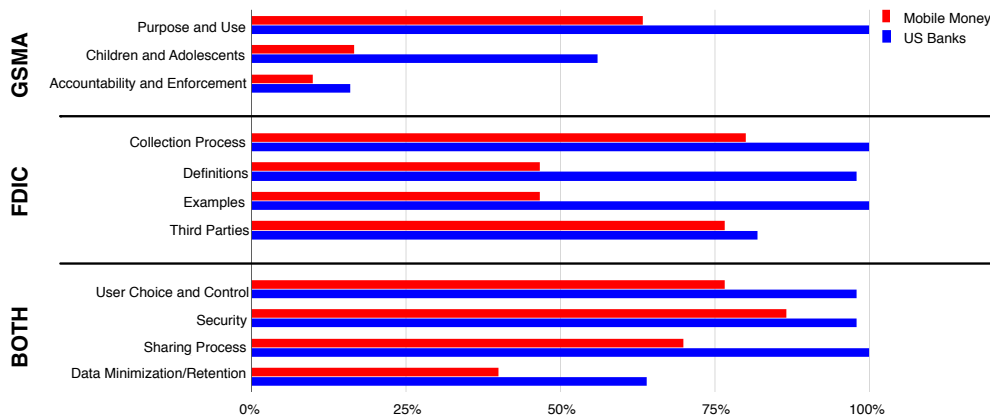
Two of the authors, both PhD students with a prior graduate course in privacy communication, served as the coders. Coders were provided with a digital copy of each policy document. A Google Form was created to streamline the coding process and eliminate error. The coders were instructed to score each policy based on the 11 principles and their corresponding keywords. During the coding process, if the coder did not find exact keywords in the codebook but did find similar text, the coder was instructed to use their best judgment when scoring that principle. The coders were instructed to only assess the policy document and not any other resources (e.g., website.) If neither the keywords nor similar text were found for a specific principle, the policy received a score of zero for that principle.

Once all documents were analyzed individually, we combined the results for every bank or service so that if any of a bank or service's documents discussed a principle, we consider that bank or service as having a documented policy for that principle. For example, Bank of America's Consumer Privacy Notice discusses data minimization/retention, while the Cookie Guide does not. Thus, we mark Bank of America as having a policy for data minimization since at least one of its documents discussed the principle.

The results of the independent trials were compared and mutually reconciled to arrive at the reported data. During the reconciliation process, if the results of the coders differed, we discussed the instructions and thought process with both coders to determine the final score for each policy and principle.



(a) Total Number of Systems



(b) Percentage of Policies Found

Figure 3: Representation of policies that cover each principle in the GSMA, FDIC, or both sets of recommendations. For every principle, banks outperform mobile money services

We computed Cohen’s Kappa to measure inter-rater reliability on codings of each policy. Coders agreed “substantially” ($\kappa > 0.8$) on five categories: Purpose and Use, Children and Adolescents, Definitions, Examples, and Security. In addition, the results of five other categories (Accountability and Enforcement, Collection Process, Third Parties, User Choice and Control, and Data Minimization/Retention) were classified “moderate” (0.41-0.60) and one (Sharing Process) was classified “slight” (0-0.20) [23]. In this latter case, the coders differed in their interpretation of whether the Sharing Process principle was met. One coder gave the policy credit if it simply mentioned sharing, while the other coder looked for a more concrete process (e.g., the sentence “We will limit the access, collection, sharing, disclosure, and further use of your Personal Information to meeting legitimate business purposes or to otherwise meet legal obligations” in the GCash policy was interpreted differently). Coders reconciled their differences by agreeing to adopt the broadest reasonable interpretation of the principle. The same procedure occurred with respect to categories with moderate kappa values.

4.4 Readability Analysis

The linguistics community has created a number of metrics that compute a document’s readability score indexed to “grade level” expectations of reading ability. While there are a number of such scores, including the well-known Flesch-Kincaid score, the linguistics community has yet to identify a single, “gold-standard” technique. Accordingly, it has become common (including within the literature on privacy policies [8] and medical documents [9, 15, 40]), to use more than one readability scoring mechanism in their study.

To measure the readability of our privacy policies, we first manually condense the various policies into individual text-only documents to be analyzed. This manual canonicalization ensured that formatting and typography (e.g., two-column documents) did not prevent an accurate assessment. We then calculated a number of properties of the submitted text, including five readability scores, the estimated reading time, and summary statistics like word counts. We computed the Flesch-Kincaid Grade Level score, the Gunning-Fog score, the Coleman-Liau Index, the SMOG Index, and the Au-

tomated Readability Index. Large, distinct documents had their readability assessed independently, then averaged to produce the final score for a bank or service.

4.5 Language Analysis

Many mobile money services operate in nations that are multilingual, and it is important that the policies are provided in languages users actually can read.

Mobile money is a global phenomenon, but practically all services serve a single country. Because language needs vary in different countries, we searched the website of each mobile money service for the availability of privacy policies in multiple languages. To enable an objective comparison among services, we search for only the top two languages in the relevant country as reported by the CIA World Fact Book [6]. In some cases, the World Fact Book reports actual percentages of population that speak a particular language; we use those figures to identify the “top two” languages where available. When unavailable, we use the first two languages listed in the World Fact Book. We also found that three countries with mobile money services (Uruguay, Dominican Republic and Brazil) only had one official language, and our reported results reflect this.

We note that our analysis of policy details is limited to the available English-language policies. A deeper analysis of non-English policies was not possible given that we found documents written in more than 10 languages. Additionally, because automated translation is known to be an open problem, we did not attempt to use such tools to translate such documents as they were likely to unfairly create errors.

5. RESULTS

The individual banks and services studied and their performance on all 11 guidelines are presented in Table 1 and Table 2 in Appendix 7. A summary of the counts of both banks and mobile money services adhering to each principle are shown in Figure 3a and Figure 3b. In the figures, we present whether mobile money systems adhere to the recommendations we describe in two ways. The first is a total count basis: “of the systems we analyze, how many provide the recommended disclosures to their users.” This reflects the ability of mobile money users to learn about how their data is used. The second is on a percentage basis: “of the policies we have, how many adhere to the recommendations for privacy disclosure.” This second graph indicates the overall coverage of policies *when they exist*. We provide the first analysis of how privacy is guaranteed in mobile money services and how it compares to privacy in an established banking ecosystem.

5.1 Availability and Freshness

Our first analysis looks at the availability and update frequency of privacy policies for both top US Banks and mobile money services.

Policy Availability: We find that all of the 50 US banks provided at least one privacy policy document. However, only 30 out of the 54 mobile money services

we examined had a privacy policy, meaning that 24 services, or 44.4% of all mobile money services with smartphone apps, had *no privacy policy of any sort*, rendering any analysis of their handling of sensitive data impossible. This means that neither privacy experts nor end users have any knowledge of the data practices of these services, much less any rights or guarantees about how that data will be used.

Update Frequency: Privacy policies should be regularly updated to ensure that they still reflect current data handling practices. While the FDIC requires all banks to develop and disseminate updated privacy policies at least once in any 12-month period [16], we found that only 30 of the 50 banks had policies that had been updated within the past year. Mobile money services demonstrated less frequent updates of privacy policies. Of the 30 services that had a privacy policy, only 9 (30%), included information about when they were either written or last updated. Of these 9 services with dated policies, only 5 (17%), had policies that had been updated within the past year.

These first two measures already indicate an important difference between the practices of traditional financial institutions. While both sectors could improve their performance in keeping policies updated, traditional financial institutions far outperform mobile money services in making policies available.

5.2 Policy Content

We next examined the content of the privacy policies we obtained to determine how they adhered to both national regulators (FDIC) and industry guidelines (GSMA).

Substantially more banks adhered to every principle we track than mobile money services. Only one mobile money service, GCash, covers all principles. This is surprising because many more banks conformed to the GSMA recommendations than mobile money services. It is important to note that the GSMA is a consortium of mobile phone carriers, and banks are not members. However, many mobile money services are operated by carriers that *are* members of this organization. This means that US banks have a significantly higher rate of adherence to a standard that they are *not party to* than an industry that has agreed to implement the standard.

(GSMA) Purpose and Use: The *purpose of data collection* information is critical to users. While every bank privacy policy indicated the purpose of data collection, only 19 mobile money services, or 63% of services that have any privacy policy, indicate *why* data is actually being collected. The remaining services give *no indication* as to the purpose of data collection.

(GSMA) Children and Adolescents: The GSMA Principles recommend that any service intended for use by children have special policies for the data collected by child users. We believe that mobile money services operate in a “gray area” in this respect. Mobile money services are not intentionally marketed for children, but

where mobile money services are commonly used, children will likely use these services. We note that there is very limited consideration of children’s privacy amongst mobile money service policies, and it is only mentioned in 5 mobile money policies, in contrast to 27 bank policies. However, in both cases a substantial number of policies make no mention of children (83.33% of mobile money service policies and 46% of bank policies, respectively). We believe both mobile money services and US banks should consider this issue more seriously.

(GSMA) Accountability and Enforcement: GSMA principles charge employees with a duty to maintain data privacy according to the the privacy policy. However, only 8 US banks and 3 mobile money privacy policies have any mention of the obligations of employees. We note that many policies may not explicitly discuss this principle, presuming employees will be responsible for implementing published policies.

(FDIC) Collection Process: The FDIC recommends that financial services disclose what personal data is collected. While mobile money services tended to at least mention this principle at a higher rate than other principles (24 services, or 80% of available policies), they still fall short of the 96% coverage rate of US banks.

(FDIC) Definitions and Examples: *Definitions* and *examples* are key components of privacy policies because they give the user a clear understanding of the terms used in the policy and the specific information that will be used throughout their interaction with the bank/service. In the most significant quantitative difference seen between the two groups of policies, almost all bank policies provided definitions of the data (47 policies) that would be collected from users and gave examples of its usage (48 policies). In contrast, only 8 mobile money service policies defined what type of data would be collected and only 14 policies gave examples of its usage. Even though policies may technically inform users of the data being collected, they can be obfuscated such that the data collected and shared is difficult to define. *We find the majority of mobile money services with a privacy policy fail to identify to their users what data is actually being collected or stored.*

(FDIC) Third Parties and (Both) Data Sharing Practices: Notices of third party data sharing practices are another critically important aspect of privacy policies. Our measurement of principles distinguishes between whether third party interactions are discussed (“Third Parties”) and whether there are additional details about what is being shared with third parties and why (“Sharing Process”). We find that 24 mobile money services (80% of those with policies) address third parties in their policies, and this is actually at a rate comparable to the 41 US banks (82%). However, when it comes to details of the sharing process, there is a significant disparity between our two populations. All US banks discuss this issue, compared to only 21 mobile money services (70% of available policies). This dispar-

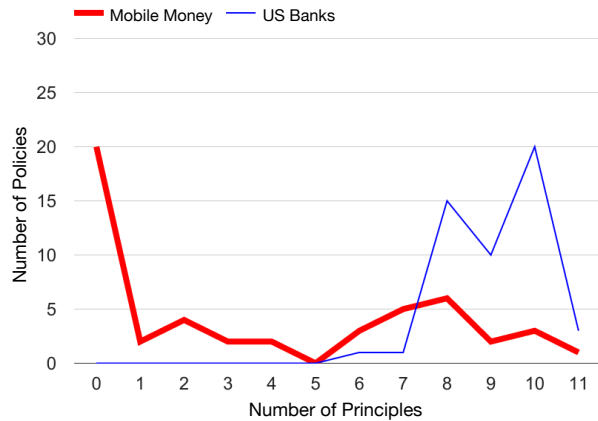


Figure 4: The total number of principles covered by banks and mobile money services. While the US banks meet most of the FDIC and GSMA principles, the mobile money industry falls far short of these standards.

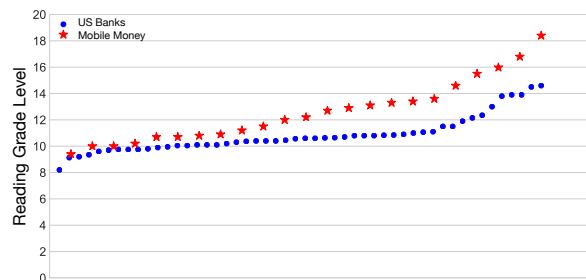


Figure 5: Reading Grade Level scores of U.S. banks and Mobile Money services.

ity is troubling, as sharing of data with unaffiliated third parties is a serious concern for customers.

(Both) User Choice and Control: While nearly every US bank (49, or 98%) provided information about a user’s ability to opt out of data collection sharing, only 23 mobile money services (77%) offered information about a user’s options to control the use of their data. We note that the United States defines a right of a customer to limit certain types of sharing, and this may explain why US banks discuss this at a greater rate. Nevertheless, this principle is present in both GSMA and FDIC recommendations, so mobile money services should improve their discussion of this issue.

(Both) Security: Both the GSMA and the FDIC recommend that services provide information about the security mechanisms used to protect the collected personal information. Nearly every US bank studied offers this information in a privacy policy (49 policies, or 98%). In addition, 26 of the mobile money services (87%) mention data security in some form. It is important to note that in this study we are simply evaluating whether policies discuss security. Given the substantial difficulty in ensuring data security, any security claims must be subject to healthy skepticism [30, 31].

(Both) Data Minimization and Retention: The final principle we measure is whether policies mention a data minimization policy or a data retention policy. We find that many US banks and mobile money services do not cover this. Only 32 US banks (64%) feature policies that cover this principle, and an even smaller number — 12 mobile money services (40%) — discuss this principle. Given the pervasiveness of data breaches, more banks and mobile money services need to adhere to good data minimization and retention policies and inform their customers of these practices.

Aggregate Analysis: With our analysis of each of the individual principles complete, we are now able to judge the overall state of the two markets that we study.

Figure 4 demonstrates the distribution of overall coverage of privacy policies defined by banks and mobile money services in the form of a histogram. All bank policies have at least 6 principles covered, and 20 banks cover exactly 10 principles. By contrast, mobile money policies tend to be far less complete than US banking policies, and it is clear that in absolute terms too many mobile money services do not have privacy policies that adhere to well-established best practices.

5.3 Readability

Our next goal was to characterize the readability of privacy policies. As discussed in Section 4.4, we use a series of grade-level estimation techniques from the linguistics community to score each policy. Of the 30 mobile money services that had privacy policies, 23 of these were originally written in English. Because different languages have different characteristics in terms of sentence structure and verbosity, to ensure that our results were consistent, we only calculated the readability scores of those 23 policies.

Figure 5 shows our results. US Banks scored an average grade-level readability score of 10.8 ($\sigma^2 = 1.9$), and had a range of between 8.2 (Northern Trust) and 14.6 (Deutsche Bank). Mobile money services had a higher mean reading level of 12.1 with much greater variance ($\sigma^2 = 5.3$), and a range of 9.4 (UseBoom) to 18.4 (Indosat).

To determine if the differences in scores in these two populations are statistically significant, we performed a two-tailed Mann-Whitney-U test. We selected this test over a traditional t-test because it does not assume that the populations are normally distributed. Our null hypothesis was that there is no difference between the readability of the mobile money and traditional banking policies. We selected a significance threshold $\alpha = 0.001$. We note that we chose this extremely conservative threshold to control for the fact that our two datasets differed in variance. The analysis resulted in a z-score of -3.29525 with a corresponding p-value of 0.00096, which is below our conservative threshold of significance. We also calculated an effect size of $r = 0.39$, which represents between a medium (0.3) and large (0.5) effect size [12]. Therefore, the null hypothesis is rejected and there is a statistically significant differ-

ence between the readability of privacy policies of mobile money services and U.S. banks. The implication of this analysis is that mobile money policies, on average, appear to be more difficult to comprehend than their traditional banking counterparts.

To further understand the difference between these two sets, we then characterized policy lengths. US Banks had a mean count of 1492 words ($\sigma^2 = 660.7$). State Street’s policy had the highest word count (3494), while First Merit was the lowest (557). In general, policies with greater word counts tended to have lower readability scores. Surprisingly, mobile money services had a slightly shorter mean length of 1374 words but with dramatically higher variance ($\sigma^2 = 1373.2$). These results can be better explained by looking at specific data points. Suvidhaa, for instance, had the greatest word count (5518), while EcoCash had the shortest (68). EcoCash is not alone in writing an extremely short policy; TigoPesa’s policy is only 268 words long. Figures 8 and 9 show the entirety of these two short policies.

We again sought to determine if our observations were statistically significant. Accordingly, we performed a two-tailed Mann-Whitney-U analysis on the word count results. For that analysis, we again set $\alpha = 0.001$ to control for the increased likelihood of a Type-1 error given the differences in variance of the datasets. Our null hypothesis was that there was no difference in the length of the privacy policies for the mobile money services and US Banks. The analysis yields a z-score of 7.08221 with p-value less than 0.00001. Moreover, with a large calculated effect size of $r = 0.83$, we determined that our results were indeed statistically significant and we could reject the null hypothesis. This implies that length of privacy policies for mobile money services differs significantly from those of traditional banks.

As a final measure of readability, we plotted our measured word counts against the grade-level estimations. Figure 6 shows our results, and includes two important trendlines. While both mobile money and US Banks see the grade-level requirement to understand their policies increase as the word count increases, mobile money services experience this trend in a greatly accelerated fashion. Second, while the privacy community has generally advocated for shorter policies in the past, our readability and coverage analyses demonstrate that shorter policies alone are not necessarily “better.” Counterintuitively, mobile money services tend to have short policies that are harder to read.

5.4 Language

In our final analysis, our goal is to determine whether the privacy policies supplied by banks and mobile money services are available in popular or official languages in the countries where they operate. This is a more general question of whether these policies are actually readable by the population for whom they are designed to serve, also noted by [44]. For example, a low-grade level policy written in English is still not readable to a customer who only speaks French. The question of language availability is critical since the principles expressed by these

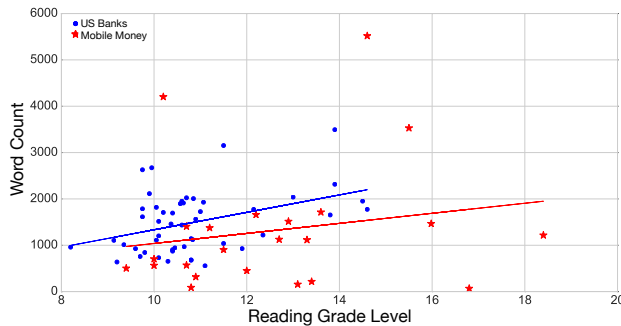


Figure 6: Reading grade level vs. word count of U.S. bank policies and mobile money policies. Note that mobile money policies tend to be shorter and yet more difficult to read.

policies become meaningless if the population of customers is unable to read them.

For US banks, every privacy policy that we examined was available in English. While the United States does not have an official language, English is by far the most popular language of communication, with over 230 million people primarily speaking it at home, while Spanish is the second-most popular language spoken in the country [35]. US banks fall short in addressing the needs of these customers as only 13 of the 50 (or 25%) of financial institutions we reviewed listed privacy policies in Spanish on their website. Furthermore, Spanish-speaking customers would likely have difficulty even accessing this information from these websites, as only two institutions, Fifth Third and East West (4% of the total) allowed users to view the entire website in Spanish.

While US banks could make greater efforts to make their privacy policies accessible to speakers of other languages, the challenges faced in providing policies in readable languages in the US pale in comparison to those presented in the mobile money space. As discussed earlier in this section, only 30 of the 54 mobile money services that we examined had any privacy policies at all. We used the CIA World Factbook [6] to determine the most widely-spoken languages in the countries of operation for these services. Many of the countries where these mobile money services are deployed have more than one official or commonly spoken language, making the question of language accessibility even more important.

Figure 7 shows the extent of these language accessibility challenges for mobile money services. We found that of the 30 services with policies, only 20 were available in either the first or second most widely-spoken language of the service’s native country, with 16 policies available in the most widely-spoken language and 6 available in the second-most widely-spoken language. This means that 10 of the 30 mobile money services with any sort of privacy policy, or 33% of this group, *do not have policies written in languages readable by speakers of the most widely-used languages in their countries*. These populations are disempowered from learning about their pri-

vacy rights because of this lack of language accessibility.

We also found that only 13 mobile money service websites (or 43% of the services with a privacy policy) were available in either the first or second-most widely spoken language within that country.

These issues represent a serious impediment to inclusion and privacy. The lack of accessible material results in the inability for large segments of the population to be able to make informed choices regarding their privacy. It is imperative that customers have the opportunity to understand their rights and options for controlling their personal data, and there can be no meaningful ability to do so unless customers are provided materials comprehensible to them in the languages they use.

5.5 Mobile Payment Apps

Our previous results showed a clear difference between privacy policies in US Banks and mobile money systems. We were also interested to know if popular mobile payment apps from developed countries performed well according to our criteria of coverage, readability, and language availability. To that end, we look at the two most popular mobile payment apps in the US: Paypal and Venmo. We found that policies covered all 11 principles with only a few exceptions: Paypal had no coverage of children’s policy, while Venmo did not cover data minimization or retention. Neither policy covered employee accountability or enforcement. Venmo’s average reading grade level was 13.2, while Paypal scored higher at 14.9. In addition, Paypal’s word count of 3,239 was over 1000 more words than Venmo’s policy (2,065 words). Although both mobile payment apps are used widely across the US, we were unable to find a privacy policy in any other language that English. We note that our sample size of 2 apps means meaningful statistical analysis is simply not possible. However, these results are similar to our findings for US banks.

6. IMPROVING MOBILE MONEY PRIVACY DISCLOSURES

Our results show that the mobile money industry, as a whole, does not provide sufficient disclosure of privacy practices. The question then is how can we improve the state of privacy disclosure in mobile money? In this subsection, we discuss the role that regulation by national governments as well as industry-driven “self-regulation” may play in improving this state of affairs. We also discuss what future improvements to mobile money privacy policy recommendations should entail. We note that while we strongly believe improvement is imperative for mobile money privacy disclosures and privacy practices, we do not take a strong stance on which path is best. Finally, we conclude by acknowledging that norms for privacy vary from culture to culture.

6.1 Regulating Mobile Money Policies

One possible path to improving mobile money privacy policies is legal regulations in the spirit of the Gramm-Leach-Bliley Act (GLBA) in the United States. Prior work by Sheng and Cranor [37] showed that the GLBA significantly improved the coverage of privacy disclo-

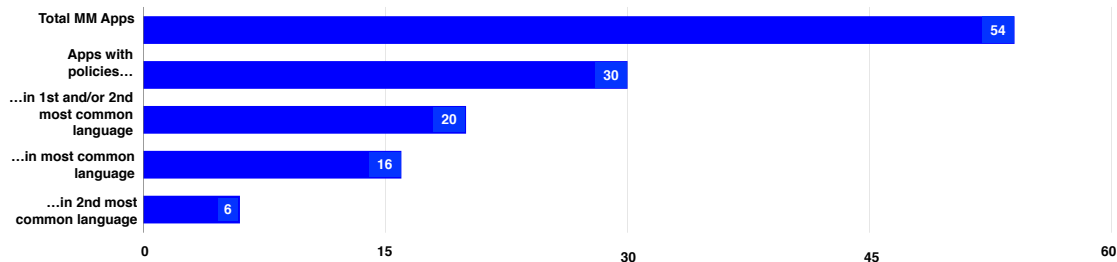


Figure 7: Language analysis of Mobile Money service policies. Note that 18% of all services (54) and 33% of services that actually have privacy policies (30) are neither available in the first or second official languages of the country in which they are deployed.

asures in the US. The data that we present on US policies confirms this earlier finding: US policies are largely complete according to the FDIC standards. We do note, however, that regulation is not a panacea. For example, some US policies lacked coverage of important information. More importantly, regulations about *disclosure* do not necessarily minimize data collection or mean that users have meaningful options about that collection [37].

We note that we are among the first to look at privacy policies from an international perspective. This comes with a number of difficulties. For example, each country will have its own laws, regulations, and local operating practices. In mobile money this is complicated by the fact that these services can be regulated by many (sometimes overlapping) agencies. These agencies include financial regulators, telecommunications regulators, or others [41]. In future work we hope to partner with experts in law in various countries served by mobile money to determine what, if any existing laws or regulations could apply to mobile money, and how effective those mechanisms are. As a case study example of the role of regulation, we examined India’s privacy regulations for all businesses (not specific to mobile finance) as well as the performance of mobile money systems based in India. These regulations are specified in a regulation document published by the Ministry of Communications and Information Technology titled the “Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.” [27] This document mandates that organizations subject to the IT Amendment Act of 2008 must provide privacy notices to users. The regulation also mandates that those notices contain information mapping to four of our analysis principles: “Purpose and Use,” “Examples,” “Security,” and “Sharing Process.” We note that the governing regulations for mobile banking by the Reserve Bank of India make no mention of privacy practices [34].

We found that all India-based systems we studied had privacy policies. More importantly we found that their coverage was among the best of mobile money systems that had a policy. All discussed the data collection pur-

pose, what data is collected, definitions of terms, third party sharing, users’ options for data practices, concrete examples of types of data, data security, and data retention and minimization policies. Three out of four apps discussed specific third-party data sharing practices, and one service (Oxigen Wallet) discussed employee accountability. No Indian services specifically addressed children’s data privacy. In total, Indian services had a higher percentage coverage of every privacy policy principle than mobile money systems from all other countries (with the exception of children’s data privacy); they also met the criteria required by the IT law. This small case study does not causally prove that regulation leads to better policies, but it does motivate further exploration of this idea.

Change in mobile money as a result of national regulations will likely take time, and this is complicated by several factors. For example, it is not always clear which entity in a country is responsible for setting and enforcing policy related to mobile money. Because this industry does not fall under the same regulatory environment as traditional banking, authority is often scattered across multiple parts of a government (e.g., the telecommunications bureau, the central bank, etc.) [41]. Government-enforced regulations may be made easier through the upcoming creation of transnational unions such as the Economic Community of West African States (ECOWAS), which plans to share a single currency and set of policies among its 15 member nations by 2020 [14].

Another route to improve privacy disclosures in mobile money would be through “self-regulation” through an industry consortium like the GSMA, whose recommendations we use in this paper [43]. Advocates of this approach argue that those within the industry are best equipped to determine what users need and balance it with the needs of that industry. Such “self-regulation” may not provide the same enforceable guarantees as government-enforced regulations. In particular, industry groups must strike a balance between representing their member companies’ interests and in requiring said companies to change their practices. “Self-regulation” does have some advantages though. For example, in-

dustry associations can deploy recommendations faster than is typically possible for governments, and it can standardize these recommendations internationally. We note that industry-based guidance is not necessarily mutually exclusive of national regulation.

6.2 Recommendations for Privacy Policy Standards

Orthogonal to the question of how to induce change in mobile money services is specifying “in what ways should these policies change.”

Expanding Policy Coverage: We believe that the GSMA standards are a minimal starting point, but recognize they are deficient in a number of ways. First, they are woefully underspecified. The principal document defining them could be characterized as an “infographic.” Second, the coverage should be expanded to cover additional areas of concern. These include the areas of coverage in the FDIC standards: describing the collection process, providing definitions of important terms, providing clear, concrete examples of how data will be used, and how data will be shared with third parties. As we discussed earlier, we note that the FDIC standards are not necessarily ideal, but they provide a strong starting point for determining a complete privacy policy. Other standards and guidelines from governments or consumer protection organizations — including established privacy policy templates and generating tools [2–4] — may also be instructive for future mobile money privacy policy standards.

Expanding User Comprehension: Finally, we note that for privacy policies to have value, users must be able to understand how their privacy is affected by using these services so they can make informed decisions. As our analysis demonstrates, privacy policies for these services often lack content and are written in ways that impair readability. In many cases, significant populations cannot make decisions as policies are not written in languages they understand. It is therefore vital that these policies are not only complete, but written in ways that allow users to understand how their data is used.

This issue is further amplified by literacy rates that can vary widely between countries. For example, Qatar’s literacy rate is over 97% while the literacy rate in Mali is less than 47% [6]. However, none of the privacy policies that we examined considered how to effectively communicate policy details to illiterate customers. In countries where literacy rates are low, it is important to consider new ways of making mobile money customers aware of their privacy rights.

6.3 Cultural Norms for Privacy

Deciding how privacy should be protected across a set of services that span a wide array of cultures and continents was not a simple task. In many parts of the world, especially Europe, privacy is carefully guarded and assumed to be a human right. Chinese culture, however, instead often values privacy less when compared to community, order and governance [24]. Similarly, in

settings where sharing or communal ownership (e.g., of cell phones) are common, there are different standards for individual privacy [29].

Accordingly, our selection of the GSMA policies was made only after careful consideration. In addition, the GSMA claims to be the embodiment international understanding on privacy. Instead of attempting to pick a universal set of values for privacy across mobile money services, we felt that the best available consensus on the matter likely comes from the industry itself. That is not to say that the protections provided by the GSMA, FDIC or any currently available policy are perfect. Rather, they form the only available lenses through which we can observe the current state of global privacy expectations in the digital financial services space.

We believe that significant work remains to be done in this space. As efforts towards interoperable services increase [33], questions about which country’s privacy rules dominate in cross-border transactions remain unanswered. Moreover, methods of communicating such policies to users whose cultural frame of reference and literacy may vary widely will also prove challenging.

7. CONCLUSION

Mobile money services provide new abilities for customers to use their mobile phones to make payments, significantly broadening financial inclusion and helping to raise people out of poverty. However, the privacy guarantees of these services has remained unexplored. We conducted a comprehensive analysis on privacy policies of all 54 mobile money services that provided smartphone apps, and compared these policies to the top 50 US banks by assets. We found that although all US banks had privacy policies, over 44% of mobile money services had no privacy policy whatsoever. For those services that did have policies, most were missing key factors, including privacy principles laid out by industry groups that these services agreed to uphold. Moreover, compared to bank policies, mobile money policies were hampered by being difficult to read, even though they were on average significantly shorter. Several mobile money services did not even offer policies written in the languages used by a majorities of their target population. Our study represents a call to action for operators, governments, and NGOs, to assure that agreed-upon principles and policies are enforced, expanded upon, and made accessible to the customers of these services in order to better protect their privacy.

Acknowledgments

We thank Jami Solli for her insights. We also thank Blase Ur, Matthew Smith, and the anonymous reviewers of our work for their valuable comments. This work was supported in part by the National Science Foundation under grant numbers CNS-1526718, and CNS-1540217. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

8. REFERENCES

- [1] Ecocash - android apps on google play. <https://play.google.com/store/apps/details?id=com.econet.ecocash>.
- [2] FreePrivacyPolicy.com.
- [3] PrivacyPolicies.com.
- [4] Final Model Privacy Form Under the Gramm-Leach-Bliley Act - 16 CFR Part 313. <http://bit.ly/1cQG1ya>, December 2009.
- [5] Federal Reserve Statistical Release: Large Commercial Banks. <https://www.federalreserve.gov/releases/lbr/current/>, September 2016.
- [6] The CIA World Factbook. <https://www.cia.gov/library/publications/the-world-factbook/geos/>, January 2017.
- [7] Asli Demirguc-Kunt, Leora Klapper, Dorothea Singer, and Peter Van Oudheusden. The Global Findex Database 2014 Measuring Financial Inclusion around the World. Technical Report Policy Research Working Paper 7255, World Bank Group, April 2015.
- [8] S. Badarudeen and S. Sabharwal. Assessing Readability of Patient Education Materials: Current Role in Orthopaedics. *Clinical Orthopaedics and Related Research*, 468(10):2572–2580, October 2010.
- [9] E. Beaunoyer, M. Arsenault, A. M. Lomanowska, and M. J. Guitton. Understanding online health information: Evaluation, tools, and strategies. *Patient Education and Counseling*, 100(2):183 – 189, 2017.
- [10] K. Butler, L. Perlman, P. Makin, H. Gerwitz, P. Traynor, Y. Grin, E. Bondarenko, and R. Miller. ITU-T Focus Group Digital Financial Services: Security Aspects of Digital Financial Services (DFS). Technical report, International Telecommunications Union Standardization Sector (ITU-T), December 2016.
- [11] S. Castle, F. Pervaiz, G. Weld, F. Roesner, and R. Anderson. Let’s Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. In *7th ACM Symposium on Computing for Development (DEV)*, November 2016.
- [12] J. Cohen. A Power Primer. *Psychological Bulletin*, (1):155–159, July 1992.
- [13] L. F. Cranor, P. G. Leon, and B. Ur. A Large-Scale Evaluation of U.S. Financial Institutions’ Standardized Privacy Notices. *ACM Trans. Web*, 10(3):17:1–17:33, August 2016.
- [14] Economic Community of West African States (ECOWAS). ECOWAS VISION 2020: Towards A Democratic And Prosperous Community. <http://www.ecowas.int/wp-content/uploads/2015/01/ECOWAS-VISION-2020.pdf>, 2010.
- [15] J. A. Eloy, S. Li, K. Kasabwala, N. Agarwal, D. R. Hansberry, S. Baredes, and M. Setzen. Readability assessment of patient education materials on major otolaryngology association websites. *Otolaryngology – Head and Neck Surgery*, 147(5):848–854, 2012.
- [16] Federal Deposit Insurance Corporation. Privacy Rule Handbook. <https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/>, 2001.
- [17] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal. How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 321–340, Denver, CO, June 2016. USENIX Association.
- [18] MMU Deployment Tracker. <http://www.gsma.com/mobilefordevelopment/programmes/mobile-money-for-the-unbanked/insights/tracker>, November 2016.
- [19] M. Hochhauser. Lost in the Fine Print: Readability of Financial Privacy Notices. <https://www.privacyrights.org/blog/lost-fine-print-readability-financial-privacy-notice-hochhauser>, July 2001.
- [20] C. Jensen and C. Potts. Privacy Policies As Decision-making Tools: An Evaluation of Online Privacy Notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, April 2004.
- [21] M. Johnson, J. Karat, C.-M. Karat, and K. Grueneberg. Optimizing a Policy Authoring Framework for Security and Privacy Policies. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, July 2010.
- [22] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A “Nutrition Label” for Privacy. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, July 2009.
- [23] J. R. Landis and G. G. Koch. The measurement of observer agreement for categorical data. *Biometrics*, 33(1):159–174, 1977.
- [24] T. Li and Z. Zhou. Do You Care About Chinese Privacy Law? Well, You Should. <https://iapp.org/news/a/do-you-care-about-chinese-privacy-law-well-you-should/>, January 2015.
- [25] A. M. McDonald and L. F. Cranor. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3):540–565, 2008.
- [26] C. Mims. 31% of Kenya’s GDP is Spent Through Mobile Phones. <http://qz.com/57504/31-of-kenyas-gdp-is-spent-through-mobile-phones/>, February 2013.
- [27] Ministry of Communications and Information Technology of India. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. <http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>, 2011.
- [28] M. Paik. Stragglers of the Herd Get Eaten: Security Concerns for GSM Mobile Banking

- Applications. In *Proceedings of the Workshop on Mobile Computer Systems and Applications (HotMobile)*. ACM, February 2010.
- [29] J. Poushter, J. Bell, D. Cuddington, K. Devlin, M. Keegan, B. Parker, K. S. B. Stokes, R. Wike, and H. Zainulbhai. Cell Phones in Africa: Communication Lifeline Texting Most Common Activity, but Mobile Money Popular in Several Countries. Technical report, Pew Research Center, April 2015.
- [30] B. Reaves, J. Bowers, N. Scaife, A. Bates, A. Bharatiya, P. Traynor, and K. Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. *ACM Transactions on Privacy and Security (TOPS)*, 2017.
- [31] B. Reaves, N. Scaife, A. Bates, P. Traynor, and K. Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, August 2015.
- [32] R. W. Reeder, C.-M. Karat, J. Karat, and C. Brodie. Usability Challenges in Security and Privacy Policy-authoring Interfaces. In *Proceedings of the International Conference on Human-computer Interaction*, September 2007.
- [33] D. G. Reiss and R. T. L. Mourao. The Regulator’s Perspective on the Right Timing for Inducing Interoperability - Findings of a survey among Focus Group Members. Technical report, International Telecommunications Union Standardization Sector (ITU-T), February 2017.
- [34] Reserve Bank of India. Master Circular - KYC norms, AML standards, CFT, Obligation of banks under PMLA, 2002. <http://rbidocs.rbi.org.in/rdocs/notification/PDFs/94CF010713FL.pdf>, 2013.
- [35] C. Ryan. Language Use in the United States: 2011 – American Community Survey Reports. United States Census Bureau. <https://www.census.gov/prod/2013pubs/acs-22.pdf>, August 2013.
- [36] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. A Design Space for Effective Privacy Notices. In *Symposium On Usable Privacy and Security (SOUPS)*, July 2015.
- [37] X. Sheng and L. F. Cranor. Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies. *ISJLP*, 2:943, 2005.
- [38] W. Shepard. After Day 50: The Results From India’s Demonetization Campaign Are In. <https://www.forbes.com/sites/wadeshepard/2017/01/03/after-day-50-the-results-from-indias-demonetization-campaign-are-in/>, January 2017.
- [39] T. Suri and W. Jack. The Long-Run Poverty and Gender Impacts of Mobile mMoney. *Science*, 354(6317):1288–1292, December 2016.
- [40] P. F. Svider, N. Agarwal, O. J. Choudhry, A. F. Hajart, S. Baredes, J. K. Liu, and J. A. Eloy. Readability assessment of online patient education materials from academic otolaryngology – head and neck surgery departments. *American Journal of Otolaryngology*, 34(1):31 – 35, 2013.
- [41] N. A. Tagoe. Who Regulates the Mobile Money Operations by Telco’s? The Need for an Effective and Robust Legislative and Regulatory Framework in Ghana. *Journal of Business and Financial Affairs*, 5(3), August 2016.
- [42] The GSM Association (GSMA). Code of Conduct for Mobile Money Providers, Version 2. <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/10/Code-of-Conduct-for-Mobile-Money-Providers-V2.pdf>, 2015.
- [43] The GSM Association (GSMA). Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem. http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf, 2016.
- [44] B. Ur, M. Sleeper, and L. F. Cranor. {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.
- [45] US Congress. Gramm-Leach-Bliley Act, Financial Privacy Rule. <https://www.gpo.gov/fdsys/pkg/PLAW-106pub1102/content-detail.html>, November 1999.
- [46] S. Zimmeck and S. M. Bellovin. Privee: An Architecture for Automatically Analyzing Web Privacy Policies. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 1–16, San Diego, CA, August 2014. USENIX Association.

APPENDIX

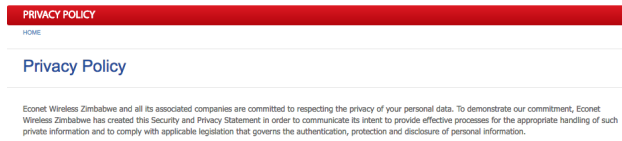


Figure 8: EcoCash, which has endorsed the GSMA's Code of Conduct, has a very short (68 word) privacy policy. In its current state, it only meets one of the GSMA's recommendations.

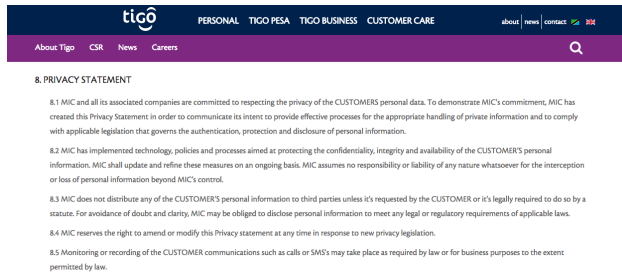


Figure 9: TigoPesa (Tanzania)'s short privacy policy (268 words) is a subsection within TigoPesa's Terms and Conditions. In its current state, it only meets one GSMA principle and one FDIC principle.

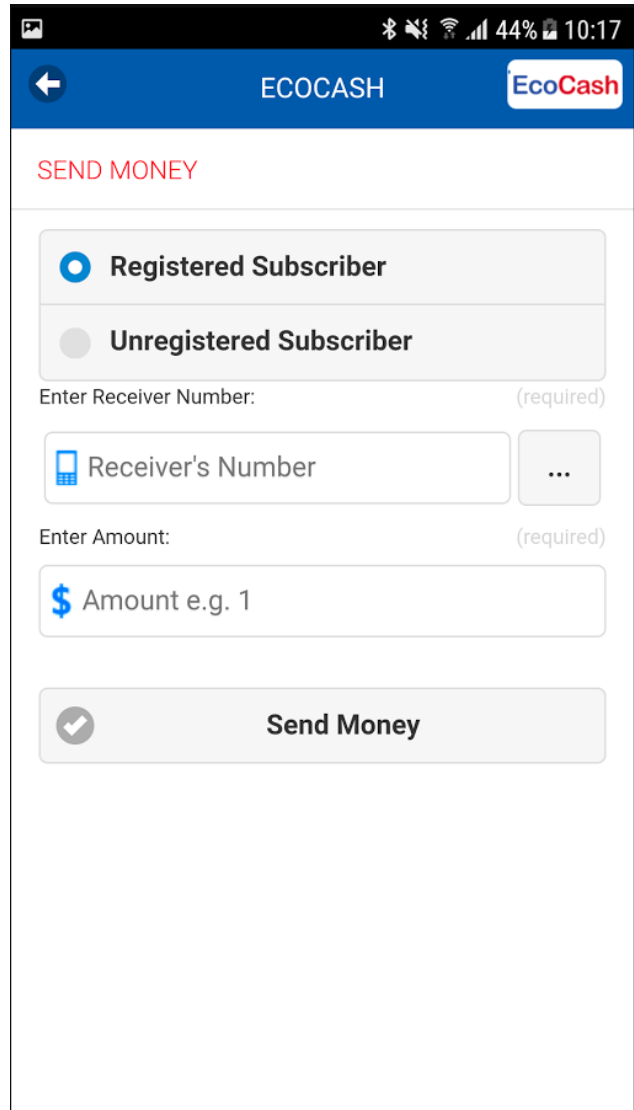


Figure 10: EcoCash mobile money application screenshot (obtained from the Google Play Store [1]).

Table 1: US Policies: Principles Included

Bank Name	GSMA			FDIC				FDIC and GSMA			
	Purpose of Data Collection	Children and Adolescents	Accountability and Enforcement	Collection Process	Definitions	Examples	Third Parties	User Choice and Control	Security	Sharing Process	Data Minimization/Retention
Ally	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Associated	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Bank of America	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Bank of NY	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Bank of West	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Bank United	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Barclays	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
BB&T	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
BBVA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
BMO	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
BOK Financial	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Capital One	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Chase	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
CIT	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Citi Bank	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Citizens	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Comerica	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Deutsche Bank	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Discover	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
EastWest	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fifth Third	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
First Citizens	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
First Merit	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
First Republic	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
First Tennessee	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Frost Bank	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Goldman Sachs	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
HSBC	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Huntington	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
JP Morgan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Key Corp	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
M&T	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Zions	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Wells Fargo	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Webster	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
US Bank	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Union Bank	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TD Bank	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Synovus	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Sun Trust	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
State Street Bank	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Silicon Valley	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Santander	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
RBC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Regions	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
PNC	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Peoples	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Northern Trust	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Morgan Stanley	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Signature	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓

Table 2: Mobile Money Policies: Principles Included

		GSMA			FDIC			FDIC and GSMA				
		Purpose of Data Collection	Children and Adolescents	Accountability and Enforcement	Collection Process	Definitions	Examples	Third Parties	User Choice and Control	Security	Sharing Process	Data Minimization/Retention
Service Name	Country											
Airtel Money	India	✓			✓	✓	✓	✓	✓	✓		✓
Bits	Uruguay				✓							
EcoCash	Zimbabwe											
eSewa	Nepal	✓			✓	✓						
EZcash	Sri Lanka	✓			✓	✓					✓	
FNB	South Africa	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
GCash	Phillipines	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
IdeaMyCash	India	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Indosat	Indoneisa	✓			✓		✓	✓	✓	✓	✓	✓
Mcash	Singapore	✓			✓		✓	✓	✓	✓	✓	✓
mCoin	Indonesia	✓			✓	✓	✓	✓	✓	✓	✓	✓
Mdinar	Tunisia											
MobiCash	Mali	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Mobile Money NG	Nigeria	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
mPay	Thailand	✓			✓			✓	✓	✓	✓	✓
Ooredoo	Qatar	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Orange Money	Côte d'Ivoire	✓			✓			✓	✓	✓	✓	✓
Oxigen	India	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Paga	Nigeria	✓		✓	✓			✓	✓	✓	✓	✓
Simba	Lebanon			✓	✓			✓	✓	✓	✓	✓
Standard Bank	South Africa	✓			✓	✓	✓	✓	✓	✓	✓	✓
Suvidhaa Money	India	✓			✓	✓	✓	✓	✓	✓	✓	✓
Teasy Mobile	Nigeria				✓			✓	✓	✓	✓	✓
Tigo Pesa	Tanzania							✓	✓	✓	✓	✓
Tigo SV	El Savador							✓	✓	✓	✓	✓
TPago	Dominican Republic					✓		✓	✓	✓	✓	✓
True Money	Thailand				✓			✓	✓	✓	✓	✓
UseBoom	Mexico	✓			✓	✓	✓	✓	✓	✓	✓	✓
Zenith	Nigeria				✓		✓	✓	✓	✓	✓	✓
Zuum	Brazil				✓			✓	✓	✓	✓	✓
No Policies Available:												
BKash	Bangladesh											
Ecash	Indonesia											
eZuza	South Africa											
First Monie	Nigeria											
Fortis Mobile Money	Nigeria											
Growth Enhancement Support Scheme	Nigeria											
JCUES Mobile Money	Jamaica											
Mi Billetera Movil	Argentina											
Mobile Money Guyana	Guyana											
MoneyOnMobile	India											
mService	Vietnam											
mVola	Madagascar											
my.wallet	Nigeria											
Myanmar Mobile Money	Myanmar											
Oi Carteira	Brazil											
Pido	Nigeria											
Pocket Moni	Nigeria											
Qash Mobile Banking	Côte d'Ivoire											
Ready Cash	Nigeria											
Splash Cash	Sierra Leone											
Tigo Honduras	Hondurus											
Tigo Money Bolivia	Bolivia											
VCash	Nigeria											
Wizzit	South Africa											

Table 3: Keywords and Phrases

Principle	Key Words and Phrases
Purpose of Data Collection	Reasoning, Enhance User Experience, User Experience
Children and Adolescents	Children, Children's Privacy
Accountability and Enforcement	Employee, Accountable, Accountability
Collection Process	Collect
Definitions	Means, Is, Are
Examples	Types of Personal Information, Types Of, For Example, Includes
Third Parties	Third Party, Third Parties
User Choice and Control	Disable, Edit, User Can, Change
Security	Security
Sharing Process	Share, Sharing Process
Data Minimization and Retention	Minimization, Termination, Continue to share, Retention, Retain