FOCUS NOTE

# IS DATA PRIVACY GOOD FOR BUSINESS?

December 2019

Maria Fernandez Vidal and David Medine

**Consultative Group to Assist the Poor**
1818 H Street, NW, MSN F3K-306
Washington, DC 20433
Internet: www.cgap.org
Email: cgap@worldbank.org
Telephone: +1 202 473 9594

Cover photo by Rokonuzzaman Khan.

## Executive Summary

As digital financial services grow rapidly, so do concerns over data privacy and protection for poor customers who are especially vulnerable to injury from lax policies. CGAP set out to test how much poor people value their privacy and whether there was a business case for financial services providers to offer poor customers data protection. The results from six experiments in Kenya and India make the case for offering poor customers products with data privacy and protection options, opening an avenue for voluntary self-regulation to protect consumers in markets that do not have strong policies in place.

We found that poor customers:

- **Value data privacy and are willing to pay for it.** In Nairobi, 64 percent of 220 customers surveyed chose a loan with a 10 percent fee and strong data privacy rather than a loan at half that rate. In Bangalore, results were similar: 66 percent of 197 customers chose the loan with strong privacy at a 10 percent rate versus one at 9 percent.
- **Will invest time in obtaining a loan that offers privacy.** In Bangalore, 82 percent of the 96 customers tested chose to wait 30 minutes for a loan that provided privacy protections versus 10 minutes to get a loan with no guarantees.
- **Are least willing to share data with third parties.** In Kenya, only 40 percent of 208 customers were willing to permit the sale of their financial data to parties other than their financial provider.

For **providers**, the findings suggest that offering products that have strong data privacy and protections built in could give them an edge in a competitive marketplace, which in turn could promote a voluntary, self-regulatory environment especially in low-capacity countries.

For **policy makers**, evidence that customers do care about data privacy and protection strengthens the case for providing regulatory oversight over use of data generated by financial transactions.

## Adopting Better Data Privacy Policies

As digital financial services grow, so do the digitized financial data trails of customers. This makes it increasingly important to look at how data are protected. One of the necessary enablers of financial inclusion is that customers, and specifically poor and traditionally excluded customers, trust the financial products offered to them. Financial inclusion efforts can be impaired if poor people suffer injury from bad data privacy policies.

One of CGAP's goals is to promote voluntary adoption of better data privacy policies that can protect and build consumer trust. To test the premise behind this goal, we conducted a series of research experiments to see if privacy could be good business for financial services providers. Many markets lack strong data protection regulation, and where these laws do exist, supervisors have limited capacity. As such, we looked at self-regulation and voluntary adoption of stronger data protection policies as a viable option for privacy

improvements, at least in the short term. Even in countries that have no or insufficient data protection through regulation and supervision, if providers see the business value in offering good privacy, they may be more willing to adopt better data privacy policies.

Studies comparing people's views and behaviors around privacy have been conducted mostly in developed markets, and they often point to what is referred to as the privacy paradox: an expressed concern about privacy does not translate into behavior. For example, a recent study conducted with MIT undergraduate students found that even students who said that they cared deeply about privacy and would not give away sensitive data were willing to do so in exchange for a slice of pizza.[1]

CGAP conducted a series of customer research exercises with low-income customers in India and Kenya to better understand customer behavior in different data privacy and protection settings.[2] The research focused on how customers behave (i.e., would they take a loan) rather than on their beliefs about privacy.

## Do Poor People Want Data Privacy?

**People prefer privacy, if they have a choice.** We used two approaches to assess how much people cared about privacy. The first was providing loans at differing interest rates depending on the privacy features offered, with more privacy resulting in a higher cost. In each case, the total amount to be repaid was shown to the customers to make sure they understood the additional cost if they chose a higher-interest loan. The second approach focused on time instead of money, with a privacy-protected product requiring additional wait time. When presented with a choice between products, we found that the majority of people preferred the one with better data privacy features and were willing to pay more or spend more time for it.

## Are They Willing to Pay for It?

**The majority of low-income customers were willing to pay more for privacy.** In Kenya, we offered 198 customers from low-income areas around Nairobi (Kibera and Kawangware) three loan options. The fees were selected so that the middle option had the

1 Susan Athey, Christian Catalini, and Catherine Tucker, "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk" (Cambridge: NBER, 2017). The same study also tested which bitcoin wallet students chose for their payment for participating in the experiment. They could choose from a variety of wallets, some of which protected their privacy, some of which didn't. The biggest predictor of what wallet they chose was not their privacy practices but how far they had to scroll down on the page to choose a wallet.

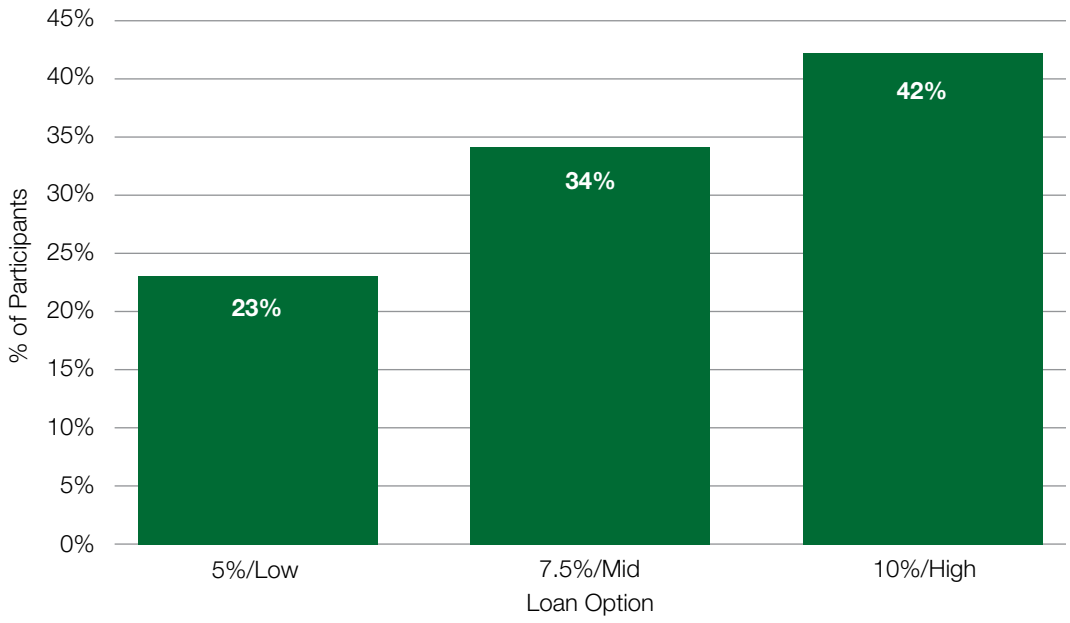
2 CGAP research partners in India and Kenya were Pensaar Design and Busara Center for Behavioral Research, respectively.

same fees as the M-Shwari product, which is the most popular digital loan product in the market. The three products had the following characteristics:

1. High data privacy and a 10 percent fee for a 30-day loan. The provider had no access to personal phone data.
2. Medium data privacy and a 7.5 percent fee for a 30-day loan. The provider would be able to access personal information only at the time of issuing the loan and would not be able to access more information after that. The provider would not share the information with third parties.
3. Low data privacy and a 5 percent fee for a 30-day loan. The provider would be able to see personal information every day until the loan had been repaid. The provider might share the information with business partners, such as a bank.

As Figure 1 shows, only 23 percent of people chose the low-privacy option, and the high-privacy loan was the most popular, even at double the cost.

FIGURE 1. **Participants' choice of loan options**




We validated this preference with a different sample of 220 customers of similar characteristics from the same area in Nairobi. In this test we offered only the following two options:

1. A loan with strong data privacy (no access to personal data) and a 10 percent fee.
2. A loan with the provider getting complete access to data and a 5 percent fee.

Again, we saw that the majority of customers preferred the more expensive loan that provided better data protection. See Figure 2.

To validate our results in a different country and cultural context, we tested this with 197 low-income customers in and around Bangalore City in India. In this case, customers were presented with a pamphlet with two loan options for microfinance loans as seen in Figure 3.

FIGURE 2. **Participants' choice of loan options**

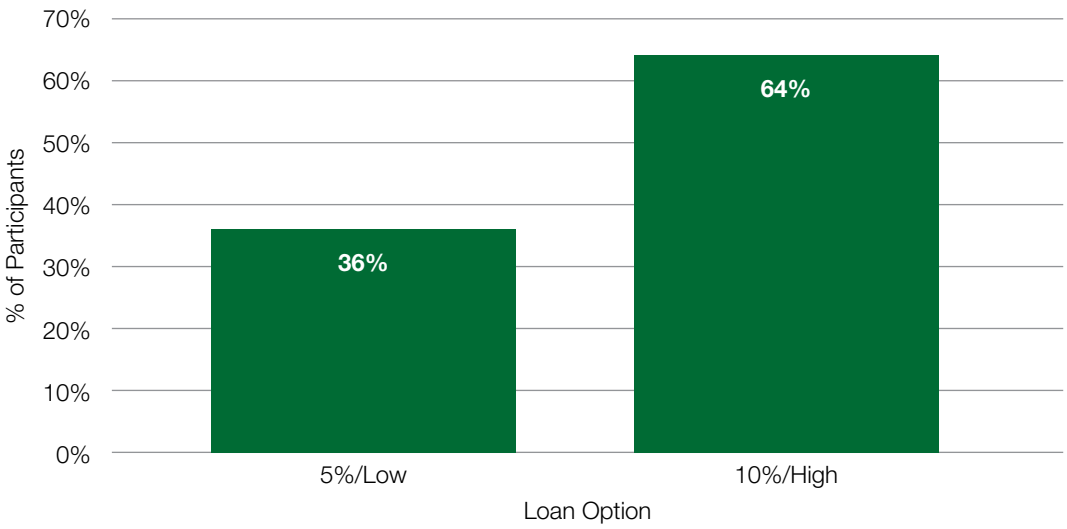
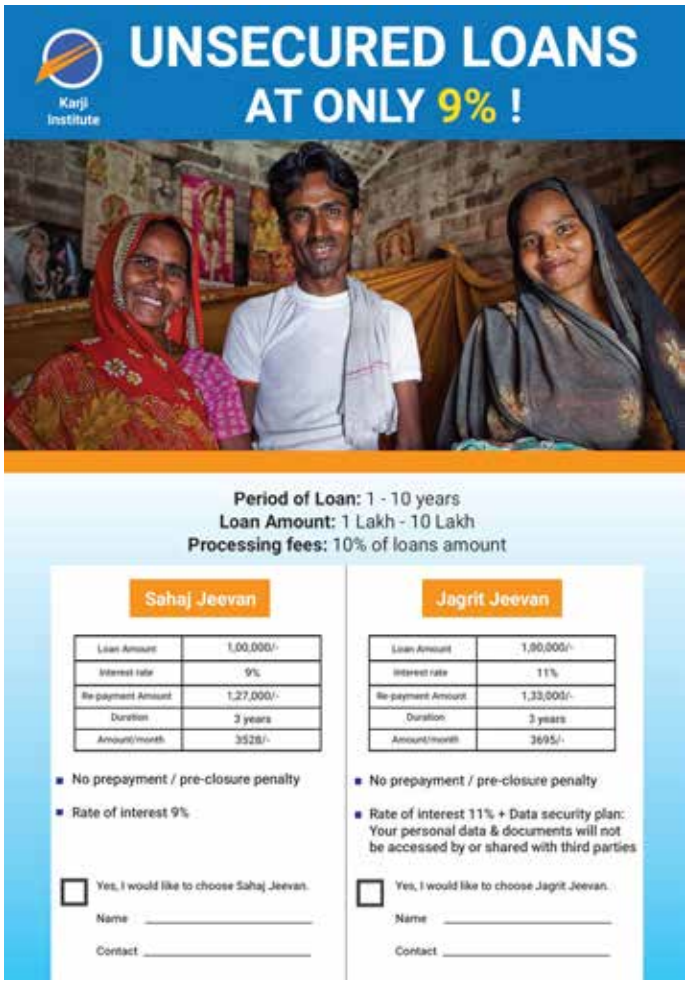



FIGURE 3. **Brochures used in the study**

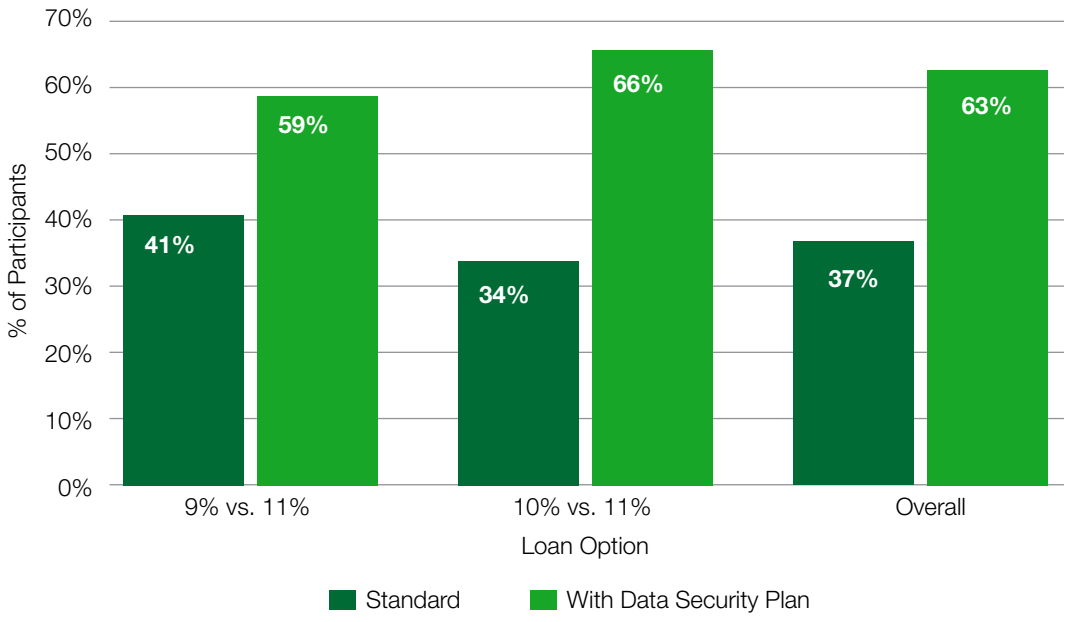




Although customers in Kenya are very familiar with short-term digital credit, in India this demographic is more familiar with microfinance loans and in-person interactions. Therefore, we designed the experiment to mimic what their real loan interactions would most likely be. We tested both 9 percent versus 10 percent interest and 9 percent versus 11 percent interest on three-year loans.

Overall, 63 percent of customers chose to apply for the more expensive product, which stated that their personal data would not be shared with third parties. Even in a low-income context, where the additional monthly payment can be a burden, we didn't find a strong price sensitivity when comparing results for the group that was offered a 1 percent interest difference versus a 2 percent interest difference. The more expensive option was selected in 66 percent and 59 percent of the cases, respectively. See Figure 4. We conducted exit interviews with participants to better understand the reasons for their choice. The most common reasons stated for not choosing the privacy protected product were the inability to verify that their data were in fact being better protected and their belief that the provider should protect their data anyway. Low valuation of data privacy did not appear to be a predominant reason.

FIGURE 4. **Participants' choice of loan options**




## Are They Willing to Wait for It?

**Customers are willing to wait longer for a product that has stronger privacy features.** A second approach to measuring people's interest in data protection was to see if they would be willing to invest their time to get protection. In this experiment, conducted in Bangalore, people were told that after applying for the loan, they could request that their data be deleted to ensure the data would not get lost or stolen but they would need to go to a different desk in the same office to get this done. Only 15 percent of customers out of a sample of 58 actually went through with requesting the deletion. Customer exit interviews

suggested this was at least partly because customers feared that having their data deleted might reduce their chances of getting approved for the loan, even when they had been told they could delete their information without impacting the loan decision. Given this, we changed our approach to ensure that it was clear to customers that the only difference was in their time, not their chances of getting the loan.

The office was then set up with two desks. Desk 1 was for quick processing, taking 10 minutes but with no guarantee of data privacy and protection. Desk 2 was for an extended processing time of 30 minutes with a guarantee of data privacy and protection. In this case, 82 percent of the 96 participants were willing to wait for the product with protections. Another test run with 20 participants, with wait times at 5 and 15 minutes, respectively, led to similar results. Ninety percent of customers were willing to wait for the safer product, again suggesting a low sensitivity to price or wait time for those who wanted the protection.

## What Is Their Biggest Concern?

**Sharing data with third parties seems to be the most sensitive issue.** Given that privacy features seem to guide customer choice, we conducted additional research to look at which privacy features were most important for customers. When given the choice between different elements of data privacy, such as anonymity, length of data collection, length of data retention, and third-party sharing, people were the least comfortable with providers sharing their data with third parties.

To test this, we conducted a month-long study in Kenya, in which 208 customers agreed to install on their phones software that was able to scrape and send out their data. Customers understood that this software was being installed and were given mobile data vouchers to compensate them for the potential cost of data use related to the data-gathering app. They were asked if they were willing to sell different privacy features and, if so, at what price. The three features tested were:

1. **Anonymity.** Whether the mobile wallet data collected on the individual would be linked to their name and personal details.
2. **Permanence.** Whether the mobile wallet data collected on the individual would be kept for six months or permanently by the researchers.
3. **Sharing.** Whether the researcher would have the right to share the data with any third party that it chose to, including to make a profit by selling the data.

At the beginning of the experiment, 73 percent of participants were willing to sell the anonymity feature, and 69 percent were willing to sell the permanence feature. However, only 54 percent were willing to allow their data to be shared with third parties. Participants

were offered up to KES 100 for each feature,[3] a significant amount of money given that 90 percent of participants reported making less than KES 3000 a month and 51 percent reported making less than KES 1000. Customers were given the chance to change their decision before the end of the study. By then, those willing to sell their privacy features had dropped to 62 percent for anonymity, 57 percent for permanence, and 40 percent for sharing, and the prices required for those willing to sell had increased. This may have been because they became more aware of the data that were being collected by the app after the data were generated. The loss of privacy may have become more tangible once the experiment started.

## What Happens If Privacy Is Not an Option?

**People are willing to give up their privacy when they don't have a choice.** A big caveat on these positive results is that they happened when we offered people a choice. Poor people often depend on loans to cover basic needs or to invest in their livelihoods, and they may not be able to afford to turn down a loan. We found that when people don't have (or don't perceive that they have) a choice, most who need a loan are willing to take it regardless of its privacy features. Although they might prefer to keep their data private or to limit the way in which a financial services provider can use their data, we did not find that it deterred them from taking a loan if that was the only loan option offered to them.

We tested this with 198 participants from Kenya, where half of the group was offered a loan where the provider had no access to their phone's personal data while the other half received an offer that stated the provider would get complete access to their phone's personal data (e.g., SMS, call information, phone contacts, WhatsApp messages, Facebook profile). Each participant received only one loan product offer, which he or she could accept or decline. Both loan products had the same characteristics, including cost. The experiment showed that having to provide access to their personal data did not reduce the proportion of consumers who accepted the loan: 69 percent of the people accepted the full privacy loan compared to 77 percent of the people who accepted the no privacy loan. Before making the choice, some individuals sat through a presentation that explained the importance of data privacy and protection. However, their behaviors did not differ from the rest. This, combined with the results when given a choice, could suggest that it is not a lack of awareness that is driving the acceptance of loans with weak privacy features, but instead a need for financing that exceeds the need for privacy.

3 To measure their willingness to pay, customers were asked to make a choice under different scenarios: in Scenario 1, the price offered was KES 10, in Scenario 2 it was KES 20, and so on up to Scenario 10 with a price of KES 100). For the payment, a scenario was selected at random, and the participant would get paid (or not) based on their choice for that scenario.



## What Does This Mean for Providers and Policy Makers?

The findings from our studies in Kenya and India have some clear messages. They show not only that poor people care about privacy but specifically that they care enough to spend their time and money on it when they are empowered to do so. Although customers are willing to give their data to a potential financial services provider, they would not want the provider to share their data with third parties. These results are particularly interesting for a segment that has limited resources to spend on fees. Our results also highlight the vulnerability of a segment that, in the absence of options, is willing to accept privacy conditions it may not like. At the same time, it's important to note that there are limitations to this research. These results should be validated on larger sample sizes and be analyzed using real-world behavior of customers signing up for real products.

For providers, this research shows that having sound privacy and data protection policies—and advertising them to customers—could not only address a regulator's concerns, but they could also be a strong marketing proposition that gives them a competitive edge. The growth of digital credit means that customers have more options to choose from. Therefore, it will be increasingly important for providers to differentiate themselves. Our research shows that sound privacy and protection policies could help providers stand out from competitors and attract and retain the best customers. This value proposition may be an incentive for self-regulation in the absence of clear legal guidance in many jurisdictions. While the focus of our effort was on self-regulation, the research also provides evidence to regulators and policy makers that their constituencies care about privacy issues, which makes a strong case for regulation and improved oversight.

CGAP

cgap.org