An Analysis of the PBOC's New Mobile Payment Regulation

Andrew Liu

In 2016 alone, China saw $9 trillion in mobile payments—in contrast to a comparably small $112 billion of mobile payments in the United States (Abkowitz 2018). The use of mobile payment systems such as Alipay and WeChat Pay are widespread in China, with users ranging from beggars to lenders to criminals. Previously, the mobile payments landscape was largely untouched and unregulated by the Chinese government because of its relative insignificance in the Chinese economy. However, with the explosive growth in mobile payment transactions, the People's Bank of China (PBOC) implemented a new mobile payment regulation on June 30, 2018. Most notably, the government will require all mobile payments to be cleared through the PBOC, and hence, all mobile payment transactions will begin to touch the hands of the Chinese Communist Party (CCP) (Hersey 2017).

The PBOC's stated reasoning for implementing this regulation is to curb money laundering and fraud. While those are valid concerns, it is unlikely that there are not additional motivations for the new regulation. In this article, I analyze the effects this new regulation has had and will likely have on the various mobile payment system stakeholders, competitors, and users, and also uncover what underlying motives the PBOC has in implementing the regulation.

Cato Journal, Vol. 39, No. 1 (Winter 2019).

Andrew Liu is a senior at Dartmouth College where he is an early Phi Beta Kappa inductee. The author thanks John Welborn for research assistance, as well as Jim Dorn for helpful feedback.

Previous literature has analyzed the security of Chinese mobile payment networks and competition, regulation, and innovation in the mobile payment industry, but no formal literature has been written to this point analyzing the PBOC's new mobile payment regulation. Liu (2015) takes a deep dive into Alipay's user service agreement and analyzes its security; Liu, Kauffman, and Ma (2015) investigate how regulation affects innovation and competition between mobile payment platform providers. This article adds to the existing literature by analyzing the observed and probable effects of the PBOC's new mobile payment regulation.

In this article, I find that China's new mobile payment regulation gives the government access to the proprietary user data of mobile payment giants and will not improve mobile payment security. Instead, the new regulation will compromise the incentives of mobile payment providers and funnel mobile payment transactions into more illicit and unsecure channels.

A Brief History of Mobile Payment Regulations in China

Until recently, the Chinese government has largely taken a hands-off approach toward regulating mobile payment transactions. Users of third-party mobile payment platforms such as Alipay and WeChat Pay have been able to make transfers without transaction caps and other restrictions. Since the transactions are routed and directly settled through a third-party mobile payment platform provider, banks cannot see transaction details. For instance, a transaction for a pair of new sneakers settled through Alipay would show up to a bank as "Alipay," not the name of merchant selling the sneakers; in addition, the merchant's location would also be omitted (Wildau 2017). As a result, mobile payment providers have enjoyed exclusive access to billions of proprietary data points describing consumer behavior. Importantly, this means that the government does not possess this proprietary data, and, thus, is missing an enormous amount of information about its citizens that it otherwise could have obtained.

The lack of regulations on mobile payment platforms has indeed allowed for money laundering and other illicit activities to occur over the mobile payment networks, but simultaneously, the lack of regulations has also allowed for mobile payments to grow explosively and transform and improve the way consumers and merchants buy and sell their goods and services (Abkowitz 2018).

The PBOC began regulating mobile payments on June 30, 2018, by requiring all mobile payment transactions to be routed through a central clearing house, called the Online Settlement Platform for Non-Bank Payment Institutions. Consequently, transactions completed over mobile payment networks can no longer be settled directly through the mobile payment platform provider and must be sent to the centralized clearinghouse for settlement. This means that the previously proprietary consumer data collected by mobile payment platform providers like Alipay and WeChat Pay is now sent to the centralized clearinghouse, where other mobile payment platform providers and banks have access to this invaluable data (Wildau 2017).

The government's stated reason for this regulation is to make mobile payments more secure for users and to curb illicit activity over mobile payment networks, as the central bank and government now have the ability to inspect transaction details for all transfers made over mobile payment platforms and can identify and investigate fraudulent or other illegal activities occurring over mobile payment platforms (Zhang 2017).

However, this is far from the only motive involved. The PBOC and CCP have a host of additional uses for this data—mobile payments have become such an integral part of China's consumer economy that mobile payment transactions paint a detailed picture of an individual's daily habits, including their consumption preferences, whereabouts, and spending power (Abkowitz 2018). Thus, by obtaining mobile payment transactions data, the PBOC and CCP gain access to an intimate view of the daily behavior of a substantial portion of their citizens, which is invaluable for a government that seeks ultimate power over its political, economic, and social systems. The government's uses of the data range from helping track and take down political opponents, to helping implement and enforce the new social credit system. In the next sections of this article, I analyze the likely ramifications of the PBOC's new mobile payment regulation and argue that it is this ulterior motive for data collection that is ultimately driving the PBOC and CCP's pursuance of this new regulation.

The Effects of Mobile Payment Regulation in China

I start my investigation of the PBOC's mobile payment regulation's ramifications by analyzing the winners and losers of the new regulation. Empirical evidence is limited given the recent

implementation of the policy, but the political and economic context suggests clear winners and losers. The primary winners of this new regulation are the CCP, PBOC, UnionPay, and smaller mobile payments providers, as they get access to the previously proprietary consumer data of mobile payment giants Alipay and WeChat Pay. The biggest losers are Alipay and WeChat Pay, entrepreneurs, and consumers, as the mobile payment giants lose one of their primary incentives to offer a state-of-the-art mobile payment platform, and entrepreneurs and consumers lose their privacy when using mobile payments, forcing them to consider alternative payment options.

Winners

The biggest winners of the new mobile payment regulation are the CCP and PBOC. By gaining access to the billions of proprietary consumer data points collected by mobile payment providers, the CCP and PBOC gain incredible insight into the behavior of the hundreds of millions of Chinese citizens that use mobile payment platforms (Abkowitz 2018). The government has a myriad of uses for this data. First, officials can now more easily track down and find incriminating evidence for political opponents by tracking their monetary transfers through mobile payment platforms. In addition, with the full-fledged implementation of the social credit system on the horizon, the government will be able to monitor its citizens on a more granular level and have more data on which to base its social credit scores (Ma 2018). Finally, the government also gains yet another way to extract potential rents, by exchanging the collected data for bribes and through fines for policy violations—for example, in August 2018, the PBOC fined four companies 100 million yuan for breaching service regulations (Ren 2018).

In all, these proprietary data enable the government to capture and retain additional political, economic, and social power, as it allows officials to better eliminate political opposition and enforce the will of the CCP on citizens in both a social and economic sense. With these enormous benefits, it is difficult to believe that the government's stated intentions of improving mobile payment security and cracking down on criminals are its sole intentions in implementing this new regulation.

UnionPay and smaller mobile payment providers also emerge as winners from this new regulation. UnionPay is the official

government-affiliated payments network and was late to the mobile payment scene. By stifling large mobile payment providers through forcing them to send their proprietary data through the central clearinghouse, the new regulation gives UnionPay and smaller mobile payment providers a chance to catch up to Alipay and WeChat Pay (Abkowitz 2018). It should be noted, however, that the smallest mobile payment providers also face the risk of getting pushed out of the mobile payments landscape entirely due to the cost of compliance with regulations and the need for a government-issued license.

Losers

Alipay and WeChat Pay are the biggest losers of the new mobile payment regulation. Combined, Alipay and WeChat Pay capture 94 percent of the mobile payment market, and thus, currently hold the most proprietary user data (Zhang 2017). Alipay and WeChat Pay are also part of larger lifestyle apps offered by Alibaba and Tencent that consumers use in all parts of their lives. The value of this proprietary data is enormous, as it helps Alibaba and Tencent inform their business decisions in the various other segments of their businesses, and is a critical driver of their competitive advantage over other firms in their respective spaces (Liao 2018). Having to give up their incredible amounts of proprietary data is an enormous blow to their businesses, as it helps level the playing field for other smaller companies.

Liu, Kauffman, and Ma (2015) find that with technological innovation, regulations can either spur or decelerate innovation: regulations that increase market uncertainty will decelerate innovation, while regulations that decrease market uncertainty will accelerate innovation. In this case, given that the Chinese government typically puts its own interests of power retention first, and given that the government has clear alternative use cases for the mobile payment data but has been ambiguous in describing its plans for these data, it is unclear what exactly the government will do with the data and how it will affect the mobile payment market. Hence, it is highly unlikely the government will implement the new regulation in an appropriate way to spur innovation.

While the Chinese government might argue that this promotes competition, it also encourages free riding of the innovating firms by followers and thus dampens the incentive to compete in an innovative sense, as the competitive advantage of being an innovator will be

severely limited by this new regulation. There also has been no evidence of a lack of competition between Alipay and WeChat Pay to this point, as they have both engaged in a fierce competition for market share and users (Hersey 2017).

Entrepreneurs, small businesses, and consumers also end up on the losing side of the new mobile payment regulation. As heavy current users of mobile payment platforms, entrepreneurs, small businesses, and consumers have a few alternative options for payment. First, they could continue to use mobile payment platforms and allow their data to be collected by the government. This is suboptimal, as it allows the government to collect personal and potentially sensitive data that could later be used to incriminate them. Another option is to revert to using cash for payments; however, this is not ideal for either merchants or consumers. For consumers, this requires holding additional cash, which can be lost and typically is not preferred; for merchants, this potentially reduces consumer demand, as some consumers will opt to purchase goods and services from merchants who accept electronic payments (Mozur 2017). A third option is to find other peer-to-peer (P2P) payment methods that skirt the new regulation and avoid having transactions tracked by the government; this saves merchants and consumers from having their data collected, but also puts them at risk of being caught for illicitly avoiding the mobile payment regulation.

None of these options come without costs—privacy will be lost, entrepreneurship harmed, and consumer demand and monetary liquidity reduced. Privacy will be lost as mobile payment users who continue to use the platforms will give up their data to the government; entrepreneurship will be harmed, as the effective cost of doing business will increase with an increase in transaction costs due to the implicit cost of having to share data with the government or find alternative payment methods; consumer demand will be reduced as transactions on the margin may no longer occur due to the reduction in payment convenience; and monetary liquidity will also be reduced, as some users will switch to more cumbersome forms of money transfer mechanisms. Entrepreneurs, small businesses, and consumers will not suffer alone—the economy at large will also suffer with potentially dampened entrepreneurship and innovation, consumption, and liquidity (Chow 2010). Everyone will be forced to either sacrifice their privacy or bear the increased costs of a more expensive payments system.

The Necessity of Mobile Payment Regulation

In thinking about the ramifications of the PBOC's new mobile payment regulation, it is important to ask the question: Is this new regulation even necessary? As mentioned previously, the PBOC's stated motives for this new regulation are to curb criminal activity and to make mobile payments more secure for consumers—if these are indeed the government's primary motives for implementing the new regulation, one would expect to see significant problems on both fronts in the current mobile payments landscape.

The government's concern regarding criminal activity occurring over mobile payments platforms is valid—however, routing every single mobile payment transaction through the central clearinghouse is an unnecessary and fruitless step to take in cracking down on criminal activity. While overseeing all mobile payment transactions may help drive out criminal activities from mobile payment platforms, there is no empirical evidence that suggests it will reduce criminal activities in aggregate. It is very possible that criminal payment transfers will move to a different medium, whether it be cash, drugs, or some other asset; these other mediums of transferring value are much harder to track than mobile payments, and hence, could very possibly make the crackdown on criminals more difficult than it already is (Pei 2016). A more effective way to crack down on criminal payments activity would be to gain the cooperation of mobile payment providers such as Alipay and WeChat Pay, and align their incentives such that they seek to identify criminal behavior themselves. For instance, the government could offer mobile payment providers tax breaks contingent on their detecting criminal activities on their payment networks.

On the other hand, mobile payments security was never a significant problem to begin with. In 2017, it was reported that $13 million was lost or stolen through mobile payments in Guangdong province ("Let's Talk" 2018). While this figure is not insignificant, even after extrapolating the figure to all provinces in China, in comparison to the $12.77 trillion in mobile payments transactions in China from the first ten months of 2017, the amount of money lost and stolen is small (Du 2018).

Meanwhile, PayPal, a prominent U.S. third-party payment platform, has a fraud rate of 0.32 percent, which is already significantly lower than the 1.32 percent that U.S. merchants see on

average (Morisy 2016). Given these figures, it is hard to imagine that China's mobile payment fraud rate would be any higher than other prominent payment platforms. In addition, Chinese mobile payments solutions like Alipay and WeChat Pay offer users buyer protection, but without the high transaction fees of PayPal. Venmo, another prominent U.S. third-party payment platform, charges users low transaction fees, but lacks any form of buyer protection, instead relying on users to transfer their money carefully ("Venmo Security" 2018).

With a low estimated fraud rate and standard buyer protection services, China's mobile payment security seems at least as secure as mobile payment security in Western countries like the United States. Thus, the Chinese government's stated mobile payment security concern does not seem to carry enough substance to warrant routing all mobile payment transactions through the central clearinghouse, suggesting that the government may have ulterior motives for pursuing this new regulation.

The Effect of Mobile Payment Regulation on Transaction Security

If the PBOC truly intended to improve mobile payment security, one would also expect the new mobile payment regulation to indeed improve security. However, this seems unlikely given the other security-bolstering options that are available. The new mobile payment regulation is a reactionary measure, not a preventive one—it assists in allowing the government to investigate fraudulent activity that has already occurred but does little to prevent illicit activity from occurring in the first place.

In fact, the new regulation has the potential to make mobile payment security worse. With the new regulation, consumer and merchant data move from the hands of private platform providers like Alipay and WeChat Pay—who have an interest in keeping the data safe in order to satisfy and retain users—to the government, through the central clearinghouse. As has been demonstrated repeatedly, Chinese government officials are frequently corruptible, and there is little evidence against government officials being willing to exchange mobile payment data for an appropriate bribe (Pei 2016).

Further, the regulation does not improve payment security outside of mobile payments either. As previously discussed, criminals

can move their monetary transfers into alternative, potentially illegal channels, which are undoubtedly less secure (though payment security for criminals certainly is not a priority). More importantly, if consumers and merchants choose to substitute away from platforms like Alipay and WeChat Pay to avoid the regulation's data collection, payment security would likely decrease as well—cash is tangible and can be stolen, and other P2P transfer mechanisms lack the advanced infrastructure present in platforms like Alipay and WeChat Pay.

There are other simpler and easier-to-implement measures that can actively promote better mobile payment security. While the PBOC has indeed advocated for some of these measures, such as transaction tokenization and dynamic QR code generation, and has set some technical requirements on QR code encryption and transaction verification, it has not done much in the way of enforcing these security measures. Instead, the PBOC now requires payment service providers to obtain a permit from them in order to use QR code payment (Jing 2017). This adds another layer of bureaucracy for payment service providers to grapple with, and like many other Chinese industries that require permits, looks like yet another way for the government to extract rents, this time from payment service providers.

Additionally, mobile payment providers have the incentives to improve payment security themselves. Platforms like Alipay and WeChat Pay strive to capture as many users as they can, and in order to gain market share, they must offer a best-in-class payment platform. There is little evidence that platforms like Alipay and WeChat Pay would not rush to improve their platforms' security should user concerns ever become significant. Despite Alipay and WeChat pay effectively having a duopoly on the mobile payments market, the competition between the two firms has been fierce—in their competition for market share, they have often even subsidized users to use their platforms (Hersey 2017). In short, Alipay and WeChat Pay have exhibited no signs of monopolistic behavior or collusion and have the incentives to independently improve their platforms' security to maximize their market share.

If the Chinese government aims to improve mobile payment security, it could start by addressing its legislatorial framework. As discussed by Liu (2015), the Chinese legal framework for mobile payments is incredibly fragmented, with numerous authorities

involved with a myriad of different laws that insufficiently protect mobile payment users. Unfortunately, this fragmented legal maze reflects a problem of the Chinese legal system as a whole, so it is very unlikely that a reformed legal framework will act as a solution for improved mobile payment security.

In short, mobile payment providers seek to retain users, and thus already have the incentives to provide their users with sufficient service security. The PBOC's new mobile payment regulation does not improve payment security and may even make mobile payments less secure by adding layers of bureaucracy into the mobile payments system and forcing user data to pass through more sets of hands. Therefore, the PBOC's true motive for pursuing the new mobile payment regulation is unlikely to be security improvement.

Conclusion

While the Chinese government puts up an altruistic front of wanting to prevent criminal activity and improve mobile payment security, the PBOC and CCP's true intentions for implementing the mobile payment regulation are far more pragmatic, and seek to help the Communist Party maintain full political, social, and economic power of the country.

The new regulation provides the government with unprecedented access to data detailing the lives of its citizens and will assist it in taking down political opponents, extracting additional rents, and closely monitoring its citizens and implementing its social credit system. While empirical evidence is still limited, the regulation poses significant risks to the Chinese economy. Mobile payment giants Alipay and WeChat Pay will lose an enormous incentive to continue pioneering mobile payment networks, and as a result, innovation will likely suffer. Further, entrepreneurs and consumers will suffer, as they will be forced to either give up their privacy or adopt an alternative method of payment. For entrepreneurs, this will manifest itself as an increase in the cost of doing business, and entrepreneurship and innovation will be dampened. Thus, while the government will indeed reap large gains from the implementation of this mobile payment policy, the costs to innovation in mobile payment networks and to entrepreneurship and innovation at large are significant and will hamper the Chinese economy as it strives for sustained growth.

References

Abkowitz, A. (2018) "The Cashless Society Has Arrived—Only It's in China." *Wall Street Journal* (January 4).

Chow, G. C. (2010) "Entrepreneurship Propelling Economic Changes in China." In *Interpreting China's Economy*, 3–20. Singapore: World Scientific.

Du, J. (2018) "China's Mobile Payment Volume Tops 81 Trln Yuan." *China Daily* (February 19).

Hersey, F. (2017) "Alipay and WeChat Pay Could Be Affected by PBOC's QR Code Standards' TechNode." *TechNode*. Available at technode.com/2017/12/28/alipay-wechat-pay-affected-pbocs-qr-code-standards.

Jing, S. (2017) "Rules Set for Bar Code, QR Code Payment." *China Daily* (December 29).

"Let's Talk about Mobile Payment Regulations in China." (2018) *Rambus*. Available at www.rambus.com/blogs/understanding-mobile-payment-regulations-in-china.

Liao, S. (2018) "How WeChat Came to Rule China." *The Verge*. Available at www.theverge.com/2018/2/1/16721230/wechat-china-app-mini-programs-messaging-electronic-id-system.

Liu, J.; Kauffman, R. J.; and Ma, D. (2015) "Competition, Cooperation, and Regulation: Understanding the Evolution of the Mobile Payments Technology Ecosystem," *Electronic Commerce Research and Applications* 14 (5): 372–91.

Liu, Y. (2015) "Consumer Protection in Mobile Payments in China: A Critical Analysis of Alipay's Service Agreement." *Computer Law and Security Review* 31 (5): 679–88.

Ma, A. (2018) "China Has Started Ranking Citizens with a Creepy 'Social Credit' System: Here's What You Can Do Wrong, and the Embarrassing, Demeaning Ways They Can Punish You." *Business Insider*. Available at www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

Morisy, M. (2016) "PayPal Practices Defense with Deep Learning." *MIT Technology Review*. Available at www.technologyreview.com/s/545631/how-paypal-boosts-security-with-artificial-intelligence.

Mozur, P. (2017) "In Urban China, Cash Is Rapidly Becoming Obsolete." *New York Times* (July 16).

Pei, M. (2016) *China's Crony Capitalism: The Dynamics of Regime Decay*. Cambridge, Mass.: Harvard University Press.

Ren, D. (2018) "China Fines Four Payment Companies 100 Million Yuan for Breaches." *South China Morning Post* (August 7).
"Venmo Security." (2018) *Venmo*. Available at venmo.com/about/security.
Wildau, G. (2017) "China Targets Mobile Payments Oligopoly with Clearing Mandate." *Financial Times* (August 9).
Zhang, M. (2017) "China Sets up Clearing House for AliPay and Tenpay." *South China Morning Post* (August 15).