
# Privacy Impact Assessment: Alipay

Privacy & Big Data
B-KUL-H00Y2A

Xinyuan Xing, Yijun Shi , Sihan Wang

# 1.Introduction

Firstly established in 2004 to facilitate transactions on Alibaba's e-commerce platform, Alipay is now the largest third-party and online payment platform around the globe. Similar to its US counterpart PayPal, Alipay enables users to register and link their bank account and make online purchases. Sprung out of China's inadequate payment infrastructure and often described as the missing piece of China's e-commerce, Alipay has a synergistic and mutually reinforcing relationship with the Alibaba ecosystem at large(Zhu et al., 2017). As indicated in Alibaba 2020 Annual Report, Alipay boasts over 1.3 billion annual active users and $17 trillion worth of annual transactions. It has evolved from an online wallet to an essential component of the larger Alibaba Ecosystem and an indispensable part of users' daily life. Since big data is fundamental to Alipay's business model, investigating and assessing Alipay's privacy impact becomes ever more relevant in the context of heightened public awareness of data protection and user privacy.

## 1.1 Functionality

### Mobile Payment Services

The primary functionalities of Alipay are peer-to-peer mobile payments, third-party online payments, and in-store payments. Payments are central to Alipay's online-to-offline strategy and crucial for its global outreach. In addition to strengthening its online dominance, Alipay is also expanding its in-store payments domestically and internationally, supporting 27 currencies and partnering up with over 200 domestic and 250 overseas financial institutions in over 36 countries. Alipay has also developed extensive value-adding functionalities over the past decades through the integration of data analytics and cloud computing technologies, as will be discussed below.

### Location-Based and Administrative Services

Alipay provides users with advanced location-based services, such as public transportation, medical appointments, entertainment, and online grocery shopping. Users could easily pay for bus fares, hail taxis, pay for their electricity, or book a weekend resort through a few taps on the Alipay mobile app. In collaboration with public organizations, Alipay also offers users online governmental and administrative services such as social benefit applications. Under the current

pandemic, Alipay has also promptly integrated the COVID-19 services, allowing users to stay updated to the latest policies and track relevant statistics.

**Financial and Investment Services**

As a direct challenge to traditional consumer banking, Alipay provides users with a broad range of value-adding financial services such as micro-loaning, investment products, and insurance services. Through cooperation with Ant Financial's Huabei, an online consumer loan entity, Alipay allows users to make installment payments for their online purchases. Users also have the option to borrow cash from Jie Bei and have funds directly transferred to their Alipay accounts. In tandem with the aforementioned loaning and installment services, Alipay's credit rating system, Zhima credit is also developed to leverage Alibaba's robust database to assess an individual user's trustworthiness and relevant risks. Users' online transaction history, in-store payments, tax and social security payment history, as well as their professional and criminal records are taken into consideration in the calculation of their Zhima Credit Scores.

Alipay also provides users with investment products and insurance offerings to help users grow their wealth and limit risks. With Alibaba's internal infrastructure such as Yu'e Bao and MYbank, Alipay users could manage their cash in a flexible manner. On Alipay, users may also invest in money market funds, fixed income products, and equity funds from external financial institutions. With the abundance of offerings available on Alipay and its low transaction costs, many users have abandoned traditional consumer wealth management in favor of this all-in-one platform.

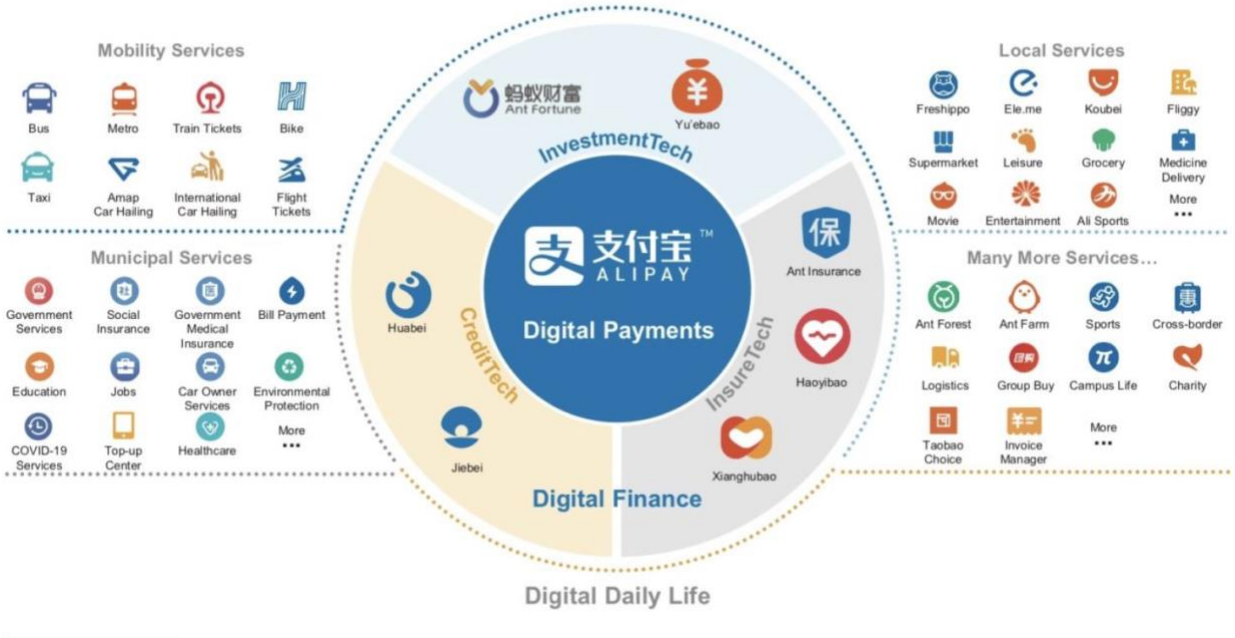


*Figure 1 Key functionalities of Alipay*

## 1.2 Key Stakeholders and Trust Assumptions

In this section, we identify all parties that are implicitly or explicitly involved in Alipay's data processing and their respective privacy needs. Identifying these stakeholders helps us better assess Alipay's privacy impact and devise various privacy-enhancing strategies.

**End Users**

The most implicated stakeholder of Alipay is its end users, whose personal information and transaction data are collected, processed, and stored by Alipay as the prerequisite of its services. For most Alipay users, the perceived ease of use is still the strongest factor in their intention to use Alipay, compared with perceived informational and financial risk(Ma et al., 2018). Still, trust from users is a major factor in the user adoption of Alipay(Mu & Lee, 2017), and it is what enables Alipay to venture beyond e-commerce to provide other value-adding services. By registering on Alipay, users provide not only general personal information such as name, contact, address, but also sensitive information such as national ID number, debit card details(Alipay, 2021d). In their extensive use of Alipay for its payment and other services, end users also assume that Alipay will

responsibly and lawfully handle their personal data. They trust that their personal data are encrypted and processed by Alipay in ways that minimize financial and other losses.

**Governments and regulatory organizations**

Due to the nature of Alipay as a payment platform, governments and regulatory organizations are also implicated in Alipay's privacy impact. According to Alipay's Privacy Notice, Alipay may disclose user information based on applicable law or regulation or upon the request of government officials or other third parties that Alipay has contractual or regulatory obligations to. For example, Alipay may disclose users' personal information as per anti-money laundering and counter-terrorist financing reporting requirements. This gives governments a toolbox to enhance social trust but also breeds the possibility of abuse and surveillance.

**Banks and other third-party Financial Institutions**

Alipay closely collaborates with commercial banks and investment institutions to provide users with extensive financial services. These financial institutions are important stakeholders because the transaction data they provide is key to the services provided by Alipay. By permitting Alipay to access these key data, these institutions trust that Alipay will not abuse these data or jeopardize their financial and other interest. In addition, traditional commercial banks also face the risk of capital and technical disintermediation because of Alipay's greater efficiency and growing prominance in users' everyday life (Lai, 2020). Therefore, banks and financial institutions can be seen as both competitors and collaborators of Alipay.

**Commercial Partners and Third-Party Vendors**

Commercial partners are crucial to the Alipay ecosystem and play a key role in maintaining the integrity of users' privacy. As Alipay strives to become a one-stop digital lifestyle platform, it increases collaboration with commercial partners and vendors to provide various services through the Alipay app (Hashim, 2020). These commercial partners have access to anonymized user data, which they may use for marketing purposes. By allowing commercial partners access to user information, Alipay trust that they will only use these data for stated purposes and not attempt to identify users through data re-identification techniques.

## 1.3 Data collection

The data collected by Alipay include general user information and personal sensitive information. The data can be divided into 4 categories, involving users, governments, banks, and commercial third parties. The Figure shows the architecture diagram of Alipay's main data storage and transaction methods in each branch.

The main data collected by Alipay are user identity data and user financial transaction data. The identification data obtains the user's name, birth and identification number data and biometric data. Alipay may collect additional public information from users related to public safety, public health, and political management to help the government legally track user activities and IP addresses to improve data risk management services. Financial data is related to the user's bank account and general consumption. Alipay directly or indirectly collects sensitive financial transaction data from users, such as personal bank cards, payment transfer details, and daily consumption records. Such data can be traded and shared between Alipay and commercial institutions or banks, so that individuals can use the functions of the application correctly and improve the application services.

## 1.4 Design and Implementation

The data workflow chart in figure 2 describes the payment transaction implementation and the data generating implementation. Alipay has two methods of payments: online payment and in-store payment. Both of the payment methods use one APIs based on SHA256 and RSA algorithm to encode the input and response, and many abilities of integration based on HTTP protocol and SDK(Alipay, 2021a). The right part of Figure 2 shows the integration of Alipay with system integrator and acquirer, involving front end and back end architecture based on payment services and data management respectively.

The main business data of Alipay is stored in Ali Cloud using ApsaraDb for OceanBase. ApsaraDB uses Paxos protocol and common MYSQL/Oracle protocols; every node has its independent storage and processing engine, hence the storage is not shared between nodes in the ApsaraDB architecture(Alibaba, 2021). OceanBase uses OBProxy and SSL link encryption(Alibaba Cloud, 2021b), together with multi-tenant architecture(Alibaba Cloud, 2021a), prohibits cross-tenant

evaluation, isolates data management from resource management, and protects and secures data transfer between users and servers from exposure.

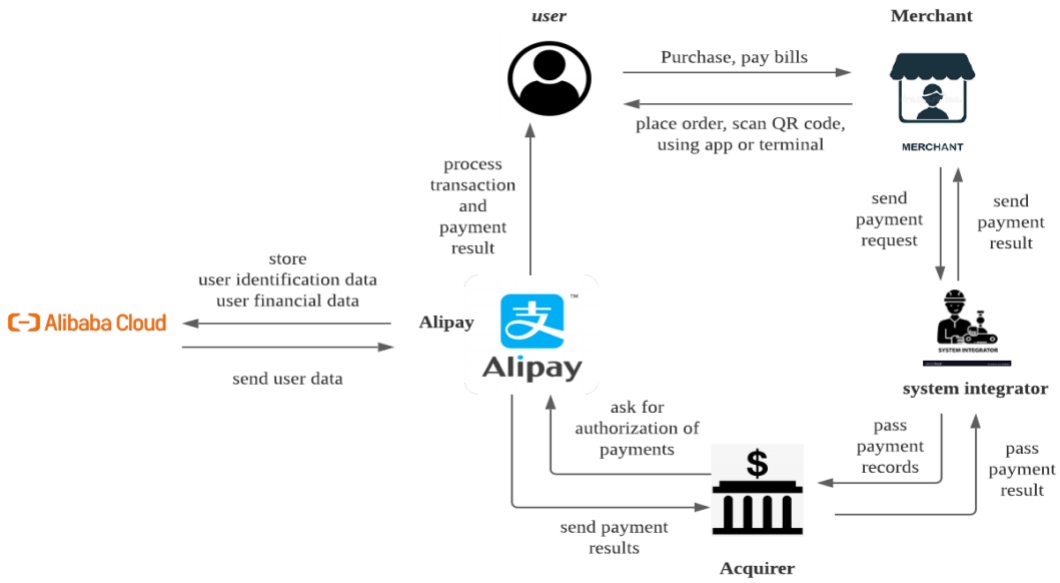


*Figure 2 Data Workflow of Alipay*

# 2.Privacy impact assessment

In the following section, we will continue to explore Alipay's privacy impact in greater depth. Several relevant technical issues such as Alipay's biometrical and financial information collection, its mobile setting, as well as its third-party cooperation will be investigated in detail.

## 2.1.1 Biometric Authentication

Biometric data involves unique physiological features that can be used to distinguish and identify individuals, such as fingerprints and facial maps. In partnership with biometric technologies and electronics companies such as megvii and Huawei, Alipay has developed and implemented various biometric technologies to optimize user experience and protect users from security threats(Mayhew, 2014). Based on the Terms and Conditions for the use of Biometric Authentication within Alipay Account and/or Alipay Wallet(Alipay, 2021b), by utilizing the biometric authentication, users authorize Alipay to use biometric information registered on their mobile devices as a method of authentication to confirm your identity in connection with the Permitted Purposes. In addition, Alipay has the right to compare and verify users' identity with

the images saved by the institution permitted by laws and regulations or authorized by the government agency. In 2019, Alipay also launched its Dragonfly facial recognition-powered point-of-sale system(Burt, 2019), which captures images of end users' facial features and enables customers to make payments to vendors without entering any identification information.

**Technical Risks Related to Biometric Authentication**

While this has streamlined the payment experience and enhanced efficiency for users, Alipay's collection and utilization of User's biometric information also presented some unprecedented risks. One particularly relevant vulnerability is the detection and prevention of presentation attack, where an attacker presents to the sensor an artifact (e.g. a photograph, a video, or a mask) to try to impersonate a genuine user(Hernandez-Ortega, 2019). Presentation attack detection (PAD) technology also represents the biggest bottleneck for biometrics systems due to the diversity and multimodality of presentation attacks, as well as the differences in related hardware and different algorithm capabilities of companies using biometrics technology. From another technical perspective, Alipay also needs to address and accommodate temporary or permanent physical changes that may lead variations in biometric conditions to enhance the reliability and accuracy of biometric authentication and identification(Pandya, 2019). These risks are especially worrying since Alipay claims that it should not be held liable for any loss, claims, costs and expenses, or damages incurred during the use of the Biometric Authentication.

**Ethical Risks Related to Biometric Authentication**

From an ethical perspective, Alipay's collection of users' biometric information raises the concern for the potential of a surveillance society. Although Alipay's use of biometric information as such is not intended to invade users' privacy, the way that such information is collected, stored and processed presents the inherent threat of conflating security with surveillance. According to Alipay's User Privacy Policy(Alipay, 2021d), Alipay may collect and use your personal information without user consent in certain circumstances in order to fulfill the obligations of national laws and regulations and relevant regulations of industry authorities. Alipay may also collect information related to national security, public safety and criminal investigation without user consent. While this may arguably enhance collective security and minimize criminal activities, it also raises the question of whether such information may be used to further strengthen and

empower the surveillance state, which may exploit such information to curb individuals' freedom of speech and suppress political dissent.

### 2.1.2 Financial information Collection

Alipay has implemented a number of financial technologies associated with banks or third-party businesses, allowing users to make consumer payments, insurance, personal loans, and query personal financial information at any time. Alipay not only protects the interests of customers and enterprises, and also improves the convenience of users' lives. As a partner of Alipay and Chinese financial institutions, Alipay provides various financial services. In Alipay's Privacy Policy(Alipay, 2021d), in order to use the applications, Alipay has the right to ask and collect basic personal information and bank account information of each user. The functions of Alipay allows financial institutions to ensure the personal identity of customers, and also allows users to make payment without making an appointment.

**Technical risks involved in financial transactions**

The basic function of payment is to use the QR code provided by Alipay. Each QR code associated with the serial number is used for payment and receipt. The recipient's QR code is only used to receive payment from the customer and the receiving code does not change once it is generated. Therefore, replacing the recipient's QR code could lead to theft and other potential financial or privacy losses(Singh, 2017). Since Alipay contains all personal financial information, another serious issue is that hackers can steal all the information from customers as they use Alipay to scan third-party QR codes(CGTN, 2017). Alipay has to adjust the security of its own payment services and applications supported by other organizations to ensure the safety of customer property.

From the perspective of virtual assets, Alipay collects user financial and credit data, leading to potential personal information leakage incidents. Alipay may request user data and share data with partner institutions for the purpose of financial credit evaluation(Alipay, 2021d). In 2017, Alipay announced that customers can check their personal credit score through the system supported by Zhima Credit, which is also known as Sesame Credit. Unknown data collection and analyzing methods have raised concerns about user privacy and security risks(Pandya, 2019). Although the sensitive and private information may be cleaned up through anonymization, the exact data

cleaning process is unclear. As personal virtual property and privacy information become more accessible to potential adversaries, individuals may struggle to protect themselves against telecom fraud, illegal debt and personal safety threats.

**Ethical Risks related to financial information collection**

Because of the huge volume of data collected by Alipay, many worry that it may utilize such data for extraneous purposes and that this may cause certain unwanted repercussions. As discussed earlier, Zhima Credit, a private credit rating feature of Alipay, incorporates insurance, loan, history payment, dating, shopping, and mobility data, as shown in figure 3.

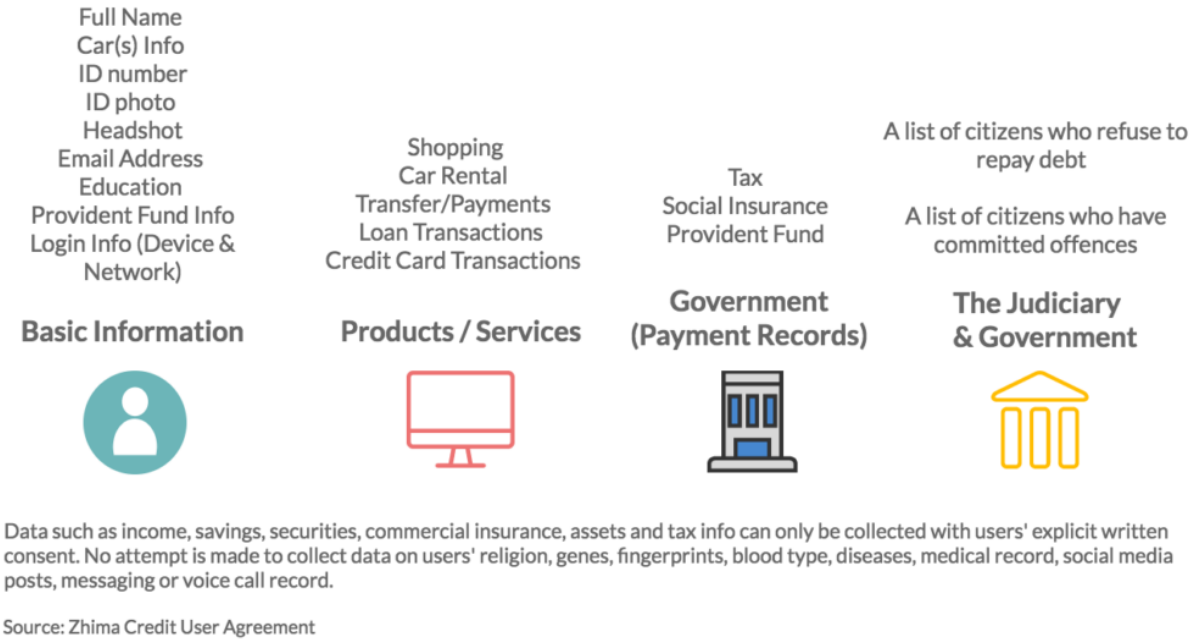


*Figure 3 Data collection by Zhima Credit*

It collects data from various sources including governmental organizations, social networks, private institutions, and other online and offline sources. Data from more than 37 million small enterprises and 300 million real-name registered users that sell or purchase on Alibaba Group marketplaces is used to fuel the system. Zhima Credit has access to all public papers, including official identity and financial records, as a result of its tight engagement with the government. While we are still learning about the long-term effects of the government-run social credit system on residents' daily lives, the impact of Zhima Credit and other commercial credit trackers, both

positive and negative, is obvious. For example, Alipay's agreements with a variety of third-party vendors, such as bike and vehicle rental firms, hotels, foreign consulates, and hospitals, waive deposits or reward Alipay users with free expedited services if they have high Zhima Credit scores. Alipay users with low ratings, on the other hand, are denied access to such services(Merics, 2018).

What is disturbing about the Zhima credit system is not just how the data is collected in the first place but also how Alipay leverages the data collected to manipulate and influence people's lives. The Zhima Credit algorithm takes into account not only whether you pay your bills on time, but also what you buy, what degrees you have, and your friends' scores(Hvistendahl, 2017). The sheer amount of data and the opacity of how these data are processed is troublesome, even if users are allegedly volunteering in participating in the Zhima Credit Scheme. On top of that, Alipay's Zhima credit system is in line with the government's history of monitoring and manipulating people's conduct. Alipay adapts, appropriates, and modifies technical trends by appealing to users' self-interest, in contrast to older communist-style posters and banners as well as propaganda-style phrases. It also uses gamified features and a loyalty-prizes program with rules, rewards, and punishments to further depoliticize the system(Chong, 2019). Underneath the rather innocuous facade of the private credit ranking scheme lies the uncertainty of whether or how participating in it could influence one's rating in the government system.

### 2.1.3 Mobile privacy setting

Alipay asks users to agree to some mobile privacy permissions, such as allowing access to their contacts, location, photos, etc. Alipay does not directly state how the information collected will be used. Because location privacy information can locate the range of activity of large numbers of people, Alipay or employees can collect this information to track users. The risk of a potential privacy data breach exists, when someone accesses a user's contacts, all of the user's human network can be captured, and this information can be collected to threaten the user or his or her family and friends. In addition, without the user's consent and without explicitly informing Alipay of the commercial analytics used, Alipay analyzes the user's consumption history and other behavior to push relevant information to the user and influence the preferences of specific groups of people. In addition, adversaries may collect users' location and contact information and commit telecom fraud against users or even threaten users' safety.

### 2.1.4 Third party cooperation

Alipay originally belonged to Alibaba group, after 2004 it belonged to Ant Financial Services subsidiary. Alipay cooperates with third parties such as Alibaba platform (Alibaba, Ali Health, Ali Cloud), Ant website (Zhima Credit, Ant Financial Technology), Taobao platform (Taobao, Tmall), the government, law enforcement agencies, local banks and so on. Alipay has many customer services associated with these third parties, and personal information collected from customer services is often sent to the third party if the customer opens a service associated with the third party. The third party's terms and conditions are independent of Alipay's terms and conditions, and Alipay has no right to standardize the data encryption processing methods used by the third parties. Consequently, Alipay has little supervisory power over how the third party may store or process user data, and the safety of users' private information may be jeopardized.

## 2.2 Legal analysis

In this section, we will assess Alipay's legal compliance to the EU's GDPR, since Alipay has expanded rapidly into the global payment market in the recent decade. With its extensive user base, Alipay controls a large amount of personal and financial information about its users. Users are required to provide personal information such as name, facial biometric information, location information, ID number and bank account for identification purposes during the registration. Alipay also requires the consent of a guardian to process information from users under the age of 14, since China sets the restrictions to offering social service to children under age 14, therefore, Alipay can be considered to meet the regulations of GDPR Art8. The end-users are natural persons and the collected information of individuals is defined by GDPR Art1. In Alipay member protection rule, Alipay declares that it collects as the minimum amount of user data as possible under legal circumstances, and uses methods such as the anonymization and de-identification of users and encrypted storage of information. Alipay also stores user identification and transaction information for as long as required by relevant laws, and according to the Alipay User Privacy Statement, Alipay meets the GDPR Art.5 regulations.

Alipay has added the User Protection Center feature to the application and updated the user protection policy, to ensure that users can access their information profile, consumption history, authorization management and privacy settings at any time in a simple and transparent way related

to GDPR Art.12[S9]. Through these features, users have better control of their information and make changes and deletions to some information in a timely manner (GDPR Art16). However, users need to provide complete personal information in order to have all functionalities of access to the Alipay application, which fails to satisfy the rights of data subjects to have incomplete user data(GDPR Art16). Moreover, Alipay provides the detailed privacy policy of Alipay and Ant Group for users to view. Alipay's open privacy policy, the details of Alipay's personal information protection agency, and contact information (GDPR Art.13.1). The updated regulations and data protection office contacts clearly state the use of personal information and protection methods, such that users can better protect their information and benefits.

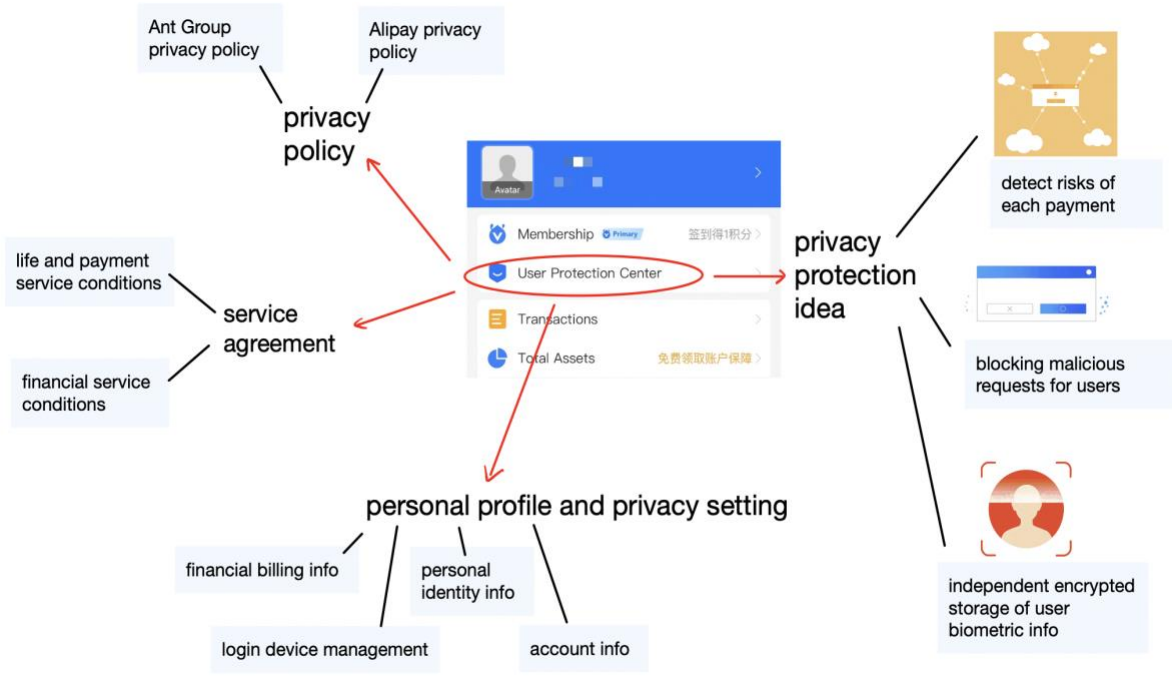


*Figure 4 Alipay User protection features*

# 3 Recommendation

Despite Alipay's effort to conform to privacy legislation in different jurisdictions in which it operates, we believe it should proactively adopt strategies to enhance its privacy architecture. In the following section, we discuss several ways in which Alipay could increase its privacy level and changes in the design and implementation of the application that it could adopt to mitigate the privacy problems identified in section 2.

**Limit data sharing with third parties**

For sharing user data to third parties, Alipay should minimize the accuracy and details of user personal information, and require those organizations to store user information in a shorter time period, while allowing users to decide which information should be disabled and which can be shared with third parties, rather than being enabled by default by Alipay or third-party applications. Alipay should consider reducing its cooperation with third parties that only collect and analyze user information for the purpose of sending relevant advertisements and consultations to users or allowing users to decide whether to receive the advertisement notifications. Construct a privacy protection framework by proposing strict and detailed contractual terms for the collection and use of user privacy information by third parties from Alipay, thus Alipay can comply with the requirements of the local country and GDPR privacy protection law.

**Employ machine learning algorithms to enhance user privacy and asset security**

Deploy modernization security machine learning algorithms to monitor account anomalies and procedures that may compromise account information and private assets. Besides, to detect whether the QR codes scanned contain online viruses and links to dangerous websites, or whether users are in high-risk consumption patterns, in order to maximize the protection of individual privacy. Furthermore, users should be explicitly informed in a transparent manner about how Alipay uses data encryption methods (such as K-anonymity, L-diversity, or other artificial intelligence methods) to reduce the risk of privacy breaches. Alipay needs to consider reducing the length of time of storing user privacy as appropriate, and striking a balance between avoiding excessive duplication of information stored in multiple components and ensuring information recovery.

**Inform and educate end users about various privacy implications**

To further fortify the user data security, we believe an indispensable piece of the picture is transparency. Many of the privacy risks mentioned earlier, such as risks related to biometric authentication and QR code transaction, can be mitigated if users could become more aware of the relevant risks involved in using these services. In addition, by making users aware of the implications of Alipay's data processing, manipulation, and storage, users could become better informed in deciding whether they or not want to share certain personal data or information. This transparency is key for gaining user trust and enhancing user experience, which in turn ensures Alipay's long-term sustainability and viability.

# References


Alibaba. (2021, June 1). *What is OceanBase Database? - Product Introduction| Alibaba Cloud Documentation Center*. https://www.alibabacloud.com/help/doc-detail/134480.htm?spm=a3c0i.20910364.9840764400.1.3e9f62a4u1zOGC

Alibaba Cloud. (2021a, June 2). *Security management - User Guide| Alibaba Cloud Documentation Center*. https://www.alibabacloud.com/help/doc-detail/139041.html

Alibaba Cloud. (2021b, September 29). *SSL link encryption - User Guide| Alibaba Cloud Documentation Center*. https://www.alibabacloud.com/help/doc-detail/254643.html

Alipay. (2021a). *Alipay APIs | Product APIs | Alipay Docs*. https://global.alipay.com/docs/ac/ams/api

Alipay. (2021b, September 17). *Alipay Biometric Authentication Terms and Conditions*. https://global.alipay.com/docs/ac/Platform/yqd3esdz?pageVersion=2

Alipay. (2021c, October 29). *Alipay Europe Account and Wallets Privacy Notice | Platform | Alipay Docs*. https://global.alipay.com/docs/ac/Platform/cxv4zkp0

Alipay. (2021d, October 31). *Alipay Privacy Notice*. https://render.alipay.com/p/c/k2cx0tg8

Burt, C. (2019, April 22). *Alipay launches new biometric facial recognition POS device with $450M incentive program*. Biometric Update |. https://www.biometricupdate.com/201904/alipay-launches-new-biometric-facial-recognition-pos-device-with-450m-incentive-program

CGTN. (2017, February 21). *Alipay makes QR code transactions more secure*. https://news.cgtn.com/news/3d677a4e77596a4d/share_p.html?t=1487676967415

Chong, G. P. L. (2019). Cashless China: Securitization of everyday life through Alipay's social credit system—Sesame Credit. *Chinese Journal of Communication*, *12*(3), 290–307. https://doi.org/10.1080/17544750.2019.1583261

Regulation, G. D. P. (2016). Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016. Official Journal of the European Union.

Hashim, S. (2020, August 18). *Alipay will allow third-party vendors on its platform.* Protocol. https://www.protocol.com/alipay-alibaba-ant-financial-china

Hernandez-Ortega, J. (2019). *Introduction to Face Presentation Attack Detection*. SpringerLink. https://link.springer.com/chapter/10.1007/978-3-319-92627-8_9?error=cookies_not_supported&code=fe71767c-bd58-4aad-9ea9-e3133aaa0f03

Hvistendahl, M. (2017, December 14). *In China, a Three-Digit Score Could Dictate Your Place in Society*. Wired. https://www.wired.com/story/age-of-social-credit/

Mayhew, S. (2014, October 17). *Alipay turns to facial and fingerprint recognition for secure payments*. Biometric Update. https://www.biometricupdate.com/201410/alipay-turns-to-facial-and-fingerprint-recognition-for-secure-payments

Merics. (2018, June 4). *Who's really responsible for digital privacy in China?* https://merics.org/en/short-analysis/whos-really-responsible-digital-privacy-china

Mu, H. L., & Lee, Y. C. (2017). Examining the influencing factors of third-party mobile payment adoption: a comparative study of Alipay and WeChat Pay. The Journal of Information Systems, 26(4), 247-284.

Lai, Y. (2020). *Alipay and the impact of e-payment systems resulting in new regulations in China and other jurisdictions - China Working Group*. International Bar Association. https://www.ibanet.org/article/5D63B47D-B8C6-47E9-92ED-D32EEDEB00F8

Pandya, J. (2019, April 17). *Hacking Our Identity: The Emerging Threats From Biometric Technology*. Forbes. https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/

Shen, X. (2020, June 5). *WeChat rolls out its own credit system nationwide, rivaling Alipay's Sesame Credit*. South China Morning Post. https://www.scmp.com/abacus/tech/article/3087781/wechat-rolls-out-its-own-credit-system-nationwide-rivaling-alipays

Singh, A. (2017, July 8). *Cashless Society, Cached Data: Are Mobile Payment Systems Protecting Chinese Citizens' Data?* The Citizen Lab. https://citizenlab.ca/2017/01/cashless-society-cached-data-mobile-payment-systems-protecting-chinese-citizens-data/

Statista. (2021, June 14). *Leading third-party payment providers in China Q2 2020*. https://www.statista.com/statistics/426679/china-leading-third-party-online-payment-providers/

Towson, J. (2021, November 23). *Ant Financial Is 3 Platform Business Models Combined. (Asia Tech Strategy – Daily Lesson / Update)*. Jeffrey Towson. https://jefftowson.com/membership_content/ant-financial-is-3-platform-business-models-combined-jeffs-asia-tech-class-daily-lesson-update/

Zhu, D. H., Lan, L. Y., & Chang, Y. P. (2017). Understanding the Intention to Continue Use of a Mobile Payment Provider: An Examination of Alipay Wallet in China. International Journal of Business & Information, 12(4).