THE CENTRE FOR internet & society

Protection of Privacy in Mobile Phone Apps

Author **Hitabhilash Mohanty**
Editor **Leilah Elmokadem**

Contents

Designed by **Saumyaa Naidu**

Introduction

The term “Fintech” refers to technology-based businesses that compete against, enable and/or collaborate with financial institutions. The year 2015 was a critical year for the Indian fintech industry, which saw the rise of numerous fintech start-ups, incubators and investments from the public and private sector. According to NASSCOM, the Indian fintech market is worth an estimated USD 1.2 billion, and is predicted to reach USD 2.4 billion by 2020.[1] The services brought forth by Fintech, such as digital wallets, lending, and insurance, have transformed the ways in which businesses and institutions execute day-to-day transactions. The rise of fintech in India has rendered the nation’s market a point of attraction for global investment.[2] Fintech in India is perceived both as a catalyst for economic growth and innovation, as well as a means of financial inclusion for the millions of unbanked individuals and businesses. The government of India, along with regulators such as SEBI (Securities and Exchange Board of India) and RBI (Reserve Bank India), has consistently supported the digitalization of the nation’s economy and the formation of a strong fintech ecosystem through funding and promotional initiatives.[3]

The RBI has been pivotal in enabling the development of India’s fintech sector and adopting a cautious approach in addressing concerns around consumer protection and law enforcement. Its key objective as a regulator has been to create an environment for unimpeded innovations by fintech, expanding the reach of banking services for unbanked populations, regulating an efficient electronic payment system and providing alternative options for consumers. The RBI’s prime focus areas for enabling fintech have been around payment, lending, security/biometrics and wealth management. For example, the RBI has introduced “Unified Payment Interface” with the NPCI (National Payments Corporation of India), which has been critical in revolutionizing digital payments and pushing India closer to the objective of a cash-less society. It has also released a consultation paper on regulating Peer 2 Peer (P2P) lending market in India, highlighting the advantages and disadvantages of regulating the sector.[4]

The consultation paper offers a definition of P2P lending as well as a general explanation of the activity and the digital platforms that facilitate transactions between lenders and borrowers. It also provides a set of arguments for and against regulating P2P lending. The arguments against regulating the sector mainly pertain to the risk of stifling the growth of an innovative, efficient and accessible avenue for borrowers who either lack access to formal financial channels or are denied loans by them.[5] This is the general consensus around the positive impact of the Fintech sector in India: its facilitation of financial inclusion and economic opportunity. However, the paper lists many more arguments for regulation than against. One of the main points made is with regards to P2P lending’s potential to disrupt the financial sector by challenging traditional banking channels. There is also the argument that, if properly regulated, the P2P lending platforms can more efficiently and effectively exercise their potential of promoting alternative forms of finance.[6] The paper concludes that the balance of advantage would lie in developing an appropriate regulatory and supervisory toolkit that facilitates the orderly growth of the P2P lending sector in order to harness its ability to provide an alternative avenue for credit for the right borrowers.[7] The RBI’s regulatory framework for P2P lending platforms encompasses the permitted activity, prudential regulations on capital, governance, business continuity plan (BCP) and customer interface, apart from regulatory reporting.[8]

The Securities and Exchange Board of India (SEBI) is also a prominent regulator of the Indian fintech sector. They issued a consultation paper on “crowdfunding”, which is defined as the solicitation of funds (small amounts) from multiple investors through a web-based platform or social networking site for a specific project, business venture or social cause. P2P lending is then a form of crowdfunding, which can be understood as an umbrella term that covers fintech lending practices. SEBI’s paper aimed to provide a brief overview of the global scenario of crowdfunding including the various prevalent models under it, the associated

benefits and risks, the regulatory approaches in different jurisdictions, etc. It also discusses the legal and regulatory challenges in implementing the framework for crowdfunding. The paper proposes a framework for ushering in crowdfunding by giving access to capital markets to provide an additional channel of early stage funding to Start-ups and SME's and seeks to balance the same with investor protection.[9] Unlike RBI's consultation paper on P2P lending, SEBI's paper on crowdfunding was intended mainly to invite discussion and not necessarily to implement a framework for regulation.

Some of the benefits cited in SEBI's crowdfunding paper pertain to the commonly mentioned advantages of fintech: economic opportunity for the SME sector and start-ups, alternative lending systems to keep SMEs alive when traditional banks crash, new investment avenues for the local economy and increased competition in the financial sector.[10] The paper also lists a set of risks that suggest the need for a regulatory framework for crowdfunding. For example, it mentions the "substitution of institutional risk by retail risk", meaning that individual lenders, who's risk tolerance may be low, bear the risk of low/no return investors when they lend to SMEs without adequate assessment of credit worthiness. Also, there is the risk that the digital platform that facilitates lending and issues all the transactions, may not conduct proper due diligence. If the platform is temporarily shut down or closed permanently, no recourse is available to the investors.[11]

The SEBI paper mentions a long list of other risks associated with crowdfunding, mostly associated with systemic failures, loan defaults, fraud practices, and information asymmetry. Information asymmetry refers partially to the chance that lending decisions are made based on incomplete data sets that are based on social networking platforms. There is a lack of transparency and reporting obligations in issuers including with respect to the use of funds raised.[12] Similar to the RBI consultation paper, SEBI makes a decent effort to weigh the costs and benefits of crowdfunding practices but only does this from an economic/financial perspective. Most of the cited risks, benefits and concerns tend to overlook information security and risks of privacy breaches of the implicated borrowers.

India Stack is a paperless and cashless service delivery system that has been supported by the Indian government as part of the fintech sector. It is a new technology paradigm that is designed to handle massive data inflows, and is poised to enable entrepreneurs, citizens and governments to interact with one another transparently. It is intended to be an open system to electronically verify businesses, people and services. It allows the smartphone to become the delivery platform for services such as digital payments, identification and digital lockers. The vision of India Stack is to shift India towards a paperless economy.[13] The central government, based on its experience with the Aadhaar project, decided to launch the open-data initiative in 2012 supported by an open API policy, which would pave the way for private technology solutions to build services on top of Aadhaar and to make India a digital cash economy. Unified Payments Interface (UPI), which will make mobile payments card-less and completely digital, allows consumers to transact directly through their bank account with a unique UPI identity that syncs to Aadhaar's verification and connects to the merchant, the settlement and the issuing bank to close transactions.[14]

It is suspected that India Stack will shift in business models in banking from low-volume, high-value, high-cost and high fees to high-volume, low-value, low cost and no fees. This well lead to a drastic increase in accessibility and affordability, and the market force of consumer acquisition and the social purpose of mass inclusion will converge.[15] India Stack serves as an example of how the Government of India has supported initiatives that would promote the fintech sector while facilitating economic growth and financial opportunity for unbanked individuals. However, there is continuous discussion around India Stack's attachment to the Aadhaar system, which can lead to the exclusion of unregistered individuals from the benefits that would otherwise be reaped from the open-data initiative. It can also result in many privacy and security breaches when records of individuals' daily transactions are attached to their Aadhaar numbers, which carry their biometric information and is linked to other personal data that is held by the government such as health records.

Global Steps Towards Enhancing Privacy Practices of Mobile Application Developers

The Governments and companies around the world have taken actions towards improving privacy practices of mobile application developers. Reviewing some of these initiatives and approaches would provide useful insight on how, with proper adjustment to the local context, the Indian government can address privacy and security concerns posed by the multitude of smartphone apps that have become prominent with the digital transformation of the Indian economy. This section will look at relevant initiatives by three global actors: The American Federal Trade Commission (FTC), the Office of the Australian Information Commissioner (OAIC), and GSMA Mobile for Development Foundation.

In 2012, the American Federal Trade Commission (FTC) published a guide titled "*Marketing Your Mobile App: Get it Right from the Start*".[16] It was intended to help mobile app developers observe truth-in-advertising and basic privacy principles when marketing new mobile apps. The guide encourages app developers to advertise with honesty with regards to what their apps can and cannot do, to disclose key information clearly, to integrate privacy considerations from the beginning, to honour privacy promises, to collect sensitive information only with consent, and to keep user data secure.[17] The guide does not delve into legal requirements of privacy protection or explain the benefits of utilizing privacy protection as a point of vantage for app developers. It merely provides a list of general recommendations without thorough explanation of how they can be fulfilled or their significance the app developer and the user.

In 2014, the Office of the Australian Information Commissioner (OAIC) released a practice guide for mobile app developers that focuses on mobile privacy. The purpose of the guide is to help smartphone application developers integrate better privacy practices in their products and services, and assist those who are operating in the Australian market to comply with the government's privacy law and best practice.[18] This government initiative takes a unique approach towards enhancing privacy practices by framing itself as a helpful tool rather than only a rigid policy or enforceable legislation. It states that its purpose is also to help businesses make their apps more "privacy friendly", regardless of whether they fall under the government's Privacy Act 1988.[19] Instead of presenting privacy practices as a set of limiting policies, it frames the privacy guide as a resource that can benefit app developers and their users. The document delivers this idea by encouraging app developers to make user privacy their "competitive advantage". It states that the Australian community places a high level of trust in the mobile apps and that apps that fail to protect their user privacy lose user confidence and gain negative publicity.[20] The guide does only encourage and incentivize privacy practices, but it also explains how the Privacy Act applies to apps and their developers, facilitating a thorough understanding of and compliance with the existing laws around privacy protection.

The OAIC guide encourages the "Privacy by Design" (PBD) approach, which intends to build privacy and data protection functions in advance, into the design specifications and architecture of information and communication systems and technologies.[21] The idea here is that privacy protection facets of apps should be accounted for throughout every part of the development process, as opposed to being implemented at the end as a "Terms and Agreement" page or a "Request to Access" pop-up. This would be done by applying privacy-enhancing practices throughout the life cycle of the personal information handled by the app—that is collection, use, disclosure, storage and destruction.[22] The appendix of the document consists of a comprehensive checklist to which app developers may refer to ensure that they have fulfilled their privacy responsibilities, transparency expectations, consent requirements and security measures.

In 2015, the GSMA Mobile for Development Foundation Inc* published a document titled "*Mobile Privacy Principles*", promoting a user-centric privacy framework for the mobile ecosystem. The report highlights that in a rapidly evolving and globally connected information society, the variation of laws between countries poses a challenge as online and mobile providers seek to comprehend and comply with myriad national legal requirements, while at the same time seeking to meet users' privacy expectations.[23] GSMA hereby suggests that industry should play a pivotal role in creating consistent privacy standards and codes based upon internationally agreed principles that meaningfully protect the privacy of mobile users. Without replacing applicable law and regulations where they exist, GSMA claims that its initiative marks the beginning of a process that will seek to shape the way privacy is advanced, managed and protected across the emerging mobile ecosystem. This process seeks to involve a wide community of participants, including a variety of industry players, regulators, civil society and consumer representatives.[24]

The ultimate objective of GSMA's initiative is to create a framework that identifies "privacy outcomes", which in broad terms refers to the privacy standards that mobile users can expect from the wide range of applications and services that they use. These privacy outcomes should reflect commonly accepted privacy principles set out in international instruments and guidelines on privacy and data protection.[25] Like the OAIC, GSMA also cites the "Privacy by Design" (PBD) model, seeking to ensure that the practices suggested throughout their document are as consistent and harmonized as far as possible across mobile services and applications, so that both industry stakeholders and users become familiar with how privacy can and should be managed.

Similar to OAIC, GSMA takes an informative approach to promote privacy practices by providing guidelines and defining global principles of privacy protection. It acknowledges the shortcomings of legal legislation when it comes to protecting privacy across borders in a rapidly globalizing context. By doing so, it suggests that all the stakeholders implicated in mobile app privacy shall collaborate to establish universal privacy principles that would be adopted by mobile app developers across the globe.

Indian Legal Regime Regulating Phone Apps

The In India, there is no absolute law safeguarding the privacy of users in the context of cell phone apps. The Information Technology Act of 2000 regulates the sphere of information technology and vaguely ensures the protection of privacy, which can be derived from the constructive interpretation of the statute. Section 43A provides compensation for failure to protect data. The Department of Information Technology has notified Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under section 43A of the Information Technology Act, 2000 on 11.4.2011. These rules are regarding sensitive personal data or information and are applicable to the body corporate or any person located within India.[26] The rules under section 43A put onus on companies to ensure privacy and prevent disclosure of information. Any such disclosure of sensitive personal data by body corporate to any third party shall require prior permission from the provider of such information.[27]

The rules provide checks and balances in the following form:[28]

- The government agencies must have been mandated under the law to obtain such information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution and punishment of offences and
- Any such agency receiving such information has to give an undertaking that the information so obtained shall not be published or shared with any other person. The government agencies are required to follow lawful process and procedures.

Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 in *Rule 3* defines "sensitive personal data or information." According to this provision, sensitive personal data means: "such personal information which consists of information relating to passport; financial information such as bank account, debit or credit cards or any other payment instrument; physical psychological and mental health condition; sexual orientation; medical records and history; biometric information and any other information received by the body corporate for processing, stored or processed under lawful contract or otherwise". [29]

The Information Technology Rules, 2011 states that the body corporate should provide for clear and accessible statements of its practice and policies, type of personal data collected under *Rule 3*, purpose of collection and usage of such information and disclosure of information including sensitive personal data as provided in *Rule 6.* [30]

Consent should be obtained for collection of sensitive personal information by the body corporate or someone on its behalf in writing through letter or Fax or email. The body corporate shall collect sensitive personal data only when the information is collected for a lawful purpose and must be necessary for its purpose. [31] According to Rule 5 (3), while collecting the information from the person concerned, he should have the knowledge of the fact that the information is being collected, the purpose for which the information is being collected, the intended recipient of the information and the name and address of the agency collecting and retaining the information. The information so collected must be used for the purpose for which it has been collected. The information provider shall be given opportunity to withdraw his consent at any point of time.

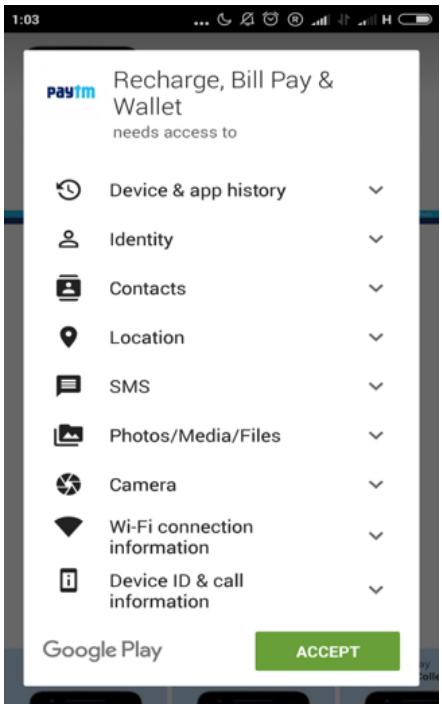
Although the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 do not expressly apply to smartphone apps, these rules would apply through implication as the apps obtain sensitive personal information from its users.

Analysis of 10 Indian Fintech Apps

For the purpose of analyzing the policy practices of the Indian Apps, this paper considers 10 Indian Fintech applications. Fintech apps collect users' financial data, which is considered sensitive personal data as defined under Rule 3 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. The study at the first instance elaborates on the permission that the app developer seeks in order to have access to information before downloading the application. After that, it analyses the privacy policies of the following apps.

1. Paytm

Founded in 2010 by Vijay Shekhar Sharma, Paytm emerged in the field of e-commerce. It initially provided services such as recharging cell phone top-ups and DTH recharges. Thereafter, it extended its services to include online shopping and also provided an e-wallet to its users, which can be used to make payment in almost all spheres (including IRCTC payments).



Permission Details

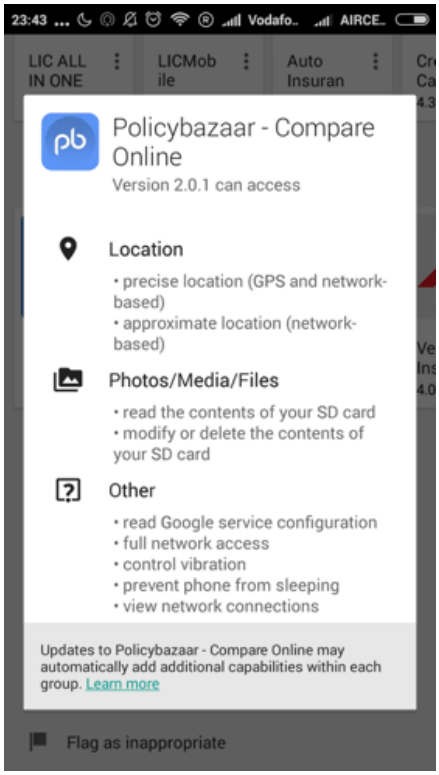
Paytm seeks permission to find the accounts on the device. It reads calendars and confidential information and can also add or modify calendar events and can send e-mails to guests without user's knowledge. It seeks access to read and modify the contacts, can read the contents of the SD card used in the device and can modify or delete its contents.

Privacy Policy

As per the privacy policy, Paytm does not sell, share or rent the user's personal information to any 3rd party or use emails addresses/mobile numbers for unsolicited emails and/or SMS. Any emails and/or SMS sent by Paytm will only be in accordance with the provision of agreed services & products and this Privacy Policy. Patym might reveal general statistical information about Paytm & its users, such as number of visitors, number and type of goods and services purchased, etc. Patym reserves the right to communicate the user's personal information to any third party that makes a legally-compliant request for its disclosure. [32]

2. PolicyBazaar

PolicyBazaar allows its users to compare and buy wide ranges of insurance and financial products such as general insurance, vehicle insurance, travel insurance, etc. It also offers features like the hospital locator and garage locator. It provides full claim support to its users and helps in solving all the issues occurring with the policy provider. It compares insurance quotes from insurance providers like Bajaj Allianz, ICICI Prudential Life Insurance, MetLife, Reliance General Insurance, AXA Life Insurance, New India Assurance, L&T, HDFC Life Insurance and many others.



Permission Details

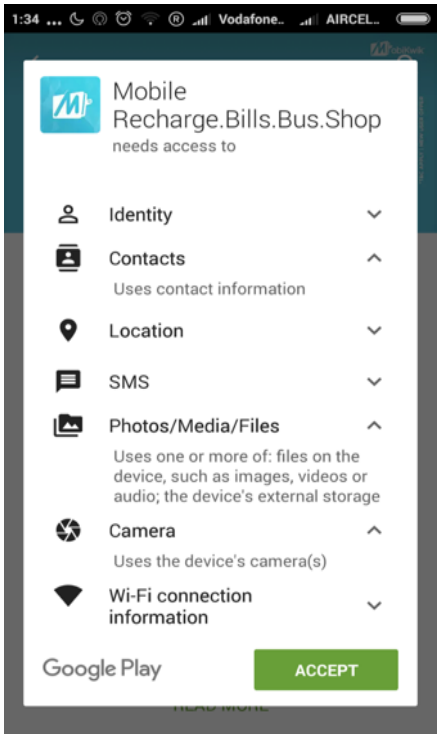
Before downloading the app, policybazaar displays a notice seeking permission to access the 'location of the device' and to use 'files on the device, such as images or videos in the external storage.'

Privacy Policy

The privacy policy of the app is displayed to its potential users before downloading the app. It states that the personally identifiable information collected by the app will not be sold or rented to anyone other than an affiliate or associate partner/business partner. The policy clarifies that PII can also be given to any successor in interest as a result of sale or merging with any other entity. Furthermore, it expressly mentions that there may be situations where it needs to share information in order to be discharged from its legal obligations. [33]

3. Mobikwik

Mobikwik provides a platform for recharging prepaid mobile, DTH, payment of postpaid bills broadband, data card, electricity, gas, insurance and utility bills. It also provides services for booking bus tickets across India and provides various shopping coupons and cash back offers. Its' online wallet can be loaded using Debit/Credit Cards or Net-Banking. It was awarded as the best wallet app by the Google.



Permission Details

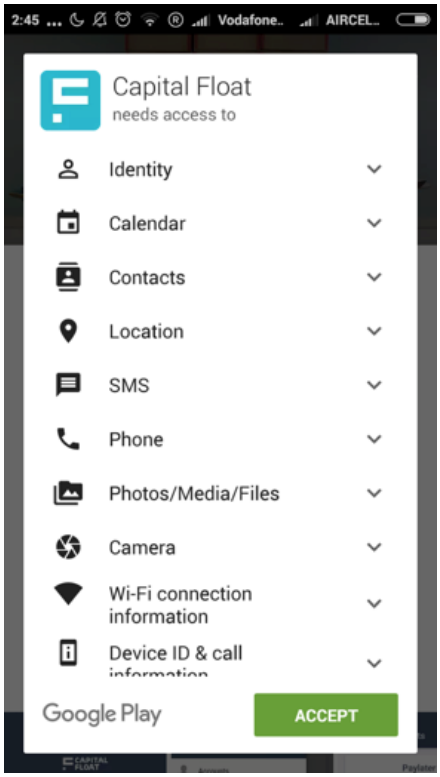
Mobiwiki takes permission to access accounts on the device and read the phone contacts of the user. It receives the precise location of the device. It also seeks permission to read the contents of the SD card and can also modify or delete the contents. It further takes permission to take pictures and videos through the app.

Privacy Policy

Mobikwik has established a set of binding corporate rules. These rules are implemented to protect the information of the user regardless of where the data resides. The policy also states that these corporate binding rules may provide additional privacy rights through the user's local privacy regulator or government. The policy specifies what information it collects including: IP address, domain servers, types of browsers, referring sources and other information associated. The application collects user information such as name, address, e-mail id, telephone number, date of birth, bank card details, online banking PIN, Taxation Authentication Number. The policy also addresses the use and storage of the information and further states that it retains certain records (this does not include credit card information) for at least 5 years after closure of the Mobikwik account. The policy reserves the right to disclose information if required to do so by law or if it believes that it is necessary to do so to protect and defend the rights, property or personal safety of the Website, or its users. [34]

4. Capital Float

Capital Float is a Bangalore-based company whose area of operation lies in the digital lending platform for working capital finance to SMEs. In the past three years, it has disbursed close to over Rs. 250-300 crores and has over 1,000 customers in 40 cities across the country with interest on loan amount varying from 16 to 19 percent. Capital Float is the official mobile application which manages the user's loan account. It tracks the existing loan, views loan details, checks and downloads the loan statements and allows users to apply for new loans.



Permission Details

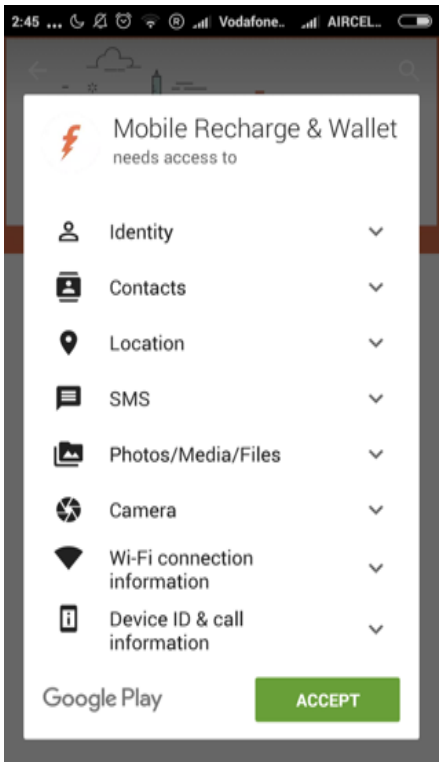
Capital float seeks permission to find the accounts on the device. The app reads calendar and confidential information and can also add or modify calendar events and can send e-mails to guests without the owner's knowledge. It seeks access to read and modify the contacts, can read the contents of the SD card used in the device and can modify or delete its contents.

Privacy Policy

The policy states that the company is strongly committed to protect the privacy of its users and has taken all necessary and reasonable measures to protect the confidentiality of the user's information and its transmission through the Internet. It provides for the collection of the user's information. In its non-disclosure clause, the policy pledges that it shall not sell or rent the information collected from the user to anyone. The policy provides for the exceptions where the company will disclose the user's personal information. It may be disclosed to government or other statutory bodies with appropriate authorization, for complying its legal obligations as per the policy, to its agents in strict code of confidentiality, or to its related or group companies including its subsidiaries. "Capital Float takes the security of its User's information rather seriously. Capital Float protects the User's information using bank-level data security: 128 bit-encryption and a Secure Sockets Layer (SSL) protocol." It retains user's data as long as the user account is active or as needed to provide service to the user. It further states that it has made every effort to ensure that its privacy policy adheres with the applicable laws.

5. FreeCharge

FreeCharge was acquired by Snapdeal on April 8th, 2015. This app provides a gateway for online recharges, payment of post-paid mobile bills, landline bills, data card and DTH recharge. It provides an online wallet and claims to be the most convenient wallet for making day-to-day transactions. Money can be transferred to the wallet using debit/credit card or net banking.



Permission Details

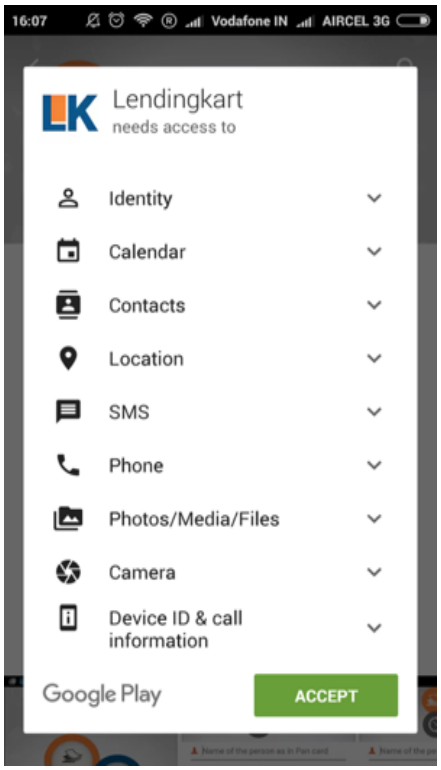
The FreeCharge app seeks permission prior to download to find out the account on the device, add or remove accounts. It seeks permission to access contacts (read and modify), location, SMS, contents of the SD card (modify or delete), device ID and call log information, and others such as creating accounts and setting passwords, preventing phone from sleeping, etc.

Privacy Policy

There is no privacy policy attached in the download page of the app.[35]

6. Lendingkart

The android version of the Lendingkart app allows users to complete loan applications. This app can be used to fill in application forms for new loans and submit required pdf documents as proofs. Users also get a chance to review their application status.



Permission Details

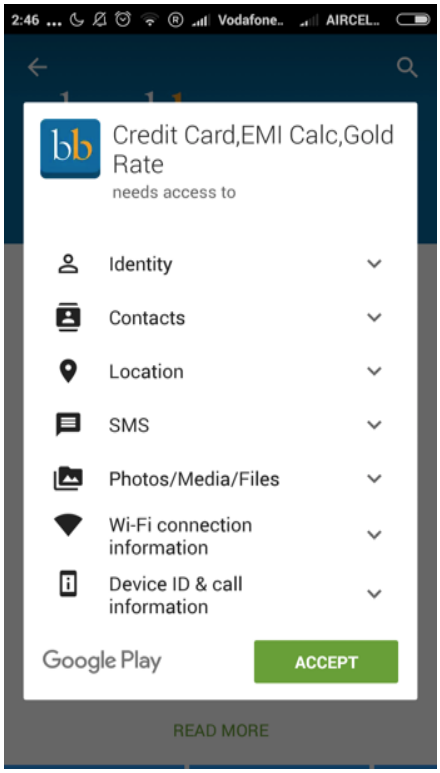
Lendingkart seeks permission to use the accounts on the device, calendar information, contact information, device location, SMS, and multiple files on the device such as images, audios and videos. It allows the app to determine the phone number and device IDs.

Privacy Policy

There is no privacy policy attached in the download page of the app. [36]

7. BankBazaar.com

BankBazaar.com is an app that allows users to compare various financial products like credit cards, home loans, personal loans, car loans and fixed deposits offered by different banks. It helps the users to choose a card, loan or deposit account that is best suited for their interest. The app is loaded with user friendly features like the loan EMI calculators and the Loan Eligibility Calculators for the banks like HDFC, Citibank, Axis Bank, SBI and ICICI Bank. The status of the application can be tracked in the app.



Permission Details

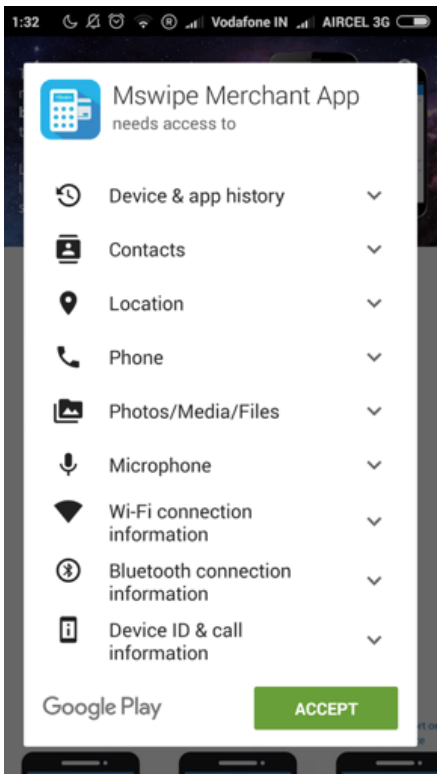
BankBazaar seeks permission to use the accounts on the device, access the contact information, the device's location, SMS and multiple files on the device such as images, audios and videos. It also uses device ID and call information.

Privacy Policy

It states that the company acknowledges the expectation of its customers with regard to privacy, confidentiality and security of their personal information that resides with the BankBazaar. It defines the personal information by stating that it means "any information that relates to the natural person, either directly or indirectly, in combination with other information available or likely to be available with the BankBazaar, that is capable of identifying such person. This is stated in the 'express consent' that the app takes from its user before installing the app. The privacy policy also states the purpose and usage of the of the personal information collected by the app. BankBazaar does not disclose sensitive personal data or information about the user except as directed by the law or as per mandate received from the customer or applicant. It provides exceptions upon which the personal information would be disclosed such as to help complete a transaction initiated by the user, or to perform support services through a third party service provider, provided it conforms to the privacy policy and prior consent of the user is obtained to do so.[37]

8. Mswipe Merchant App

Mswipe Technologies Pvt. Ltd. is the parent company that also owns the Mswipe app. It is a universal merchant app which works with all Mswipe terminals. It accepts card payments anywhere using this app in an android phone. It deals as a merchant acquirer and mobile POS solution provider.



Permission Details

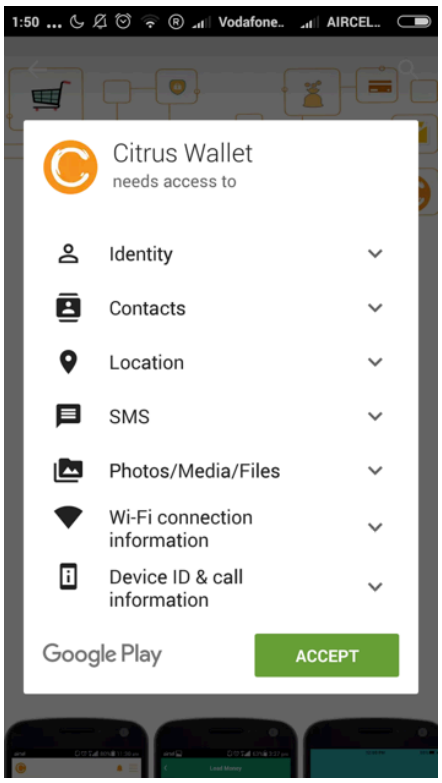
Mswipe seeks permission to find the accounts on the device. It reads calendars and confidential information and can also add or modify calendar events as well as send e-mails to guests without the user's knowledge. It seeks access to read and modify the contacts, read the contents of the SD card used in the device and to modify or delete its contents. It also seeks access to allow the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices.

Privacy Policy

The download/install page has a feature for privacy policy but upon opening the page it shows the disclaimer stating the acceptance of the terms of the company, provisions of service, proprietary rights. However, it does not mention the privacy protection of the customer.[38]

9. Citrus Wallet

Citrus Wallet is a financial technology and mobile wallet company with over 21 million users. It operates in the field of mobile payments and as a payment gateway. The app provides an online wallet for secured money transfer. It can transfer money using mobile numbers. It is known for allowing the splitting bills amongst friends.



Permission Details

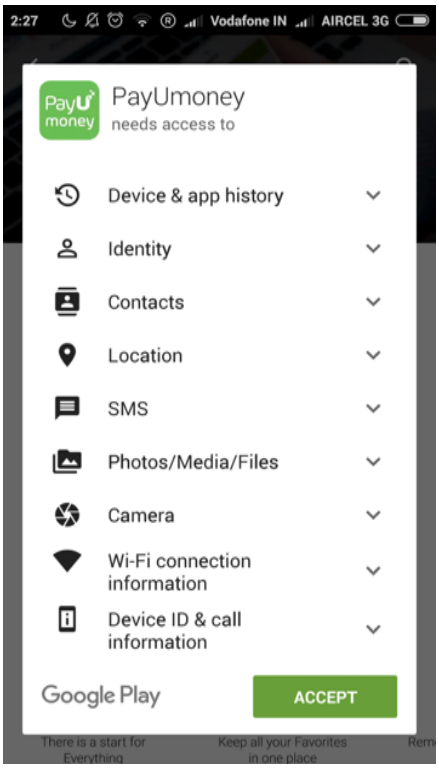
Citrus Wallet requires access to use the accounts on the device, the contact information, the device's location, SMS, and multiple files on the device such as images, audios and videos. It also uses device ID and call information.

Privacy Policy

It states that the privacy policy for the app is published in accordance with the provisions of Rule 4(1) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which requires the publishing of a privacy policy for handling of or dealing with personal information including sensitive personal data or information. The policy states the use of information for access to site and the services of Citrus. It does not sell or rent the personal information of the user. It states the they shall disclose the personal information of the user in order to fulfil their legal obligation. [39]

10. PayU Money

PayUmoney app provides services for online mobile and DTH recharge and payment of bills. It records all the spending of the user in one place. It facilitates payment of gas bill for Adani Gas Limited and Mahanagar Gas Limited, electricity bill for BESCOM, Reliance Energy Mumbai, Southern Power Distribution Company of Telengana Ltd. It also acts as an online wallet for facilitating the process of payment.



Permission Details

PayU Money needs access to use the accounts on the device, the contact information, the device's location, SMS, and multiple files on the device such as images, audios and videos. It also uses device ID and call information.

Privacy Policy

There is no privacy policy attached in the download page of the app.[40]

Survey of Privacy Policies and Analysis Under Section 43A of Information Technology Act, 2000

For analyzing the privacy policies of the above-mentioned apps, four mandatory requirements under *Rule* 4 of the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* are formulated. The following tables explain whether the app providers have complied with the mandatory requirements under the *Information Technology Rules*.

1. Paytm

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	Yes
Informs about type to data collected	Yes
Informs about purpose of collection and usage of such data	Yes
Informs about disclosure of information	Yes
Informs about reasonable security practices and procedures	Yes
Intended recipient of information, name and address	Yes
Informs about data retention policies and agencies	No
Provides option to *opt in* or *opt out*	No
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	Yes

2. PolicyBazaar

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	Yes
Informs about type to data collected	Yes
Informs about purpose of collection and usage of such data	Yes
Informs about disclosure of information	Yes
Informs about reasonable security practices and procedures	No
Intended recipient of information, name and address	Yes
Informs about data retention policies and agencies	No
Provides option to *opt in* or *opt out*	No
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	No

3. Mobikwik

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	Yes
Informs about type to data collected	Yes
Informs about purpose of collection and usage of such data	Yes
Informs about disclosure of information	Yes
Informs about reasonable security practices and procedures	Yes
Intended recipient of information, name and address	Yes
Informs about data retention policies and agencies	Yes
Provides option to *opt in* or *opt out*	Yes
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	No

4. Capital Float

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	Yes
Informs about type to data collected	Yes
Informs about purpose of collection and usage of such data	Yes
Informs about disclosure of information	Yes
Informs about reasonable security practices and procedures	Yes
Intended recipient of information, name and address	Yes
Informs about data retention policies and agencies	Yes
Provides option to *opt in* or *opt out*	Yes
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	No

5. FreeCharge

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	No
Informs about type to data collected	No
Informs about purpose of collection and usage of such data	No
Informs about disclosure of information	No
Informs about reasonable security practices and procedures	No

Requirements under 43A	Existence
Intended recipient of information, name and address	No
Informs about data retention policies and agencies	No
Provides option to *opt in* or *opt out*	No
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	No

6. Lendingkart

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	Yes
Informs about type to data collected	Yes
Informs about purpose of collection and usage of such data	Yes
Informs about disclosure of information	Yes
Informs about reasonable security practices and procedures	Yes
Intended recipient of information, name and address	Yes
Informs about data retention policies and agencies	No
Provides option to *opt in* or *opt out*	No
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	Yes

7. BankBaazar.com

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	Yes
Informs about type to data collected	Yes
Informs about purpose of collection and usage of such data	Yes
Informs about disclosure of information	Yes
Informs about reasonable security practices and procedures	Yes
Intended recipient of information, name and address	Yes
Informs about data retention policies and agencies	No
Provides option to *opt in* or *opt out*	No
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	No

8. Mswipe Merchant App

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	No
Informs about type to data collected	No
Informs about purpose of collection and usage of such data	No
Informs about disclosure of information	No
Informs about reasonable security practices and procedures	No
Intended recipient of information, name and address	Yes
Informs about data retention policies and agencies	No
Provides option to *opt in* or *opt out*	No
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	No

9. Citrus Wallet

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	Yes
Informs about type to data collected	Yes
Informs about purpose of collection and usage of such data	Yes
Informs about disclosure of information	Yes
Informs about reasonable security practices and procedures	Yes
Intended recipient of information, name and address	Yes
Informs about data retention policies and agencies	Yes
Provides option to *opt in* or *opt out*	Yes
Provides for withdrawal of consent at anytime	Yes
Informs about Grievance Officer	Yes

10. PayU Money

Requirements under 43A	Existence
Clear and accessible statements of practice and policies	No
Informs about type to data collected	No
Informs about purpose of collection and usage of such data	No
Informs about disclosure of information	No
Informs about reasonable security practices and procedures	No

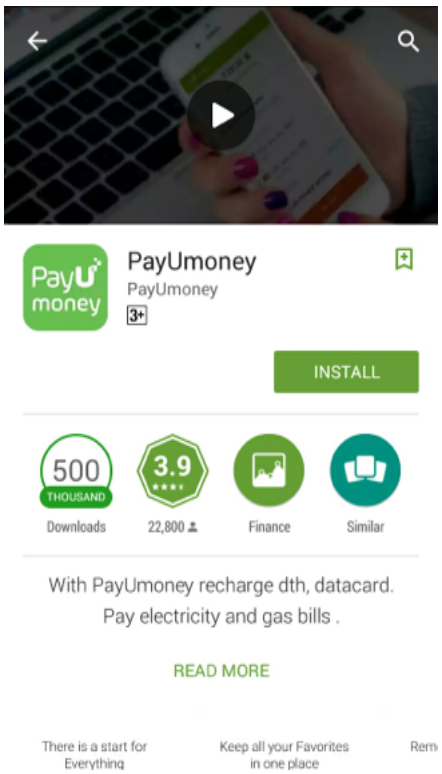
Requirements under 43A	Existence
Intended recipient of information, name and address	No
Informs about data retention policies and agencies	No
Provides option to *opt in* or *opt out*	No
Provides for withdrawal of consent at anytime	No
Informs about Grievance Officer	No

Conclusion

The above-mentioned data is examined under the requirements of the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011*. The survey is conducted with the help of the apps contained in 'Google Play not informing their users about their privacy policy; namely, FreeCharge, Mswip Merchant App and PayU Money. Out of the 10 apps analyzed, '*Citrus Wallet*' app is the only one that complies fully with all the criteria mentioned in the Rules. No other apps have provided provision for withdrawal of consent.

In the above-mentioned analysis, 3 out of the 10 fintech companies have not provided the information regarding the disclosure of the 'sensitive personal information'. In protection of the sensitive personal information, disclosure of the personal data retained by the service providing company becomes a major concern for the data provider. For example, the privacy policy of '*BankBaazar*' provides that it reserves the right to communicate the personal information to any third party and if the disclosure of such information is *necessary or appropriate under the law* for the time being in force.

In the Indian market, the compliance of the privacy policies with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 does not affect the download rate of these applications. For example, the PayUmoney App has neither provided privacy policy prior downloading nor after downloading the app.



The picture shows that there has been over 500 Thousand downloads despite not providing any privacy policy prior downloading the App.

This paper makes an effort to assess the ways in which mobile apps in India are implicated in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. This is important to explore considering India's recent wave of digitization in the service sector, which places the personal privacy and security of individual users at considerable risk. The general finding here is that the majority of the fin tech apps assessed in this report do not provide a provision for withdrawal of consent or the information regarding the disclosure of the 'sensitive personal information' belonging to the users. This poses a genuine concern with regards to the digital privacy and security of app users. It is important that users remain aware of their digital privacy rights under national legislation and to remain cautious with regards to which digitized services they choose to trust with their personal information. Looking forward, it would be beneficial to understand how laws and policies can be improved to apply more directly to smartphone apps. It would also be useful to encourage public awareness of digital security and privacy protection to the Indian app users. This would affect their decisions to download and use certain apps, ideally incentivizing mobile app companies to implement and comply with more rigid privacy policies for their users.

ENDNOTES

1. KPMG: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/FinTech-new.pdf
2. *Id.*
3. *Id.*
4. *Id.*
5. RBI 2P2 Consultation Paper, https://rbidocs.rbi.org.in/rdocs/content/pdfs/CPERR280416.pdf
6. *Id.*
7. *Id.*
8. *Id.*
9. SEBI Crowdfunding consultation paper, http://www.sebi.gov.in/cms/sebi_data/attachdocs/1403005615257.pdf
10. *Id.*
11. *Id.*
12. *Id.*
13. Krishna, https://yourstory.com/2016/07/india-stack/
14. *Id.*
15. Nilekani, http://indianexpress.com/article/opinion/columns/the-coming-revolution-in-indian-banking-2924534/
16. FTC Guide, https://www.ftc.gov/news-events/press-releases/2012/09/ftc-publishes-guide-help-mobile-app-developers-observe-truth
17. *Id.*
18. OAIC practice guide, https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-for-mobile-app-developers.pdf
19. *Id.*
20. *Id.*
21. *Id.*

22. *Id.*
23. GSMA mobile privacy principles, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf
24. *Id.*
25. *Id.*
26. "Clarification on Information technology Rules, 2011 under section 43A of the Information Technology Act, 2000" Press Information Bureau, Govt. of India, Ministry of Communication and Information and Technology, available at http://deity.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf, last visited 1st August 2016.
27. Section 43A, Information Technology Act, 2000.
28. "Access to Sensitive Personal Information under New IT Rules Only with Checks and Balances: Clarifies DIT", Press Information Bureau, Govt. of India, Ministry of Communication and Information Technology, 10 May 2011. Available at http://deity.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf last visited 1st August 2016.
29. Rule 3 (i) to (viii), Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
30. Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
31. Rule 5(2) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
32. Privacy Policy, Paytm, available at https://paytm.com/privacy-policy.html.
33. Privacy Policy, PolicyBazaar, available at https://www.policybazaar.com/legal-and-admin-policies/.
34. Privacy Policy, Mobikwik, available at https://www.mobikwik.com/privacypolicy.
35. Google Play Store download page, FreeCharge (no privacy policy attached), available https://play.google.com/store/apps/details?id=com.freecharge.android&hl=en.
36. Google Play Store download page, Lendingkart (no privacy policy attached), available https://play.google.com/store/apps/details?id=com.LendingKart&hl=en.
37. Privacy Policy, BankBaazar.com, available at https://www.bankbazaar.com/privacy-policy.html.
38. Disclaimer Page (shows terms and conditions), Mswipe (privacy policy redirects to disclaimer page), available at https://www.mswipe.com/disclaimer.html.
39. Privacy Policy, Citrus Wallet, available at http://www.citruspay.com/citrus-privacypolicy.html.
40. Google Play Store app download page, PayU Money (no privacy policy attached), available at https://play.google.com/store/apps/details?id=com.payu.payumoney&hl=en.