FinTech in India

A study of privacy and security commitments

April, 2019

Authored by (in alphabetical order) **Aayush Rathi** and **Shweta Mohandas**

Edited by **Elonnai Hickok**

Privacy policy testing by **Anupriya Nair**

Visualisations by **Saumyaa Naidu**

Supported by **The William and Flora Hewlett Foundation**

The Centre for Internet and Society (CIS), India
https://cis-india.org

Table of contents

Introduction

Fintech, a contraction of financial technology, represents the latest iteration of the embeddedness of technology within the delivery of financial services.[1] What distinguishes the current wave of the marriage of financial services and technology is not so much the array of new financial products and business models that have been devised as it is about *who* delivers them (i.e. not just incumbent financial institutions) and their availability at the retail and wholesale levels. Also distinguishing the so called 'fintech revolution'[2] is the utilisation of rapidly developing information and communication technologies in the delivery of financial services[3].

It has been estimated that the payments in India made through digital means which was USD 50 billion in 2016, would exceed USD 500 billion by 2020.[4] The growth of the fintech sector in India can be attributed to the growth of mobile technology and the mobile connectivity.[5] A study conducted by Deloitte in 2016 revealed that India has over a billion mobile phones, 330 million internet users and 240 million smartphones.[6] The convenience that mobile technology brought resulted in the growth of services such as internet banking, mobile banking and payment apps, and peer to peer lending. The banks and the government also encouraged the use of these services and advocated towards a cashless economy.[7] A significant impetus to fintech's growth was the November 2016 decision by the Government of India to discontinue the use of INR 500 and INR 1,000 currency notes in its demonetisation drive.[8] The cash crunch led to the convenience of instant services and money transfer being one of the main attractions for consumers. Subsequently, a report by PwC and Startupbootcamp identified that the number of fintech startups in India were around 1,500,

[1] Arner D et al (2015) The evolution of fintech: a new post-crisis paradigm. The University of New South Wales (UNSW) and the University of Hong Kong, UNSW Law Research Paper No. 2016-62, Hong Kong, Sydney

[2] Gupta, Bejoy D. "Opinion | The promise of fintech revolution." livemint. Retrieved from:https://www.livemint.com/Opinion/3mfGEc84q7n8xfIufMvmbJ/Opinion--The-promise-of-fintech-revolution.html

[3] Financial Stability Implications from FinTech. Financial Stability Board. 2017. Retrieved from:http://www.fsb.org/wp-content/uploads/R270617.pdf

[4]Digital Payments 2020. (2016, July). The Boston Consulting Group. Retrieved from:http://image-src.bcg.com/BCG_COM/BCG-Google%20Digital%20Payments%202020-July%202016_tcm21-39245.pdf

[5] ibid.

[6] Banking on the Future: Vision 2020. (2016, September 16). Deloitte. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-deloitte-bankingcolloquium-thoughtpaper-cii.pdf

[7] The Hon'ble Finance Minister, in his budget speech announced several activities for the promotion of digital payments including setting a target of 2,500 crore digital payment transactions in FY 2017-18, through Unified Payments Interface (UPI), Unstructured Supplementary Service Data (USSD), Aadhar Pay, Immediate Payment Service (IMPS) and Debit Cards.http://meity.gov.in/digidhan

[8]Panchal, S."Demonetisation gives a boost to banks, fintech companies". Forbes India. Retrieved from:http://www.forbesindia.com/article/the-demonetisation-debate/demonetisation-gives-a-boost-to-banks-fintech-companies/45111/1

half of which were set up in 2016-2017.[9] In a similar vein, another step towards the growth of fintech was the introduction of the Unified Payments Interface (UPI)-based payment system. The UPI, developed by the National Payments Corporation of India, provides for instant and real time mobile to mobile money transfer between participating banks.[10]

Fintech apps with their easy to use interfaces and services such as QR code reading and accounts linked to mobile numbers, are now said to be a viable option for individuals across India from different walks of life to send and receive money.[11] However the unprecedented growth of this sector with a number of players that have an amorphous nature (not banking entities) has concomitantly come with regulatory challenges around *inter alia* privacy and security concerns. For instance, A survey of 1300 senior executives in the global financial services, and fintech industries revealed that 54% of respondents identified privacy and data protection as barriers to fintech innovation.[12] This is especially important due to the centrality of information to the dispensation of financial services[13] leading the data-heavy nature of operationalising fintech services.

Research overview

Objective

In India, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (subsequently referred to as SPD/I Rules) framed under the Information Technology Act, 2000 (subsequently referred to as IT Act) make privacy policies a ubiquitous feature of websites and mobile applications of firms operating in India. Privacy policies are drafted in order to allow consumers to make an informed choice about the privacy commitments being made vis-à-vis their information, and is often the sole document that lays down a companies' privacy and security practices.[14]

The objective of this study is to understand privacy commitments undertaken by fintech companies operating in India as documented in their public facing privacy policies. This exercise will be useful to understand what standards of privacy and security protection fintech companies are committing to via their organisational privacy policies. The research will do so by aiming to understand the alignment of the privacy policies with the requirements mandated under the SPD/I Rules. Contingent on the learnings from this

[9]Fintech Trends Report 2017.PricewaterhouseCoopers. Retrieved from:https://www.pwc.in/assets/pdfs/publications/2017/fintech-india-report-2017.pdf
[10]What's Driving India's Fintech Boom? (2010,February 11).Retrieved from:http://knowledge.wharton.upenn.edu/article/whats-driving-indias-fintech-boom/
[11]Demonetisation effect: Digital payments gain new momentum.PWC India. Retrieved from:https://www.pwc.in/consulting/financial-services/fintech/fintech-insights/demonetisation-effect-digital-payment-gain-new-momentum.html
[12] Fintech Trends Report 2017.PricewaterhouseCoopers. Retrieved from:https://www.pwc.in/assets/pdfs/publications/2017/fintech-india-report-2017.pdf
[13] Puschmann, T. Bus Inf Syst Eng (2017) 59: 69. https://doi.org/10.1007/s12599-017-0464-6
[14] Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 471-478). ACM.

exercise, trends observed in fintech companies' privacy and security commitments will be culled out.

Methodology

The research studies the publicly available privacy policies from the websites of 48 fintech companies operating in India. The privacy policies were assessed against a template enumerating the privacy policy requirements mandated by the SPD/I Rules. The template is designed akin to a checklist comprising each requirement that is required to be complied with by "body corporates". These requirements are re-phrased as questions posed to the content of the privacy policy (Annexure 1), and in some instances the terms of service, with the output then being one of three responses - 'Yes', 'No' or 'Partially'. This testing template has been borrowed from a study undertaken by the Centre for Internet and Society to assess the organisational privacy standards of Telecommunications (TSP) and Internet Service Providers (ISP).[15]

Scope

Fintech being a loosely used term, the Report of the Inter-Regulatory Working Group on FinTech and Digital Banking[16] is used to outline some overarching service types. Taking cues from the taxonomy of the Indian fintech industry provided under Paragraph 3.1 of the Working Group report, the broad categorisations that are carved out for this study are: (a) Payment gateways, (b) Payment gateway aggregators, (c) Mobile and online wallets, (d) Digital payments banks, (e) Peer-to-peer lending platforms and (f) Miscellaneous entities that share features of the above categorisation (but could not necessarily be bucketed into any). It must be noted that these categorisations and the firms falling within these categorisations form only a part of the offerings that can be found within the fintech industry. Moreover, this study treats privacy policies at face value and does not look at a more rounded understanding of privacy commitments by addressing questions around privacy by design. Similarly, a more complete understanding of security commitments is precluded that may have been possible through rigorous security testing of the websites and applications of firms operating in the fintech space.

[15] A Study of the Privacy Policies of Indian Service Providers and the 43A Rules.(2015, 12 January). Retrieved from:https://cis-india.org/internet-governance/blog/a-study-of-the-privacy-policies-of-indian-service-providers-and-the-43a-rules

[16] Report of the Working Group on FinTech and Digital Banking.(2018, February 8).Reserve Bank of India. Retrieved from:https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=892

Privacy policy snapshots

Clear and accessible statements of its practices and policies

Interpretation

Rule 4 of the SPD/I Rules mandates that a body corporate dealing with or handling the information (a "data controller") of an information provider (a "data subject") shall effect a privacy policy that binds the data controller to dealing with the information in a manner prescribed under the SPD/I Rules. It is further required that the privacy policy should be published on the website of the data controller and that the policy should be "clear and easily accessible".

However, the SPD/I Rules are silent on the specific requirements of what would constitute a "clear and accessible" privacy policy. In the absence of this specification, for the purpose of this research, "accessibility" can be understood to mean the number of clicks that are required to access the data controller's privacy policy. As a proxy, a privacy policy is accessible if it is linked to on the homepage of the data controller's website and the text of the hyperlink adequately indicates so. The threshold for "clarity" is met if the privacy policy states the data controller's practices in dealing with the data subject's information in language that can be expected to be comprehended by a data subject being fluent in English and does not require prior legal or technical knowledge to be comprehended.[17]

Testing Results

Whether the privacy policy is accessible through the main website of the body corporate?

Image 1.1

[17] For a survey/quiz based approach that tested privacy policy comprehension, see *Disclosures in privacy policies: Does notice and consent work?,* Rishab Bailey, Smriti Parsheera, Faiza Rahman, Renuka Sane. December 2018. A survey of 155 undergraduate and graduate respondents across five colleges around New Delhi (administering education in English) was undertaken that tested the quality of privacy policies of five popular online services in India from the perspective of access and readability.

Whether the privacy policy is mentioned or included in the terms and conditions of all document of the body corporate that collects personal information?

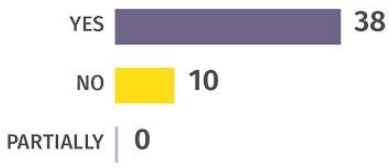

Image 1.2

Whether the privacy policy can be comprehended by persons without legal and technical knowledge?

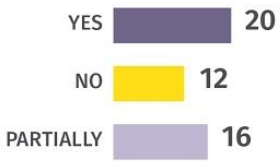

Image 1.3

Sample 'yes' excerpt:

"Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing a song in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting"[18]

Sample 'no' excerpt:

"The rights and remedies available under this Policy may be exercised as often as necessary and are cumulative and not exclusive of rights or remedies provided by law. It may be waived only in writing. Delay in exercising or non-exercise of any such right or remedy does not constitute a waiver of that right or remedy, or any other right or remedy."[19]

[18] Privacy Policy. Google Pay. Retrieved from: https://policies.google.com/privacy
[19] Privacy Policy. Capital Float. Retrieved from: https://www.capitalfloat.com/privacy-policy

Sample 'partially' excerpt:

"Itz Cash Card Limited strive to keep the level of security state-of-the-art at all times and takes steps to protect your personally identifiable information and has adopted generally accepted standards of technology in order to protect your personally identifiable information. We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input. We store information gathered on secure computers. We use advanced security technology to prevent our computers from being accessed by unauthorized persons."[20]

Observation

Placement of privacy policies

Most fintech companies have adopted the now standard practice utilised for placing privacy policies on websites - that of providing a hyperlink to the privacy policy at the bottom of the main page of their website. The text of the hyperlink, however, is usually displayed in font smaller than that used for the rest of the page making it more challenging to locate prior to using the services provided by the data controller.

Further, for some of the companies the privacy policy had to be located in the terms of service[21] or under separate categories such as 'legal agreements', 'key policies', 'security', further making the privacy police more inaccessible. Resultantly, we anticipate that unless the data subject is specifically looking for the privacy policy, it is unlikely for the privacy policy to be perused in the usual course of a data subject's usage of the services of the fintech provider.

Type and acknowledgment of personal or sensitive personal data/information collected

Interpretation

Section 2(1)(i) of the IT Act defines personal information as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." Rule 3 of the SPD/I Rules further demarcates sensitive personal data/information as personal information which consists of passwords; financial information, physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information. Two other broad categories are included - any related details provided to the body corporate, and any information received by the body corporate in relation to the categories listed above. Rule 4(1)(ii) further elaborates that the privacy policy must specify the type of personal or sensitive personal data or information collected.

[20] Privacy Policy. Itzcash. Retrieved from: http://itzcash.com/privacy-policy/
[21] See, for example http://www.hotremit.com/terms.html#privacy. Also see https://paytm.com/about-us/our-policies/#tandc and https://www.i-lend.in/index.html

Testing Results

Whether the privacy policy mentions all categories of personal information including SPD/I being collected?

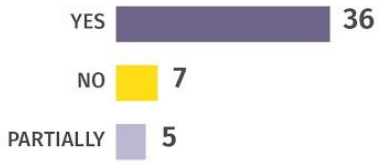

Image 2.1

Sample 'yes' excerpt:

"INFORMATION THAT WE COLLECT AND THAT YOU PROVIDE
I. PERSONAL INFORMATION
Personal Information means and includes all information that can be linked to a specific individual or to identify any individual, such as:
a. Your full name, address, e-mail address, telephone number, date of birth and bank or payment card details and any proof of Your identity and/or address that we may request;
b. Details of any transactions that You carry out through our Website or application using Your Oxigen account and of the fulfilment of Your requests;
c. Details of any credit, debit or other card used by You for transactions;
d. Details of any bank account (including but not limited to, account holder, account name, account number, sort code, online banking PIN, Transaction Authentication Number "TAN" and password, available balance and transaction history of Your bank account), ITR, TAX certificates or any other income documents as necessary by Us;
e. Any correspondence sent by You to Us;
f. Survey that You complete through the Website or based on our request;
g. Your participation in any promotion sponsored by Us;
h. Calls that we make to You or You make to Us;
i. Information collected through Cookies;
j. Your IP address, log-in times, operating system and browser type;
k. Details of Your visits to our Website/ mobile application including, but not limited to, Traffic Data, location data, weblogs and other communication data, whether this is required for Our own billing purposes or otherwise and the resources that You access whilst visiting Our Website or mobile application."[22]

[22]Privacy Policy. Oxigen.Retrieved from http://www.myoxigen.com/assets/pdf/Oxigen%20Privacy%20Policy.pdf

Sample 'no' excerpt:

"We store your email ID so that in future we can mail you a backup of your Chillr data upon receiving a request from you."[23]

Sample 'partially' excerpt:

"We may permit use of your name, e-mail addresses, addresses, telephone and fax numbers and other relevant details for our own marketing or we may permit others to access the same for marketing."[24]

Whether the privacy policy explicitly specifies the type of SPD/I being collected?

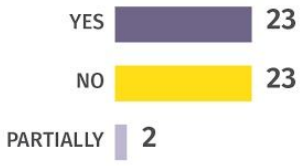

Image 2.2

Sample 'yes' excerpt:

"Upon signing up on Our Website, You are required to provide Us with certain basic mandatory information inter-alia Your name, title, physical address, phone number, e-mail address, details regarding Your credit/debit Card and other sensitive information."[25]

Sample 'no' excerpt:

"Personal Information means and includes all information that can be linked to a specific individual or to identify any individual, such as name, address, mailing address, telephone number, email ID, credit card number, cardholder name, card expiration date, information about your mobile phone, DTH service, data card, electricity connection, Smart Tags and any details that may have been voluntarily provide by the user in connection with availing any of the services on Paytm."[26]

Sample 'partially' excerpt:

"We may permit use of your name, e-mail addresses, addresses, telephone and fax numbers and other relevant details for our own marketing or we may permit others to access the same for marketing. However, no informations relating to your personal bank accounts or personal investments will be revealed to any third party without your consent unless required by law."

[23] Privacy Policy. Chillr.Retrieved from https://chillr.com/privacy.html
[24] Privacy Policy. Direcpay. Retrieved from http://www.direcpay.com/direcpay/dpprivacypolicy.jsp
[25]Privacy Policy. Oxigen.Retrieved from http://www.myoxigen.com/assets/pdf/Oxigen%20Privacy%20Policy.pdf
[26] Privacy.Paytm.Retrieved from https://pages.paytm.com/privacy.html

Observations

Lack of specificity

While most fintech companies in the sample explicitly specified personal information that was being collected, fewer privacy policies contained categorical provisions segregating the *sensitive* personal information that was being collected.

Another trend that emerged pertained to the manner in which the information being collected is detailed. In nearly all instances, the listing of collected information was not exhaustive with the usage of terminology such as 'etc.', 'inter alia', 'information such as', being commonplace. Another terminology that is often incorporated to broaden the ambit of information being collected is the definition of personal information as any information that may be provided by the user. This squarely places the onus of restricting information collection on the data subject further compounding the handicaps users face in ascertaining the information that that firms are seeking to collect because of the illustrative nature of the listing of information.

Option to not provide information and withdrawal of consent

Interpretation

Rule 5(7) states that the data controller should inform data subjects prior to the collection of information (including sensitive personal data or information) that they have an option to not provide the data or information. The rule also specifies that the individual must also be informed that he/she has an option to subsequently withdraw consent from the use of the data or information collected by the data controller.

Testing Results

Whether the Privacy Policy specifies that the user has the option to not provide information?

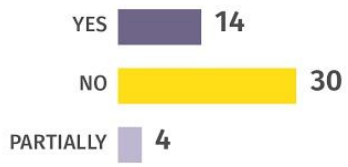

Image 3.1

Sample 'yes' excerpt:

"The User always has the option to not provide information by choosing not to use a particular service or feature."[27]

[27] Privacy Policy. I2ifunding. Retrieved from:https://www.i2ifunding.com/privacy-policy

Sample 'no' excerpt:

For privacy policies that returned a 'no' response, the privacy policies did not specify that the user has the option to not provide information.

Sample 'partially' excerpt:

"We provide you the opportunity to opt-out of having your Personal Information used for certain purposes. For example, if you purchase a product/service but do not wish to receive any additional marketing material from us, you can indicate your preference on our order form. If you no longer wish to receive our newsletters and promotional communications, you may opt-out of receiving them by following the instructions included in each newsletter or communication or by emailing us at support@faircent.com. We also offer you an opportunity to opt-out of certain communications through the account management screen. If you need assistance you may contact us at support@faircent.com."[28]

Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?

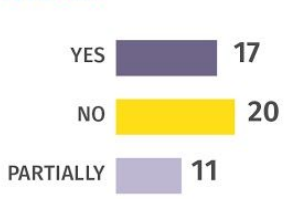

Image 3.2

Sample 'yes' excerpt:

"(ii) The User can at any time while availing the services or otherwise, withdraw his/her consent given previously to PayU for collecting, receiving, possessing, storing, dealing or handling Information of the User, by sending us your request by email on privacy@payu.in. In such case, PayU will unfortunately not be in a position to provide the Services to you."[29]

Sample 'no' excerpt:

For privacy policies that returned a 'no' response, the privacy policies did not specify that the user has the option to subsequently withdraw consent.

Sample 'partially' excerpt:

"We provide you the opportunity to opt-out of having your Personal Information used for certain purposes. For example, if you purchase a product/service but do not wish to receive any additional marketing material from us, you can indicate your preference on our order form. If you no longer wish to receive our newsletters and promotional communications, you may opt-out of receiving them by following the instructions included in each newsletter or communication or by emailing us at support@faircent.com. We also offer you an opportunity

[28]Privacy Policy. Faircent. Retrieved from: https://www.faircent.com/privacy-policy
[29] Privacy Policy. PayUmoney. Retrieved from: https://www.payumoney.com/privacypolicy.html

to opt-out of certain communications through the account management screen. If you need assistance you may contact us at support@faircent.com."

Observation

Option to opt-out of further processing

The phrasing of opt-out clauses generally only provided users with the limited right to stop receiving correspondence from the data controller (promotional calls and emails, newsletters etc.). The option to opt-out, then, is restricted only to certain uses of a user's information.

Fintech providers, generally, have equated users opting out of the use of their personal information with a complete termination of services. . The same way as consent should not mean that the user consents to all the forms of data processing, a data subject must also have the option to withdraw her consent from certain types of processing while still enjoying the services she has consented to. For example, she could withdraw her consent from the use of her previously shared biometric information from being used by a Fintech company, while still allowing for the use of her financial information for services that only require the latter. How Fintech companies have structured their privacy policies generally do not allow for this possibility.. Privacy policies, then, should first clearly state how the users data is being processed and shared as well as provide the users to withdraw their consent from certain types of processing and still enjoy the services she consents to.

Grievance officer

Interpretation

Rule 5(9) of the SPD/I Rules prescribe that data controllers are required to have a grievance redressal mechanism in place vis-a-vis the data controller's privacy practices. This entails the provision of a grievance officer whose contact information is to be provided on the website. Further, the body corporate is required to address grievances in a "time bound" fashion within a maximum time-frame of 1 month. Consequently, another criteria we assessed was whether the procedural specificities of the grievance redressal mechanism were provided to enable the effective use of the redressal mechanism. This would entail providing information around recognition of receipt of the complaint by the grievance officer, binding the grievance officer to adhere to granular time milestones, appeals process etc.

Testing Results

Whether the privacy policy mentions the existence of a grievance officer?

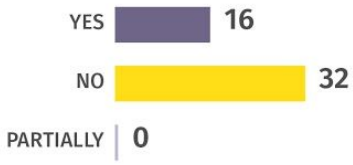

Image 4.1

Sample 'yes' excerpt:

"If you have any questions, or concerns about this Policy or any complaints or grievances about the manner in which we handle your personal information or the use of your personal information (in doing so acknowledging that we may be unable to provide you all or some of the services), please feel free to contact the Grievance Officer any time."[30]

Sample 'no' excerpt: For privacy policies that returned a 'no' response, the privacy policies did not mention a grievance officer.

Sample 'partially' excerpt: No privacy policies only partially mentioned the existence of a grievance officer.

Whether the privacy policy provides the contact information of the grievance officer?

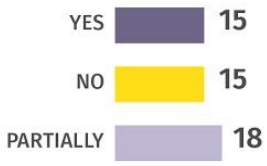

Image 4.2

Sample 'yes' excerpt:

"In accordance with Information Technology Act, 2000 and rules made there under, the name and contact details of the Grievance Officer is provided below:

Contact Name: Vishal Gupta

Email: grievanceofficer@phonepe.com"

Sample 'no' excerpt:

[30] Privacy.Paytm.Retrieved from https://pages.paytm.com/privacy.html

For privacy policies that returned a 'no' response, the privacy policies did not provide contact information of the grievance officer.

Sample 'partially' excerpt:

"If you have any questions, or concerns about this Policy or any complaints or grievances about the manner in which we handle your personal information or the use of your personal information (in doing so acknowledging that we may be unable to provide you all or some of the services), please feel free to contact the Grievance Officer any time."[31]

Whether the privacy policy provides details of the grievance redressal mechanism?

Image 5.1

Sample 'yes' excerpt:

""Level 4"

In accordance with Information Technology Act, 2000 and rules made there under, the name and contact details of the Grievance Officer is provided below:

Contact Name: Vishal Gupta

Email: grievanceofficer@phonepe.com

Address- Ashford Park View, Site No - 9 Industrial Layout, Koramangala 3rd Block, 80 ft Road, Bangalore-560034, India.

Working hours: Mon-Fri 10 am to 7 pm

- Any Level 4 escalation email should contain the following information –
    - User's name
    - Registered contact number
    - Ticket number of the complaint registered by Level 1
    - Details of why the resolutions provided at previous levels were deemed unsatisfactory
- Resolution of Complaints:
    - We are committed to providing a first response within 24 hours of receiving the complaint.
    - We aim to resolve all Level 2 complaints within 3 business days. Any delay in

[31] Privacy Policy. Rubique. Retrieved from:https://www.rubique.com/privacy-policy

- the resolution time shall be proactively communicated to you"[32]

Sample "no" excerpt: For privacy policies that returned a 'no' response, the privacy policies did not provide details of the grievance redressal mechanism.

Sample "partially" excerpt:

"VIII. QUESTIONS OR CONCERNS

If you have any questions or concerns regarding our privacy policies, please send us a detailed message to privacy@instamojo.com, and we will try to resolve your concerns."[33]

Observation

Missing mechanisms

Insofar as grievance redressal is concerned, the starkest absence was that of the details about the grievance redressal mechanism seems. With respect to the requirement that the data controllers mention the existence of grievance officers, thirty two companies failed to not just provide a redressal mechanism but also failed to mention the existence of a grievance officer specific to the resolution of issues that data subjects may encounter vis-à-vis the data controller's privacy practices.

However with respect to the question of providing contact details of grievance officers a few of the companies did comply with this requirement partially by providing contact details of a person who could be contacted in case of any problem. Although they fail to specify what exact authority and responsibility that the person assigned has, in our study we considered it as a point of contact for grievances. For example CCAvenue's privacy policy reads, "If you have questions about CCAvenue.com privacy practices, please contact us at contact@ccavenue.com."[34] Similarly PayU Money's reads, "In the event that you encounter any person is improperly collecting or using information about Users, please contact us by emailing at support@payumoney.com".[35]

Purpose of collection and usage of information

Interpretation

The SPD/I Rules mandate that the privacy policies of data controllers collecting sensitive personal data or information must provide for the purpose for such collection and the subsequent usage of the SPD/I.[36] Harmoniously read with Rule 4(1)(iii), this requirement can be further to extended to information collected not limited to SPD/I. Further, the data controller is permitted to collect *information* only for a lawful purpose connected with the data controller's function or activity and only if it is considered necessary for that purpose.

---

[32] Privacy Policy.Phonepe. Retrieved from:https://phonepe.com/en/policy.html
[33] Privacy.Instamojo. Retrieved from:https://www.instamojo.com/privacy/
[34] Privacy Policy. CC Avenue. Retrieved from https://www.ccavenue.com/privacy.jsp
[35] Privacy Policy. PayU. Retrieved from:https://www.payumoney.com/privacypolicy.html
[36] Rule 4(1)(iii) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Further, the data controller can only use the *information* collected for the purpose for which it had been collected.

Along with the need to specify the purpose of collection Rule 5(4) of the SPD/I Rules require that the data controllers holding sensitive personal data or information shall not retain that information for longer than is necessary for the purpose for which the information may lawfully be used or is otherwise required under any other law. Apart from purpose limitation, Rule 5(6) also requires the data controller to provide the data subject with the ability to review as well as correct or amend the information provided to the data controller.

Testing Results

Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?

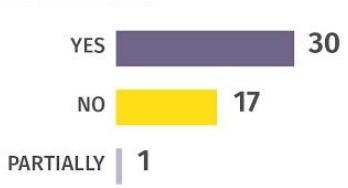

Image 6.1

Sample 'yes' excerpt:

"III. Usage of Your Personal Data

We use your Personal Data in our business activities for providing our or our partners' products/services and to perform, among other actions, the following:

1. to facilitate the transactions or report on these transactions;

2. to undertake research and analytics for offering or improving our products/services and their security and service quality;

3. to check and process your requirements submitted to us for products/services and/or instructions or requests received from you in respect of these products/services;

4. to share with you, updates on changes to the products/services and their terms and conditions;

5. to take up or investigate any complaints/claims/disputes;

6. to respond to your queries or feedback submitted by you;

7. to verify your identity for us to provide products/services to you;

8. to carry credit checks, screenings or due diligence checks as lawfully required by us;

9. to monitor and review products/services from time to time;

10. to undertake financial/regulatory/management reporting, and create and maintain various risk management models;

11. for conducting audits and for record keeping purposes;

12. for selective offers and promotions.

External processing: We may provide your personal information to our affiliates or other trusted businesses or persons or service providers engaged by us, or institutions that we partner with to assist us with providing you with products/services to better serve your needs and interests, based on your instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

We also use your Personal Data to fulfill the requirements of applicable laws/regulations and/or court orders/regulatory directives received by us."

Sample 'no' excerpt:

For privacy policies that returned a 'no' response, the privacy policies do not enumerates the purpose(s) for which information is collected.

Sample 'partially' excerpt:

"Personal Information which we share with our affiliates and/or third parties for marketing purposes, and providing contact information for such affiliates and/or third parties."

Whether the privacy policy makes explicit provisioning regarding the retention of users' information?

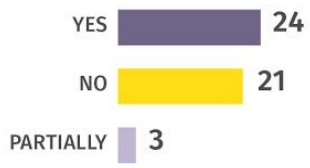

Image 6.2

Sample 'yes' excerpt:

"(i) BankBazaar will retain your information for as long as it is necessary for providing you the Services available on the Website or your request for termination of your account with BankBazaar, whichever is later.

(ii) Post termination of your account, BankBazaar may continue to use your anonymized data aggregated or in combination with anonymized data of other users. We use this aggregated anonymized data for data analysis, profiling and research purposes, for example to gain insights about our users and their profiles. We may keep your contact information along with

your application details (if any) for fraud prevention purposes and for the exercise/ defense of a legal claim or for providing evidence in legal proceeding(s)."[37]

Sample 'no' excerpt:

"Your personal data will be stored and collected by Policybazaar Insurance Web Aggregator Private Limited".[38]

Sample 'partially' excerpt:

"When You use the Website and the Service provided by Simpl on the Website, Simpl makes good faith efforts to provide You with access to Your Information and other relevant data, either to correct this data if it is inaccurate, or to delete such data at Your request, if it is not otherwise required to be retained by law or for legitimate business purposes."

Whether the privacy policy outlines a mechanism allowing users to review, correct and amend the information provided by the user?

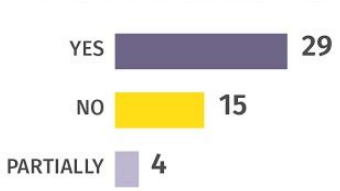

Image 6.3

Sample 'yes' excerpt:

"When you are signed in, you can always review, and update information. You can also review and control information saved in your account. You can also always export copy of content in your Account if you want to back it up."[39]

Sample 'no' excerpt: For privacy policies that returned a 'no' response, the privacy policies did not outline a mechanism allowing users to review, correct and amend the information provided by the user.

Sample 'partially' excerpt:

"We store all the transaction related information including amounts, remarks, location tags, pictures so that you can access your data even after changing your device."[40]

---

[37] Privacy Policy.Bankbazaar. Retrieved from: https://www.bankbazaar.com/mobile-app-privacy-policy.html
[38] Privacy Policy. Policybazaar. Retrieved from:https://www.policybazaar.com/legal-and-admin-policies/
[39]Privacy Policy. I2ifunding. Retrieved from:https://www.i2ifunding.com/privacy-policy
[40] Privacy.Chillr.Retrieved from: https://chillr.com/privacy.html

Observations

No purpose limitation

Most privacy policies that were studied contained provisions outlining the purposes behind the collection of information from the data subjects. Some of the common purposes outlined by fintech firms were that of utilising the information collected for: (a) providing services and enhancing service delivery, (b) communication of marketing and promotional material, (c) developing measures to protect both the data subjects and controllers against fraud and security threats, (d) aggregating information to undertake statistical analyses of user behavior. While outlining these purposes results in compliance with the SPD/I Rules and would return a 'yes' in this study, the observed trend was that of the lack of any granular particulars about what the constituents of these broad categories of purposes outlined.

This also hints at a lack of organisational motivations in specific determinations of the purpose of collection and processing of information. Overbroad purpose disclosures may have also become the norm owing to challenges in determining the proximity between the original purpose and new purpose that may arise owing to changing financial and/or technological logics in the fintech space. The lack of any instruction in legislation on the delta between original use and subsequent use is important to be highlighted here as well. The implications this practice has on individuals' right to privacy is further compounded when read together with the lack of segregation of sensitive personal information as outlined previously. In other words, the additional protection envisioned to be accorded to sensitive personal information is being diluted, as its collection and use is being treated with the same (dis)regard as other information.

Access and rectification

The SPD/I Rules require data controllers to provide a mechanism allowing users to access and rectify the information provided by the users. This is especially relevant as the data controllers are not accountable for the veracity of the information provided by the users. While some fintech companies provide their users with no such rights to access and rectification, those that do allow these rights to be exercised in one of two ways: either by looking at the information recorded in the user's profile settings and the other by sending a request to a designated email id. While the former provides users access to the information provided by them that is associated with their account, the contours of the latter are unclear.

Further, it is unclear if users have access to information about them that has been processed by data controllers that may not have been directly provided by the users (such as telemetric data, IP and location data etc.) but is still personal information insofar as the SPD/I Rules are concerned. While data controllers that collect this information seek to use this information in a form that is aggregated and anonymised, this practice is not just in abeyance of the SPD/I Rules buts also ignores the growing concerns around the assumed privacy-protecting power of anonymisation.

Data Retention

The SPD/I Rules require body corporates to explicitly state their data retention policy. The body corporates as data controllers store different personal and sensitive personal data. The privacy policies should ideally state the period for which the data is stored and how the data

is retained. In our study we observed that while some of the privacy policies expressly stated that the data would be retained even after the user chooses to delete their profile. Whereas some data controllers did not expressly state their retention policy, they did state that the data might be stored indefinitely in order to comply with law enforcement requirements. When data controller did not state their retention policy, it was unclear whether these agencies retain the data, even after the data subject has requested deletion of her account. This is highly problematic as some of the companies that did provide the user with the provision to withdraw consent did not clarify their data retention policy. It is to be noted that Rule (4) of the SPD/I Rules states that the companies should not retain the data longer than is required for the purpose for which it is collected or otherwise required by law. This provision has been interpreted by most data controllers to store the data indefinitely stating that the data is stored in order to comply with the government or law enforcement agencies. In the absence of a law that explicitly states the time after which the data should be deleted, data controllers also have no option but to account for all possible scenarios in which they may be obligated to provide information.

Disclosure of information

Interpretation

The SPD/I Rules govern the disclosure of such information to third parties and government agencies. The disclosure by body corporates to third parties requires prior permission from the provider of the information - this requirement is waived if a pre-existing contractual agreement between the data subject and the data controller, permitting such disclosure, already exists or if the disclosure is required to made in order to comply to a legal obligation. This contractual agreement, typically, is in the form of explicit provisions in either the privacy policy or the terms of service provided on the body corporate's website.

Disclosing information to legally mandated government agencies, however, does not require the provider's prior permission. However, the data controller is required to disclose information to a government agency only upon the furnishing of an authorised request to the data controller. Mirroring the phrasing in the text of Rule 6(1), a privacy policy is compliant only when it specifically commits to the procedure outlined specifically when disclosing information to legally mandated government agencies.

Testing Results

Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties?

Image 7.1

Sample 'yes' excerpt:

"(a). You hereby unconditionally agree and permit that the Freecharge Entities may transfer, share, disclose or part with all or any of Your Information, within and outside of the Republic of India to various Freecharge Entities, Third Party Service Providers / Partners / Banks and Financial Institutions for one or more of the Purposes, government agencies upon directions of such agency, or to any other third party as may be required under applicable law. In case of any Personal Information so transferred, shared, disclosed or parted with, We will contractually oblige the receiving parties of the Information to ensure the same level of data protection adopted by the Freecharge Entities is adhered to by the receiving party, subject to applicable law.

Sample 'no' excerpt: The privacy policies and that returned a 'no' response did not contain any provisions addressing the disclosure of information.

Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?

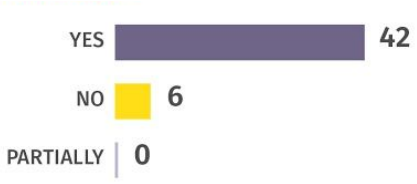

Image 7.2

Sample 'yes' excerpt:

[...]

(f). We reserve the right to disclose Your Information when required to do so by law or regulation, or under any legal obligation or order under law or in response to a request from a law enforcement or governmental agency or judicial, quasi-judicial or any other statutory or constitutional authority or to establish or exercise Our legal rights or defend against legal claims."[41]

[41] Terms and Conditions. Freecharge. Retrieved from: https://www.freecharge.in/termsandconditions

Sample 'no' excerpt: For privacy policies that returned a 'no' response, the privacy policies did not contain provisions relating to information disclosure to government agencies/LEA/IA.

Observation

Ambiguous taxonomy

Most privacy policies contained provisions speaking to the disclosure of personal information to third parties. Generally speaking, the third parties usually are: (a) affiliated or related entities, (b) law enforcement or (c) data processing service providers engaged by the data controller.

However, there is ambiguity in the terminology being used leading to a lack of clarity about what personal information could be shared with which third parties. For instance, it is often left undefined who "affiliates" are, and what entities are subsumed within the understanding of related entities within a group of companies. When it comes to data processing service providers, most privacy policies also only provide illustrative lists, leaving the data subjects guessing. For example, Amazon Pay's privacy policy indicates that third parties "include sending postal mail and e-mail, analyzing data, providing marketing assistance, processing payment transactions, verifying identity, fraud screening and providing customer service. [emphasis supplied]."

Sharing of personal information with law enforcement is also captured in most privacy policies, although no privacy policy that was studied provides any notice to the data subject prior to or post sharing information. Also, it is rare for privacy policy provisions to acquiesce to disclosing such information only when such requests adhere to the procedural requirements legitimising the request for information. For instance, PayTM's privacy policy clarifies that one of the circumstances in which personal information is shared is when "it is directed or required by legal/regulatory/statutory/governmental authorities under applicable laws/regulations though a legally obligated request."

Reasonable security practices and procedures

Interpretation

The SPD/I Rules require the body corporate to have implemented standard security practices and procedures commensurate to the information assets intended to be protected. These are further required to have been documented as a part of the body corporate's information security program and policies and should contain appropriate "*managerial, technical, operational and physical security control measures*". An international security standard that is used to illustrate these requirements is the IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements". The SPD/I Rules do not specify that this documentation be incorporated in the privacy policies; it is only mandated that the body corporates' privacy policies provide information pertaining to the reasonable security practices and procedures being implemented. The body corporate, then, is required to include as many details as possible in the privacy policy regarding the measures adopted to ensure the security of the information being collected and stored.

Testing Results

Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?

Image 8.1

Sample 'yes' excerpt:

"We adopt reasonable security practices and procedures, in line with international standard IS/ISO/IEC 27001, to include, technical, operational, managerial and physical security controls in order to protect your personal information from unauthorized access, or disclosure while it is under our control.

Our security practices and procedures limit access to personal information on need-only basis. Further, our employees are bound by Code of Conduct and Confidentiality Policies which obligate them to protect the confidentiality of personal information.

We take adequate steps to ensure that our third parties adopt reasonable level of security practices and procedures to ensure security of personal information.

We may retain your personal information for as long as required to provide you with services or if otherwise required under any law.

When we dispose of your personal information, we use reasonable procedures to erase it or render it unreadable (for example, shredding documents and wiping electronic media).

Internet Use - We maintain the security of our internet connections, however for reasons outside of our control, security risks may still arise. Any personal information transmitted to us or from our online products or services will therefore be your own risk. However, we will strive to ensure the security of your information. We observe reasonable security measures to protect your personal information against hacking and virus dissemination."[42]

Sample 'no' excerpt:

"Your account is protected by a password for your privacy and security. If you access your account via a third party site or service, you may have additional or different sign-on protections via that third party site or service. You must prevent unauthorized access to your account and Personal Information by selecting and protecting your password and/or other

[42] Airtel.(2019, March 20). Retrieved from: https://www.airtel.in/forme/privacy-policy/security-practices-and-procedures

sign-on mechanism. appropriately and limiting access to your computer or device and browser by signing off after you have finished accessing your account.

We endeavor to protect the privacy of your account and other Personal Information we hold in our records, but we cannot guarantee complete security. Unauthorized entry or use, hardware or software failure, and other factors, may compromise the security of user information at any time.

The Services may contain links to other sites. We are not responsible for the privacy policies and/or practices on other sites. When following a link to another site you should read that site's privacy policy."[43]

Sample 'partially' excerpt:

"The security of your Personal Information is important to us. When you enter sensitive information such as a credit card number on our registration or order forms, we encrypt that information using secure socket layer technology (SSL).

We follow generally accepted industry standards to protect the Personal Information submitted to us, both during transmission and once we receive it. However, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, while we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security."[44]

Observation

Security provisioning

Amongst the companies that made full or partial disclosures about the security practices being adopted, a trend that emerged was that of companies committing to using the Secure Sockets Layer (SSL) protocol to ensure confidentiality of the data subject's information. The SSL protocol, however, only provides protection during transport, and is deprecated by the Transport Layer Security (TLS) protocol. TLS, in comparison, is a considerably more secure protocol. It is pertinent to note that even the utility of TLS is limited only to communication encryption, and may still leave room for data to be compromised through other means such as insecure database configurations, or through other vulnerabilities that may be present in the application or infrastructure of a particular company.

The SPD/I Rules prescribe the adoption of the ISO/IEC 27001 standard to ensure compliance with the requirement of data controllers having "reasonable security practices and procedures" in place. The ISO/IEC 27001 standard can be thought of as an overarching suite of activities that provides organisations of all kinds with a managerial framework to address 'information security risks'. This allows for ensuring the security of information far beyond network security that SSL/TLS aids with, by factoring in inter alia physical and environmental security, communications and operations management etc.

[43] Instamoji. (2019, March 20). Retrieved from: https://www.instamojo.com/privacy/
[44] Faircent.(2019, March 20). Retrieved from: https://www.faircent.com/privacy-policy

Additional observations

Language as a barrier

All privacy policies, barring one, were provided solely in English; one firm - PhonePe - provided a privacy policy in both English and Hindi[45]. Even when the terms and conditions were provided in languages other than English, the privacy policy was still solely drafted in English.[46] With the growth of the digital economy, a multitude of Indians are using online services, and it is imperative that privacy policies be accessible and understandable to all users of the service. In the context of the fintech sector, accessibility to privacy policies takes on added significance given the fintech sector's avowed promise of increasing access to financial products to hitherto underserved sections of the society[47].

Fintech companies operating in India, then, should strive to look beyond the bare minimum prescription of the SPD/I Rules and ensure that the privacy policies are not just in English, but also in other Indic languages. The current provisioning is grossly insufficient given the linguist demographics of the Indian population: less than half the population recognises even Hindi as its first language.[48] While official data on English nativity is not available, estimates peg this number to be half of all English speakers in the country (~230,000 people)[49].

Readability

Like many jurisdictions, India ascribes to the 'notice-and-choice' regime of web-based privacy enforcement which requires that operators of electronic media provide to their users a notice of *inter alia* their data collection, storage and processing practises. In theory then, users can choose to accept these practices or not avail of the services. In practice, however, research shows that few consumers, if any, read online privacy policies, despite expressing concern about their online privacy.[50] Privacy policies are notoriously technical, long and infeasible for customers to peruse.[51] A few of the reasons for the impracticality is the placement of the policies (often at the end of the web page), the length, font and the language of the policies, as well as the lack of awareness about the contents of the

[45]Privacy Policy (hindi), PhonePe, Retrieved from:https://www.phonepe.com/hi/policy.html
[46] Consumer Terms and Conditions,Jio money, Retrieved from:https://www.jiomoney.com/tandc.html
[47] Fintech Trends Report 2017.PricewaterhouseCoopers. Retrieved from:https://www.pwc.in/assets/pdfs/publications/2017/fintech-india-report-2017.pd
[48] GOI. (2001). Statement 4, Scheduled languages in descending order of Speaker's strength - 2001. Census of India, Government of India. Retrieved from https://bit.ly/2NoZUjb
[49] Kroulek, A. (2018). Which countries have the most English speakers? K Interna-tional. Retrieved from https://bit.ly/2mi9t94
[50] Patrick Gage Kelley et al., A "Nutrition Label" for Privacy, PROC. 5TH SYMP. ON USABLE PRIVACY AND SECURITY (SOUPS), July 2009, https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.
[51] McDonald, A. M., and Cranor, L. F. "The cost of reading privacy policies". I/S –A Journal of Law and Policy for the Information Society 4(3), 2008.

documents.[52] In a recent study it was found that more women and young and rural users were using digital technologies, however the usage of digital technology and finance were low. The study also noted that the key barrier in them reading privacy policies were length, language and legalese.[53] Another study stated identified that 79.4 percent of the surveyed participants stated that they did not read the privacy policies and only 11 percent of them stated that they understood them.[54] Yet another study conducted on the most popular apps in India also observed that the privacy policies were drafted to protect the service providers from liability, rather than to help the consumers.[55] This situation has worsened with users interacting with increasingly complex data collection practices and accessing services through devices such as smartphones which make reading privacy policies harder.[56]

Given the poor state of financial literacy in India[57], the legalese of privacy policies makes fintech privacy policies may make it harder for to engage with fintech services in an informed fashion. One of the ways to navigate these realities, along with lucid language accompanied by detailed explanations for technical terminology, is the use of visual aids. In our study we found that all the privacy policies were purely textual and were often lacking in visual markers such as bold and bigger font for paragraphs, section separators, contrast in colour typography to distinguish between the types of content etc. Further, they had no visual aids, such as picture or infographics. By using visual summaries, or supporting infographics these privacy policies can be made more engaging.[58] Another modality than can be explored is the use of videos that explain the privacy policy especially in light of growing video-based consumption of internet data in India[59].

[52] Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 471-478). ACM. See also Federal Trade Commission. 2012. Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers.

[53]Kulkarni A,Narayan S and Punia S, Users' Perspectives on Privacy Policy and Data Protection, Cuts International Retrieved from:http://snip.ly/2dfaj0#http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf

[54]Kulkarni A,Narayan S and Punia S, Users' Perspectives on Privacy Policy and Data Protection, Cuts International Retrieved from:http://snip.ly/2dfaj0#http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf

[55] Bailey R, Parsheera S, Rahman F, Sane R, Disclosures in privacy policies: Does “notice and consent” work? NIPFP Working paper series Retrieved from:https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

[56] Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., Wetherall, D. “A Conundrum of Permissions: Installing Applications on an Android Smartphone”. In Proceedings of USEC2012: Financial Cryptography and Data Security Workshop on Usable Security, March 2012.

[57] https://gflec.org/wp-content/uploads/2015/11/3313-Finlit_Report_FINAL-5.11.16.pdf?x37611

[58] Naidu.S.(2018, May 29).Design Concerns in Creating Privacy Notices.:Centre for Internet and Society. Retrieved from https://cis-india.org/internet-governance/blog/design-concerns-in-creating-privacy-notices

[59]Nokia, India Mobile Broadband Index, Retrieved from:https://onestore.nokia.com/asset/206056

Notification of breaches

As the SPD/I Rules are silent on breach notifications, most data controllers did not mention any steps that would be taken by them in the event of a breach/unauthorised access.[60] On the other contrary, we observed that for privacy policies that did contain mention of breaches, the onus of preventing any breach/unauthorised access was squarely placed on the data subject. The absence of any mechanism to inform data subjects about compromise of or unauthorised access to their personal information becomes especially relevant given the sensitivity of financial information that fintech service providers are typically collecting and processing.

Notice in case of updation

As the SPD/I Rules are silent on the need to inform the user of subsequent changes in the privacy policy, most fintech companies leaves the onus of knowing about the change on the user. A majority of the privacy policies, specified that the user would have to periodically check the privacy policy page in order to know if there has been any updation in the policy. While some of these companies state that the changes would be highlighted or will be on the top of the privacy policy, the rest give no indication of how the consumer would know about the changes made, without having the means to compare the policies. However there were five companies that stated that they would email the users of the changes in the privacy policy,[61] where one of them specified that the email would only be sent in the case of any change in the use of the consumer's personal data.[62]

Notice and Consent are the basis of a privacy policy, and when there are changes in the policy a mere notice is not enough. In the case of some of these companies, the notice function was also not fulfilled. It is understandable that seeking consent anew for each change in the policy is not practical, and can cause 'consent fatigue', there is a need to seek consent anew for any change in the processing of data of the consumer. The companies could ideally as a best practice, notify the consumers through email of any change in the privacy policy, as well as seek consent anew for any new way of processing the data of the consumer.

Conclusion

Like many jurisdictions, India ascribes to the 'notice-and-choice' regime of web-based privacy enforcement which requires that operators of electronic media provide to their users a notice of inter alia their data collection, storage and processing practises. In theory then, users can choose to accept these practises or not avail of the services. In India, the SPD/I

[60] Privacy policies of only two data controllers that stated that the user will be notified if there was a breach. They were Citrus Pay and Mobikwik Wallet.
[61] Example: Instamojo https://www.instamojo.com/privacy/.
[62] UAE- Exchange https://www.uaeexchangeindia.com/privacy/

Rules framed under the IT Act make privacy policies a ubiquitous feature of websites and mobile applications of firms operating in India.

In practice, however, research shows that few consumers, if any, read online privacy policies, despite expressing concern about their online privacy.[63] Privacy policies are notoriously technical, long and infeasible for customers to peruse.[64] A few of the reasons for the impracticality is the placement of the policies (often at the end of the web page), the length, font and the language of the policies, as well as the lack of awareness about the contents of the documents.[65] In a recent study it was found that more women and young and rural users were using digital technologies, however the usage of digital technology and finance were low. The study also noted that the key barrier in them reading privacy policies were length, language and legalese.[66] Another study stated identified that 79.4 percent of the surveyed participants stated that they did not read the privacy policies and only 11 percent of them stated that they understood them.[67] Yet another study conducted on the most popular apps in India also observed that the privacy policies were drafted to protect the service providers from liability, rather than to help the consumers.[68]

The draft Personal Data Protection Bill (2018) contains provisions that go beyond just the requirements of the IT Rules. The Bill specifies a notice and consent framework with explicit consent in the case of sensitive personal data. Explicit consent is understood as consent that is informed, clear, and specific along with being free free and capable of being withdrawn.[69] Additionally the Bill also requires privacy policies to be easily comprehensible and in multiple Indian languages. However, as the Bill has not been passed by the Parliament, the SPD/I Rules and the IT Act are the only guidelines for privacy policies. As stated earlier the SPD/I Rules are the bare minimum standards and data controllers should strive to go above and beyond them.

The internet has become a diverse place which provides information to people with various degrees of ability, be it financial, physical, linguistic, technological etc. and the companies need to ensure that not only their services keep this diversity in mind, but also their privacy

---

[63] Patrick Gage Kelley et al., A “Nutrition Label” for Privacy, PROC. 5TH SYMP. ON USABLE PRIVACY AND SECURITY (SOUPS), July 2009, https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.
[64] McDonald, A. M., and Cranor, L. F. “The cost of reading privacy policies”. I/S –A Journal of Law and Policy for the Information Society 4(3), 2008.
[65] Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 471-478). ACM. See also Federal Trade Commission. 2012. Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers.
[66]Kulkarni A,Narayan S and Punia S, Users' Perspectives on Privacy Policy and Data Protection, Cuts International Retrieved from:http://snip.ly/2dfaj0#http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf
[67] Kulkarni A,Narayan S and Punia S, Users' Perspectives on Privacy Policy and Data Protection, Cuts International Retrieved from:http://snip.ly/2dfaj0#http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf
[68] Bailey R, Parsheera S, Rahman F, Sane R, Disclosures in privacy policies: Does “notice and consent” work? NIPFP Working paper series Retrieved from:https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf
[69]Section 18 of the draft Personal Data Protection Bill 2018 Retrieved from :https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

policies.[70] This situation has worsened with users interacting with increasingly complex data collection practices and accessing services through devices such as smartphones which make reading privacy policies harder.[71] The fact that no Fintech company that this research studied complied with all the provisions even of the SPD/I Rules is telling. It, then, indicates the limitations of the 'notice-and-choice' model of data privacy. While information that is provided to data subjects is necessary to be better designed, neither the SPD/I Rules, nor the the PDP Bill take into account the manner in which data flows operate in the context of Fintech business models.

Annexure 1

Clear and Accessible statements of its practices and policies

Whether the privacy policy is accessible through the main website of the body corporate?

Whether the privacy policy is mentioned or included in the terms and conditions of publicly available documents of the body corporate that collect personal information?

Whether the privacy policy can be comprehended by persons without legal knowledge?

Collection of personal or sensitive personal data/information

Type

Whether the privacy policy mentions all categories of personal information including SPD/I being collected?

Whether the privacy policy explicitly specifies the type of SPD/I being collected?

Option

Whether the Privacy Policy specifies that the user has the option to not provide information?

Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?

[70] Naidu S, Design Concerns in Creating Privacy Notices, Centre for Internet and Society, Retrieved from:https://cis-india.org/internet-governance/blog/design-concerns-in-creating-privacy-notices
[71] Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., Wetherall, D. "A Conundrum of Permissions: Installing Applications on an Android Smartphone". In Proceedings of USEC2012: Financial Cryptography and Data Security Workshop on Usable Security, March 2012.

Grievance Officer

Whether the privacy policy mentions the existence of a grievance officer?

Whether the privacy policy provides the contact information of the grievance officer?

Purpose of Collection and usage of information

Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?

Whether the privacy policy makes explicit provisioning regarding the retention of users' information?

Whether the privacy policy outlines a mechanism allowing users to review, correct and amend the information provided by the user?

Disclosure of Information

Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties?

Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?

Reasonable Security practices and procedures

Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?

Fintech in India: Privacy Policies at a Glance

YES | NO | PARTIALLY

Company Name	Criteria																
	Clear and Accessible statements of its practices and policies			Collection of personal or sensitive personal data/information				Grievance officer			Purpose of Collection and usage of information			Disclosure of information		Security Practices
	Privacy policy is accessible through main website?	Privacy policy mentioned in terms and conditions?	Privacy policy can be comprehended by persons without legal knowledge?	Privacy policy mentions all categories of personal information being collected?	Privacy policy explicitly specifies the type of SPD/I being collected?	Privacy policy specifies user the option to Not provide information?	Privacy policy specifies user the option to withdraw consent?	Privacy policy mentions the existence of grievance officer?	Privacy policy provides contact info of grievance officer?	Privacy Policy provides details of grievance redressal mechanism?	Privacy policy enumerates purpose(s) for collection?	Privacy policy makes explicit provisioning regarding the retention of users' information?	Privacy policy outlines mechanism to review and amend information provided by the user?	Contractual provisions in privacy policy or ToS addressing disclosure of PI with 3rd parties	PI disclosed to government agencies/LEA/IA only when legally mandated?	Privacy policy provides details of reasonable security practices and procedures followed to secure PI?
BillJunction																
CC Avenue																
EBS																
PayU																
InstaMojo																
JusPay																
RazorPay																
BillDesk																
DirecPay																
Citrus Pay																
Stripe																
Udio by Transerv																
HotRemit by Digit Secure India																
Zeta																
Amazon Pay																
Simpl																
Itz Cash																
Walnut																
Freecharge																
Oxigen																
X-Pay by UAE Exchange																
Mobikwik Wallet																
JioMoney																
Airtel Payments Bank																
Paytm																
FiNo Paytech																
Jio Payments Bank																
FairCent																
LendBox																
LoanMeet																
i-Lend																
I2IFunding																
LendenClub																
Cashkumar																
Credy																
Tachyloans																
LoyltyRewardz																
Rubique																
Paymate																
Chillr																
Suvidhaa																
BankBazaar																
Policybazaar																
Capital Float																
BHIM UPI																
Google Pay																
FT cash																
PhonePe																

Privacy policy snapshots

Clear and accessible statements of its practices and policies

Interpretation

Rule 4 of the SPD/I Rules mandates that a body corporate dealing with or handling the information (a "data controller") of an information provider (a "data subject") shall effect a privacy policy that binds the data controller to dealing with the information in a manner prescribed under the SPD/I Rules. It is further required that the privacy policy should be published on the website of the data controller and that the policy should be "clear and easily accessible".

However, the SPD/I Rules are silent on the specific requirements of what would constitute a "clear and accessible" privacy policy. In the absence of this specification, for the purpose of this research, "accessibility" can be understood to mean the number of clicks that are required to access the data controller's privacy policy. As a proxy, a privacy policy is accessible if it is linked to on the homepage of the data controller's website and the text of the hyperlink adequately indicates so. The threshold for "clarity" is met if the privacy policy states the data controller's practices in dealing with the data subject's information in language that can be expected to be comprehended by a data subject being fluent in English and does not require prior legal or technical knowledge to be comprehended.[17]

Testing Results

Whether the privacy policy is accessible through the main website of the body corporate?

Image 1.1

[17] For a survey/quiz based approach that tested privacy policy comprehension, see *Disclosures in privacy policies: Does notice and consent work?,* Rishab Bailey, Smriti Parsheera, Faiza Rahman, Renuka Sane. December 2018. A survey of 155 undergraduate and graduate respondents across five colleges around New Delhi (administering education in English) was undertaken that tested the quality of privacy policies of five popular online services in India from the perspective of access and readability.

Whether the privacy policy is mentioned or included in the terms and conditions of all document of the body corporate that collects personal information?

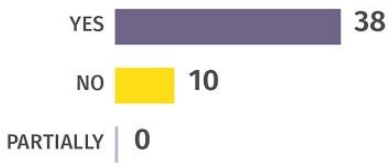

Image 1.2

Whether the privacy policy can be comprehended by persons without legal and technical knowledge?

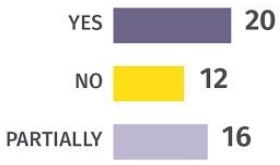

Image 1.3

Sample 'yes' excerpt:

"Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing a song in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting"[18]

Sample 'no' excerpt:

"The rights and remedies available under this Policy may be exercised as often as necessary and are cumulative and not exclusive of rights or remedies provided by law. It may be waived only in writing. Delay in exercising or non-exercise of any such right or remedy does not constitute a waiver of that right or remedy, or any other right or remedy."[19]

[18] Privacy Policy. Google Pay. Retrieved from: https://policies.google.com/privacy
[19] Privacy Policy. Capital Float. Retrieved from: https://www.capitalfloat.com/privacy-policy

Sample 'partially' excerpt:

"Itz Cash Card Limited strive to keep the level of security state-of-the-art at all times and takes steps to protect your personally identifiable information and has adopted generally accepted standards of technology in order to protect your personally identifiable information. We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input. We store information gathered on secure computers. We use advanced security technology to prevent our computers from being accessed by unauthorized persons."[20]

Observation

Placement of privacy policies

Most fintech companies have adopted the now standard practice utilised for placing privacy policies on websites - that of providing a hyperlink to the privacy policy at the bottom of the main page of their website. The text of the hyperlink, however, is usually displayed in font smaller than that used for the rest of the page making it more challenging to locate prior to using the services provided by the data controller.

Further, for some of the companies the privacy policy had to be located in the terms of service[21] or under separate categories such as 'legal agreements', 'key policies', 'security', further making the privacy police more inaccessible. Resultantly, we anticipate that unless the data subject is specifically looking for the privacy policy, it is unlikely for the privacy policy to be perused in the usual course of a data subject's usage of the services of the fintech provider.

Type and acknowledgment of personal or sensitive personal data/information collected

Interpretation

Section 2(1)(i) of the IT Act defines personal information as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." Rule 3 of the SPD/I Rules further demarcates sensitive personal data/information as personal information which consists of passwords; financial information, physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information. Two other broad categories are included - any related details provided to the body corporate, and any information received by the body corporate in relation to the categories listed above. Rule 4(1)(ii) further elaborates that the privacy policy must specify the type of personal or sensitive personal data or information collected.

[20] Privacy Policy. Itzcash. Retrieved from: http://itzcash.com/privacy-policy/
[21] See, for example http://www.hotremit.com/terms.html#privacy. Also see https://paytm.com/about-us/our-policies/#tandc and https://www.i-lend.in/index.html

Testing Results

Whether the privacy policy mentions all categories of personal information including SPD/I being collected?

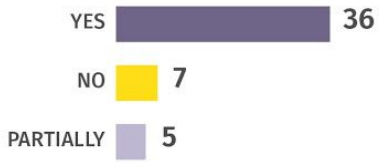

Image 2.1

Sample 'yes' excerpt:

"INFORMATION THAT WE COLLECT AND THAT YOU PROVIDE
I. PERSONAL INFORMATION
Personal Information means and includes all information that can be linked to a specific individual or to identify any individual, such as:
a. Your full name, address, e-mail address, telephone number, date of birth and bank or payment card details and any proof of Your identity and/or address that we may request;
b. Details of any transactions that You carry out through our Website or application using Your Oxigen account and of the fulfilment of Your requests;
c. Details of any credit, debit or other card used by You for transactions;
d. Details of any bank account (including but not limited to, account holder, account name, account number, sort code, online banking PIN, Transaction Authentication Number "TAN" and password, available balance and transaction history of Your bank account), ITR, TAX certificates or any other income documents as necessary by Us;
e. Any correspondence sent by You to Us;
f. Survey that You complete through the Website or based on our request;
g. Your participation in any promotion sponsored by Us;
h. Calls that we make to You or You make to Us;
i. Information collected through Cookies;
j. Your IP address, log-in times, operating system and browser type;
k. Details of Your visits to our Website/ mobile application including, but not limited to, Traffic Data, location data, weblogs and other communication data, whether this is required for Our own billing purposes or otherwise and the resources that You access whilst visiting Our Website or mobile application."[22]

[22]Privacy Policy. Oxigen.Retrieved from http://www.myoxigen.com/assets/pdf/Oxigen%20Privacy%20Policy.pdf

Sample 'no' excerpt:

"We store your email ID so that in future we can mail you a backup of your Chillr data upon receiving a request from you."[23]

Sample 'partially' excerpt:

"We may permit use of your name, e-mail addresses, addresses, telephone and fax numbers and other relevant details for our own marketing or we may permit others to access the same for marketing."[24]

Whether the privacy policy explicitly specifies the type of SPD/I being collected?

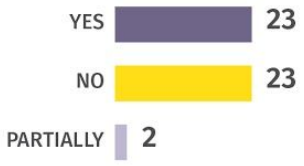

Image 2.2

Sample 'yes' excerpt:

"Upon signing up on Our Website, You are required to provide Us with certain basic mandatory information inter-alia Your name, title, physical address, phone number, e-mail address, details regarding Your credit/debit Card and other sensitive information."[25]

Sample 'no' excerpt:

"Personal Information means and includes all information that can be linked to a specific individual or to identify any individual, such as name, address, mailing address, telephone number, email ID, credit card number, cardholder name, card expiration date, information about your mobile phone, DTH service, data card, electricity connection, Smart Tags and any details that may have been voluntarily provide by the user in connection with availing any of the services on Paytm."[26]

Sample 'partially' excerpt:

"We may permit use of your name, e-mail addresses, addresses, telephone and fax numbers and other relevant details for our own marketing or we may permit others to access the same for marketing. However, no informations relating to your personal bank accounts or personal investments will be revealed to any third party without your consent unless required by law."

[23] Privacy Policy. Chillr.Retrieved from https://chillr.com/privacy.html
[24] Privacy Policy. Direcpay. Retrieved from http://www.direcpay.com/direcpay/dpprivacypolicy.jsp
[25]Privacy Policy. Oxigen.Retrieved from http://www.myoxigen.com/assets/pdf/Oxigen%20Privacy%20Policy.pdf
[26] Privacy.Paytm.Retrieved from https://pages.paytm.com/privacy.html

Observations

Lack of specificity

While most fintech companies in the sample explicitly specified personal information that was being collected, fewer privacy policies contained categorical provisions segregating the *sensitive* personal information that was being collected.

Another trend that emerged pertained to the manner in which the information being collected is detailed. In nearly all instances, the listing of collected information was not exhaustive with the usage of terminology such as 'etc.', 'inter alia', 'information such as', being commonplace. Another terminology that is often incorporated to broaden the ambit of information being collected is the definition of personal information as any information that may be provided by the user. This squarely places the onus of restricting information collection on the data subject further compounding the handicaps users face in ascertaining the information that that firms are seeking to collect because of the illustrative nature of the listing of information.

Option to not provide information and withdrawal of consent

Interpretation

Rule 5(7) states that the data controller should inform data subjects prior to the collection of information (including sensitive personal data or information) that they have an option to not provide the data or information. The rule also specifies that the individual must also be informed that he/she has an option to subsequently withdraw consent from the use of the data or information collected by the data controller.

Testing Results

Whether the Privacy Policy specifies that the user has the option to not provide information?

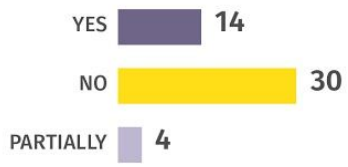

Image 3.1

Sample 'yes' excerpt:

"The User always has the option to not provide information by choosing not to use a particular service or feature."[27]

[27] Privacy Policy. I2ifunding. Retrieved from:https://www.i2ifunding.com/privacy-policy

Sample 'no' excerpt:

For privacy policies that returned a 'no' response, the privacy policies did not specify that the user has the option to not provide information.

Sample 'partially' excerpt:

"We provide you the opportunity to opt-out of having your Personal Information used for certain purposes. For example, if you purchase a product/service but do not wish to receive any additional marketing material from us, you can indicate your preference on our order form. If you no longer wish to receive our newsletters and promotional communications, you may opt-out of receiving them by following the instructions included in each newsletter or communication or by emailing us at support@faircent.com. We also offer you an opportunity to opt-out of certain communications through the account management screen. If you need assistance you may contact us at support@faircent.com."[28]

Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?

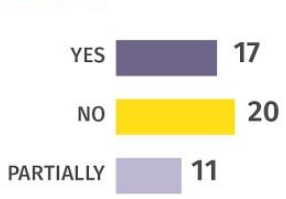

Image 3.2

Sample 'yes' excerpt:

"(ii) The User can at any time while availing the services or otherwise, withdraw his/her consent given previously to PayU for collecting, receiving, possessing, storing, dealing or handling Information of the User, by sending us your request by email on privacy@payu.in. In such case, PayU will unfortunately not be in a position to provide the Services to you."[29]

Sample 'no' excerpt:

For privacy policies that returned a 'no' response, the privacy policies did not specify that the user has the option to subsequently withdraw consent.

Sample 'partially' excerpt:

"We provide you the opportunity to opt-out of having your Personal Information used for certain purposes. For example, if you purchase a product/service but do not wish to receive any additional marketing material from us, you can indicate your preference on our order form. If you no longer wish to receive our newsletters and promotional communications, you may opt-out of receiving them by following the instructions included in each newsletter or communication or by emailing us at support@faircent.com. We also offer you an opportunity

[28]Privacy Policy. Faircent. Retrieved from: https://www.faircent.com/privacy-policy
[29] Privacy Policy. PayUmoney. Retrieved from: https://www.payumoney.com/privacypolicy.html

to opt-out of certain communications through the account management screen. If you need assistance you may contact us at support@faircent.com."

Observation

Option to opt-out of further processing

The phrasing of opt-out clauses generally only provided users with the limited right to stop receiving correspondence from the data controller (promotional calls and emails, newsletters etc.). The option to opt-out, then, is restricted only to certain uses of a user's information.

Fintech providers, generally, have equated users opting out of the use of their personal information with a complete termination of services. . The same way as consent should not mean that the user consents to all the forms of data processing, a data subject must also have the option to withdraw her consent from certain types of processing while still enjoying the services she has consented to. For example, she could withdraw her consent from the use of her previously shared biometric information from being used by a Fintech company, while still allowing for the use of her financial information for services that only require the latter. How Fintech companies have structured their privacy policies generally do not allow for this possibility.. Privacy policies, then, should first clearly state how the users data is being processed and shared as well as provide the users to withdraw their consent from certain types of processing and still enjoy the services she consents to.

Grievance officer

Interpretation

Rule 5(9) of the SPD/I Rules prescribe that data controllers are required to have a grievance redressal mechanism in place vis-a-vis the data controller's privacy practices. This entails the provision of a grievance officer whose contact information is to be provided on the website. Further, the body corporate is required to address grievances in a "time bound" fashion within a maximum time-frame of 1 month. Consequently, another criteria we assessed was whether the procedural specificities of the grievance redressal mechanism were provided to enable the effective use of the redressal mechanism. This would entail providing information around recognition of receipt of the complaint by the grievance officer, binding the grievance officer to adhere to granular time milestones, appeals process etc.

Testing Results

Whether the privacy policy mentions the existence of a grievance officer?

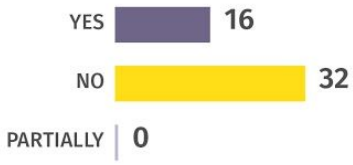

Image 4.1

Sample 'yes' excerpt:

"If you have any questions, or concerns about this Policy or any complaints or grievances about the manner in which we handle your personal information or the use of your personal information (in doing so acknowledging that we may be unable to provide you all or some of the services), please feel free to contact the Grievance Officer any time."[30]

Sample 'no' excerpt: For privacy policies that returned a 'no' response, the privacy policies did not mention a grievance officer.

Sample 'partially' excerpt: No privacy policies only partially mentioned the existence of a grievance officer.

Whether the privacy policy provides the contact information of the grievance officer?

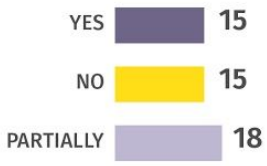

Image 4.2

Sample 'yes' excerpt:

"In accordance with Information Technology Act, 2000 and rules made there under, the name and contact details of the Grievance Officer is provided below:

Contact Name: Vishal Gupta

Email: grievanceofficer@phonepe.com"

Sample 'no' excerpt:

[30] Privacy.Paytm.Retrieved from https://pages.paytm.com/privacy.html

For privacy policies that returned a 'no' response, the privacy policies did not provide contact information of the grievance officer.

Sample 'partially' excerpt:

"If you have any questions, or concerns about this Policy or any complaints or grievances about the manner in which we handle your personal information or the use of your personal information (in doing so acknowledging that we may be unable to provide you all or some of the services), please feel free to contact the Grievance Officer any time."[31]

Whether the privacy policy provides details of the grievance redressal mechanism?

Image 5.1

Sample 'yes' excerpt:

""Level 4"

In accordance with Information Technology Act, 2000 and rules made there under, the name and contact details of the Grievance Officer is provided below:

Contact Name: Vishal Gupta

Email: grievanceofficer@phonepe.com

Address- Ashford Park View, Site No - 9 Industrial Layout, Koramangala 3rd Block, 80 ft Road, Bangalore-560034, India.

Working hours: Mon-Fri 10 am to 7 pm

- Any Level 4 escalation email should contain the following information –
    - User's name
    - Registered contact number
    - Ticket number of the complaint registered by Level 1
    - Details of why the resolutions provided at previous levels were deemed unsatisfactory
- Resolution of Complaints:
    - We are committed to providing a first response within 24 hours of receiving the complaint.
    - We aim to resolve all Level 2 complaints within 3 business days. Any delay in

[31] Privacy Policy. Rubique. Retrieved from:https://www.rubique.com/privacy-policy

- the resolution time shall be proactively communicated to you"[32]

Sample "no" excerpt: For privacy policies that returned a 'no' response, the privacy policies did not provide details of the grievance redressal mechanism.

Sample "partially" excerpt:

"VIII. QUESTIONS OR CONCERNS

If you have any questions or concerns regarding our privacy policies, please send us a detailed message to privacy@instamojo.com, and we will try to resolve your concerns."[33]

Observation

Missing mechanisms

Insofar as grievance redressal is concerned, the starkest absence was that of the details about the grievance redressal mechanism seems. With respect to the requirement that the data controllers mention the existence of grievance officers, thirty two companies failed to not just provide a redressal mechanism but also failed to mention the existence of a grievance officer specific to the resolution of issues that data subjects may encounter vis-à-vis the data controller's privacy practices.

However with respect to the question of providing contact details of grievance officers a few of the companies did comply with this requirement partially by providing contact details of a person who could be contacted in case of any problem. Although they fail to specify what exact authority and responsibility that the person assigned has, in our study we considered it as a point of contact for grievances. For example CCAvenue's privacy policy reads, "If you have questions about CCAvenue.com privacy practices, please contact us at contact@ccavenue.com."[34] Similarly PayU Money's reads, "In the event that you encounter any person is improperly collecting or using information about Users, please contact us by emailing at support@payumoney.com".[35]

Purpose of collection and usage of information

Interpretation

The SPD/I Rules mandate that the privacy policies of data controllers collecting sensitive personal data or information must provide for the purpose for such collection and the subsequent usage of the SPD/I.[36] Harmoniously read with Rule 4(1)(iii), this requirement can be further to extended to information collected not limited to SPD/I. Further, the data controller is permitted to collect *information* only for a lawful purpose connected with the data controller's function or activity and only if it is considered necessary for that purpose.

---

[32] Privacy Policy.Phonepe. Retrieved from:https://phonepe.com/en/policy.html
[33] Privacy.Instamojo. Retrieved from:https://www.instamojo.com/privacy/
[34] Privacy Policy. CC Avenue. Retrieved from https://www.ccavenue.com/privacy.jsp
[35] Privacy Policy. PayU. Retrieved from:https://www.payumoney.com/privacypolicy.html
[36] Rule 4(1)(iii) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Further, the data controller can only use the *information* collected for the purpose for which it had been collected.

Along with the need to specify the purpose of collection Rule 5(4) of the SPD/I Rules require that the data controllers holding sensitive personal data or information shall not retain that information for longer than is necessary for the purpose for which the information may lawfully be used or is otherwise required under any other law. Apart from purpose limitation, Rule 5(6) also requires the data controller to provide the data subject with the ability to review as well as correct or amend the information provided to the data controller.

Testing Results

Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?

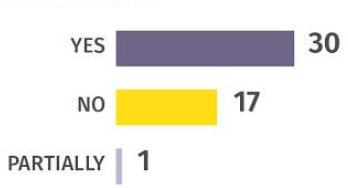

Image 6.1

Sample 'yes' excerpt:

"III. Usage of Your Personal Data

We use your Personal Data in our business activities for providing our or our partners' products/services and to perform, among other actions, the following:

1. to facilitate the transactions or report on these transactions;

2. to undertake research and analytics for offering or improving our products/services and their security and service quality;

3. to check and process your requirements submitted to us for products/services and/or instructions or requests received from you in respect of these products/services;

4. to share with you, updates on changes to the products/services and their terms and conditions;

5. to take up or investigate any complaints/claims/disputes;

6. to respond to your queries or feedback submitted by you;

7. to verify your identity for us to provide products/services to you;

8. to carry credit checks, screenings or due diligence checks as lawfully required by us;

9. to monitor and review products/services from time to time;

10. to undertake financial/regulatory/management reporting, and create and maintain various risk management models;

11. for conducting audits and for record keeping purposes;

12. for selective offers and promotions.

External processing: We may provide your personal information to our affiliates or other trusted businesses or persons or service providers engaged by us, or institutions that we partner with to assist us with providing you with products/services to better serve your needs and interests, based on your instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

We also use your Personal Data to fulfill the requirements of applicable laws/regulations and/or court orders/regulatory directives received by us."

Sample 'no' excerpt:

For privacy policies that returned a 'no' response, the privacy policies do not enumerates the purpose(s) for which information is collected.

Sample 'partially' excerpt:

"Personal Information which we share with our affiliates and/or third parties for marketing purposes, and providing contact information for such affiliates and/or third parties."

Whether the privacy policy makes explicit provisioning regarding the retention of users' information?

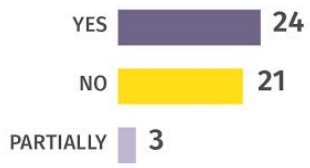

Image 6.2

Sample 'yes' excerpt:

"(i) BankBazaar will retain your information for as long as it is necessary for providing you the Services available on the Website or your request for termination of your account with BankBazaar, whichever is later.

(ii) Post termination of your account, BankBazaar may continue to use your anonymized data aggregated or in combination with anonymized data of other users. We use this aggregated anonymized data for data analysis, profiling and research purposes, for example to gain insights about our users and their profiles. We may keep your contact information along with

your application details (if any) for fraud prevention purposes and for the exercise/ defense of a legal claim or for providing evidence in legal proceeding(s)."[37]

Sample 'no' excerpt:

"Your personal data will be stored and collected by Policybazaar Insurance Web Aggregator Private Limited".[38]

Sample 'partially' excerpt:

"When You use the Website and the Service provided by Simpl on the Website, Simpl makes good faith efforts to provide You with access to Your Information and other relevant data, either to correct this data if it is inaccurate, or to delete such data at Your request, if it is not otherwise required to be retained by law or for legitimate business purposes."

Whether the privacy policy outlines a mechanism allowing users to review, correct and amend the information provided by the user?

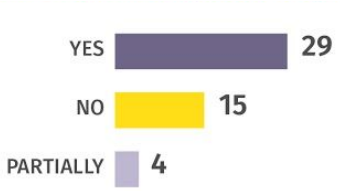

Image 6.3

Sample 'yes' excerpt:

"When you are signed in, you can always review, and update information. You can also review and control information saved in your account. You can also always export copy of content in your Account if you want to back it up."[39]

Sample 'no' excerpt: For privacy policies that returned a 'no' response, the privacy policies did not outline a mechanism allowing users to review, correct and amend the information provided by the user.

Sample 'partially' excerpt:

"We store all the transaction related information including amounts, remarks, location tags, pictures so that you can access your data even after changing your device."[40]

---

[37] Privacy Policy.Bankbazaar. Retrieved from: https://www.bankbazaar.com/mobile-app-privacy-policy.html
[38] Privacy Policy. Policybazaar. Retrieved from:https://www.policybazaar.com/legal-and-admin-policies/
[39]Privacy Policy. I2ifunding. Retrieved from:https://www.i2ifunding.com/privacy-policy
[40] Privacy.Chillr.Retrieved from: https://chillr.com/privacy.html

Observations

No purpose limitation

Most privacy policies that were studied contained provisions outlining the purposes behind the collection of information from the data subjects. Some of the common purposes outlined by fintech firms were that of utilising the information collected for: (a) providing services and enhancing service delivery, (b) communication of marketing and promotional material, (c) developing measures to protect both the data subjects and controllers against fraud and security threats, (d) aggregating information to undertake statistical analyses of user behavior. While outlining these purposes results in compliance with the SPD/I Rules and would return a 'yes' in this study, the observed trend was that of the lack of any granular particulars about what the constituents of these broad categories of purposes outlined.

This also hints at a lack of organisational motivations in specific determinations of the purpose of collection and processing of information. Overbroad purpose disclosures may have also become the norm owing to challenges in determining the proximity between the original purpose and new purpose that may arise owing to changing financial and/or technological logics in the fintech space. The lack of any instruction in legislation on the delta between original use and subsequent use is important to be highlighted here as well. The implications this practice has on individuals' right to privacy is further compounded when read together with the lack of segregation of sensitive personal information as outlined previously. In other words, the additional protection envisioned to be accorded to sensitive personal information is being diluted, as its collection and use is being treated with the same (dis)regard as other information.

Access and rectification

The SPD/I Rules require data controllers to provide a mechanism allowing users to access and rectify the information provided by the users. This is especially relevant as the data controllers are not accountable for the veracity of the information provided by the users. While some fintech companies provide their users with no such rights to access and rectification, those that do allow these rights to be exercised in one of two ways: either by looking at the information recorded in the user's profile settings and the other by sending a request to a designated email id. While the former provides users access to the information provided by them that is associated with their account, the contours of the latter are unclear.

Further, it is unclear if users have access to information about them that has been processed by data controllers that may not have been directly provided by the users (such as telemetric data, IP and location data etc.) but is still personal information insofar as the SPD/I Rules are concerned. While data controllers that collect this information seek to use this information in a form that is aggregated and anonymised, this practice is not just in abeyance of the SPD/I Rules buts also ignores the growing concerns around the assumed privacy-protecting power of anonymisation.

Data Retention

The SPD/I Rules require body corporates to explicitly state their data retention policy. The body corporates as data controllers store different personal and sensitive personal data. The privacy policies should ideally state the period for which the data is stored and how the data

is retained. In our study we observed that while some of the privacy policies expressly stated that the data would be retained even after the user chooses to delete their profile. Whereas some data controllers did not expressly state their retention policy, they did state that the data might be stored indefinitely in order to comply with law enforcement requirements. When data controller did not state their retention policy, it was unclear whether these agencies retain the data, even after the data subject has requested deletion of her account. This is highly problematic as some of the companies that did provide the user with the provision to withdraw consent did not clarify their data retention policy. It is to be noted that Rule (4) of the SPD/I Rules states that the companies should not retain the data longer than is required for the purpose for which it is collected or otherwise required by law. This provision has been interpreted by most data controllers to store the data indefinitely stating that the data is stored in order to comply with the government or law enforcement agencies. In the absence of a law that explicitly states the time after which the data should be deleted, data controllers also have no option but to account for all possible scenarios in which they may be obligated to provide information.

Disclosure of information

Interpretation

The SPD/I Rules govern the disclosure of such information to third parties and government agencies. The disclosure by body corporates to third parties requires prior permission from the provider of the information - this requirement is waived if a pre-existing contractual agreement between the data subject and the data controller, permitting such disclosure, already exists or if the disclosure is required to made in order to comply to a legal obligation. This contractual agreement, typically, is in the form of explicit provisions in either the privacy policy or the terms of service provided on the body corporate's website.

Disclosing information to legally mandated government agencies, however, does not require the provider's prior permission. However, the data controller is required to disclose information to a government agency only upon the furnishing of an authorised request to the data controller. Mirroring the phrasing in the text of Rule 6(1), a privacy policy is compliant only when it specifically commits to the procedure outlined specifically when disclosing information to legally mandated government agencies.

Testing Results

Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties?

Image 7.1

Sample 'yes' excerpt:

"(a). You hereby unconditionally agree and permit that the Freecharge Entities may transfer, share, disclose or part with all or any of Your Information, within and outside of the Republic of India to various Freecharge Entities, Third Party Service Providers / Partners / Banks and Financial Institutions for one or more of the Purposes, government agencies upon directions of such agency, or to any other third party as may be required under applicable law. In case of any Personal Information so transferred, shared, disclosed or parted with, We will contractually oblige the receiving parties of the Information to ensure the same level of data protection adopted by the Freecharge Entities is adhered to by the receiving party, subject to applicable law.

Sample 'no' excerpt: The privacy policies and that returned a 'no' response did not contain any provisions addressing the disclosure of information.

Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?

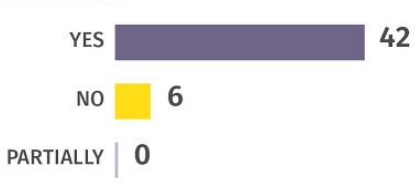

Image 7.2

Sample 'yes' excerpt:

[...]

(f). We reserve the right to disclose Your Information when required to do so by law or regulation, or under any legal obligation or order under law or in response to a request from a law enforcement or governmental agency or judicial, quasi-judicial or any other statutory or constitutional authority or to establish or exercise Our legal rights or defend against legal claims."[41]

[41] Terms and Conditions. Freecharge. Retrieved from: https://www.freecharge.in/termsandconditions

Sample 'no' excerpt: For privacy policies that returned a 'no' response, the privacy policies did not contain provisions relating to information disclosure to government agencies/LEA/IA.

Observation

Ambiguous taxonomy

Most privacy policies contained provisions speaking to the disclosure of personal information to third parties. Generally speaking, the third parties usually are: (a) affiliated or related entities, (b) law enforcement or (c) data processing service providers engaged by the data controller.

However, there is ambiguity in the terminology being used leading to a lack of clarity about what personal information could be shared with which third parties. For instance, it is often left undefined who "affiliates" are, and what entities are subsumed within the understanding of related entities within a group of companies. When it comes to data processing service providers, most privacy policies also only provide illustrative lists, leaving the data subjects guessing. For example, Amazon Pay's privacy policy indicates that third parties "include sending postal mail and e-mail, analyzing data, providing marketing assistance, processing payment transactions, verifying identity, fraud screening and providing customer service. [emphasis supplied]."

Sharing of personal information with law enforcement is also captured in most privacy policies, although no privacy policy that was studied provides any notice to the data subject prior to or post sharing information. Also, it is rare for privacy policy provisions to acquiesce to disclosing such information only when such requests adhere to the procedural requirements legitimising the request for information. For instance, PayTM's privacy policy clarifies that one of the circumstances in which personal information is shared is when "it is directed or required by legal/regulatory/statutory/governmental authorities under applicable laws/regulations though a legally obligated request."

Reasonable security practices and procedures

Interpretation

The SPD/I Rules require the body corporate to have implemented standard security practices and procedures commensurate to the information assets intended to be protected. These are further required to have been documented as a part of the body corporate's information security program and policies and should contain appropriate "*managerial, technical, operational and physical security control measures*". An international security standard that is used to illustrate these requirements is the IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements". The SPD/I Rules do not specify that this documentation be incorporated in the privacy policies; it is only mandated that the body corporates' privacy policies provide information pertaining to the reasonable security practices and procedures being implemented. The body corporate, then, is required to include as many details as possible in the privacy policy regarding the measures adopted to ensure the security of the information being collected and stored.

Testing Results

Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?

Image 8.1

Sample 'yes' excerpt:

"We adopt reasonable security practices and procedures, in line with international standard IS/ISO/IEC 27001, to include, technical, operational, managerial and physical security controls in order to protect your personal information from unauthorized access, or disclosure while it is under our control.

Our security practices and procedures limit access to personal information on need-only basis. Further, our employees are bound by Code of Conduct and Confidentiality Policies which obligate them to protect the confidentiality of personal information.

We take adequate steps to ensure that our third parties adopt reasonable level of security practices and procedures to ensure security of personal information.

We may retain your personal information for as long as required to provide you with services or if otherwise required under any law.

When we dispose of your personal information, we use reasonable procedures to erase it or render it unreadable (for example, shredding documents and wiping electronic media).

Internet Use - We maintain the security of our internet connections, however for reasons outside of our control, security risks may still arise. Any personal information transmitted to us or from our online products or services will therefore be your own risk. However, we will strive to ensure the security of your information. We observe reasonable security measures to protect your personal information against hacking and virus dissemination."[42]

Sample 'no' excerpt:

"Your account is protected by a password for your privacy and security. If you access your account via a third party site or service, you may have additional or different sign-on protections via that third party site or service. You must prevent unauthorized access to your account and Personal Information by selecting and protecting your password and/or other

[42] Airtel.(2019, March 20). Retrieved from: https://www.airtel.in/forme/privacy-policy/security-practices-and-procedures

sign-on mechanism. appropriately and limiting access to your computer or device and browser by signing off after you have finished accessing your account.

We endeavor to protect the privacy of your account and other Personal Information we hold in our records, but we cannot guarantee complete security. Unauthorized entry or use, hardware or software failure, and other factors, may compromise the security of user information at any time.

The Services may contain links to other sites. We are not responsible for the privacy policies and/or practices on other sites. When following a link to another site you should read that site's privacy policy."[43]

Sample 'partially' excerpt:

"The security of your Personal Information is important to us. When you enter sensitive information such as a credit card number on our registration or order forms, we encrypt that information using secure socket layer technology (SSL).

We follow generally accepted industry standards to protect the Personal Information submitted to us, both during transmission and once we receive it. However, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, while we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security."[44]

Observation

Security provisioning

Amongst the companies that made full or partial disclosures about the security practices being adopted, a trend that emerged was that of companies committing to using the Secure Sockets Layer (SSL) protocol to ensure confidentiality of the data subject's information. The SSL protocol, however, only provides protection during transport, and is deprecated by the Transport Layer Security (TLS) protocol. TLS, in comparison, is a considerably more secure protocol. It is pertinent to note that even the utility of TLS is limited only to communication encryption, and may still leave room for data to be compromised through other means such as insecure database configurations, or through other vulnerabilities that may be present in the application or infrastructure of a particular company.

The SPD/I Rules prescribe the adoption of the ISO/IEC 27001 standard to ensure compliance with the requirement of data controllers having "reasonable security practices and procedures" in place. The ISO/IEC 27001 standard can be thought of as an overarching suite of activities that provides organisations of all kinds with a managerial framework to address 'information security risks'. This allows for ensuring the security of information far beyond network security that SSL/TLS aids with, by factoring in inter alia physical and environmental security, communications and operations management etc.

[43] Instamoji. (2019, March 20). Retrieved from: https://www.instamojo.com/privacy/
[44] Faircent.(2019, March 20). Retrieved from: https://www.faircent.com/privacy-policy

Additional observations

Language as a barrier

All privacy policies, barring one, were provided solely in English; one firm - PhonePe - provided a privacy policy in both English and Hindi[45]. Even when the terms and conditions were provided in languages other than English, the privacy policy was still solely drafted in English.[46] With the growth of the digital economy, a multitude of Indians are using online services, and it is imperative that privacy policies be accessible and understandable to all users of the service. In the context of the fintech sector, accessibility to privacy policies takes on added significance given the fintech sector's avowed promise of increasing access to financial products to hitherto underserved sections of the society[47].

Fintech companies operating in India, then, should strive to look beyond the bare minimum prescription of the SPD/I Rules and ensure that the privacy policies are not just in English, but also in other Indic languages. The current provisioning is grossly insufficient given the linguist demographics of the Indian population: less than half the population recognises even Hindi as its first language.[48] While official data on English nativity is not available, estimates peg this number to be half of all English speakers in the country (~230,000 people)[49].

Readability

Like many jurisdictions, India ascribes to the 'notice-and-choice' regime of web-based privacy enforcement which requires that operators of electronic media provide to their users a notice of *inter alia* their data collection, storage and processing practises. In theory then, users can choose to accept these practices or not avail of the services. In practice, however, research shows that few consumers, if any, read online privacy policies, despite expressing concern about their online privacy.[50] Privacy policies are notoriously technical, long and infeasible for customers to peruse.[51] A few of the reasons for the impracticality is the placement of the policies (often at the end of the web page), the length, font and the language of the policies, as well as the lack of awareness about the contents of the

[45]Privacy Policy (hindi), PhonePe, Retrieved from:https://www.phonepe.com/hi/policy.html
[46] Consumer Terms and Conditions,Jio money, Retrieved from:https://www.jiomoney.com/tandc.html
[47] Fintech Trends Report 2017.PricewaterhouseCoopers. Retrieved from:https://www.pwc.in/assets/pdfs/publications/2017/fintech-india-report-2017.pd
[48] GOI. (2001). Statement 4, Scheduled languages in descending order of Speaker's strength - 2001. Census of India, Government of India. Retrieved from https://bit.ly/2NoZUjb
[49] Kroulek, A. (2018). Which countries have the most English speakers? K Interna-tional. Retrieved from https://bit.ly/2mi9t94
[50] Patrick Gage Kelley et al., A "Nutrition Label" for Privacy, PROC. 5TH SYMP. ON USABLE PRIVACY AND SECURITY (SOUPS), July 2009, https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.
[51] McDonald, A. M., and Cranor, L. F. "The cost of reading privacy policies". I/S –A Journal of Law and Policy for the Information Society 4(3), 2008.

documents.[52] In a recent study it was found that more women and young and rural users were using digital technologies, however the usage of digital technology and finance were low. The study also noted that the key barrier in them reading privacy policies were length, language and legalese.[53] Another study stated identified that 79.4 percent of the surveyed participants stated that they did not read the privacy policies and only 11 percent of them stated that they understood them.[54] Yet another study conducted on the most popular apps in India also observed that the privacy policies were drafted to protect the service providers from liability, rather than to help the consumers.[55] This situation has worsened with users interacting with increasingly complex data collection practices and accessing services through devices such as smartphones which make reading privacy policies harder.[56]

Given the poor state of financial literacy in India[57], the legalese of privacy policies makes fintech privacy policies may make it harder for to engage with fintech services in an informed fashion. One of the ways to navigate these realities, along with lucid language accompanied by detailed explanations for technical terminology, is the use of visual aids. In our study we found that all the privacy policies were purely textual and were often lacking in visual markers such as bold and bigger font for paragraphs, section separators, contrast in colour typography to distinguish between the types of content etc. Further, they had no visual aids, such as picture or infographics. By using visual summaries, or supporting infographics these privacy policies can be made more engaging.[58] Another modality than can be explored is the use of videos that explain the privacy policy especially in light of growing video-based consumption of internet data in India[59].

[52] Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 471-478). ACM. See also Federal Trade Commission. 2012. Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers.

[53]Kulkarni A,Narayan S and Punia S, Users' Perspectives on Privacy Policy and Data Protection, Cuts International Retrieved from:http://snip.ly/2dfaj0#http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf

[54]Kulkarni A,Narayan S and Punia S, Users' Perspectives on Privacy Policy and Data Protection, Cuts International Retrieved from:http://snip.ly/2dfaj0#http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf

[55] Bailey R, Parsheera S, Rahman F, Sane R, Disclosures in privacy policies: Does “notice and consent” work? NIPFP Working paper series Retrieved from:https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

[56] Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., Wetherall, D. “A Conundrum of Permissions: Installing Applications on an Android Smartphone”. In Proceedings of USEC2012: Financial Cryptography and Data Security Workshop on Usable Security, March 2012.

[57] https://gflec.org/wp-content/uploads/2015/11/3313-Finlit_Report_FINAL-5.11.16.pdf?x37611

[58] Naidu.S.(2018, May 29).Design Concerns in Creating Privacy Notices.:Centre for Internet and Society. Retrieved from https://cis-india.org/internet-governance/blog/design-concerns-in-creating-privacy-notices

[59]Nokia, India Mobile Broadband Index, Retrieved from:https://onestore.nokia.com/asset/206056

Notification of breaches

As the SPD/I Rules are silent on breach notifications, most data controllers did not mention any steps that would be taken by them in the event of a breach/unauthorised access.[60] On the other contrary, we observed that for privacy policies that did contain mention of breaches, the onus of preventing any breach/unauthorised access was squarely placed on the data subject. The absence of any mechanism to inform data subjects about compromise of or unauthorised access to their personal information becomes especially relevant given the sensitivity of financial information that fintech service providers are typically collecting and processing.

Notice in case of updation

As the SPD/I Rules are silent on the need to inform the user of subsequent changes in the privacy policy, most fintech companies leaves the onus of knowing about the change on the user. A majority of the privacy policies, specified that the user would have to periodically check the privacy policy page in order to know if there has been any updation in the policy. While some of these companies state that the changes would be highlighted or will be on the top of the privacy policy, the rest give no indication of how the consumer would know about the changes made, without having the means to compare the policies. However there were five companies that stated that they would email the users of the changes in the privacy policy,[61] where one of them specified that the email would only be sent in the case of any change in the use of the consumer's personal data.[62]

Notice and Consent are the basis of a privacy policy, and when there are changes in the policy a mere notice is not enough. In the case of some of these companies, the notice function was also not fulfilled. It is understandable that seeking consent anew for each change in the policy is not practical, and can cause 'consent fatigue', there is a need to seek consent anew for any change in the processing of data of the consumer. The companies could ideally as a best practice, notify the consumers through email of any change in the privacy policy, as well as seek consent anew for any new way of processing the data of the consumer.

Conclusion

Like many jurisdictions, India ascribes to the 'notice-and-choice' regime of web-based privacy enforcement which requires that operators of electronic media provide to their users a notice of inter alia their data collection, storage and processing practises. In theory then, users can choose to accept these practises or not avail of the services. In India, the SPD/I

[60] Privacy policies of only two data controllers that stated that the user will be notified if there was a breach. They were Citrus Pay and Mobikwik Wallet.
[61] Example: Instamojo https://www.instamojo.com/privacy/.
[62] UAE- Exchange https://www.uaeexchangeindia.com/privacy/

Rules framed under the IT Act make privacy policies a ubiquitous feature of websites and mobile applications of firms operating in India.

In practice, however, research shows that few consumers, if any, read online privacy policies, despite expressing concern about their online privacy.[63] Privacy policies are notoriously technical, long and infeasible for customers to peruse.[64] A few of the reasons for the impracticality is the placement of the policies (often at the end of the web page), the length, font and the language of the policies, as well as the lack of awareness about the contents of the documents.[65] In a recent study it was found that more women and young and rural users were using digital technologies, however the usage of digital technology and finance were low. The study also noted that the key barrier in them reading privacy policies were length, language and legalese.[66] Another study stated identified that 79.4 percent of the surveyed participants stated that they did not read the privacy policies and only 11 percent of them stated that they understood them.[67] Yet another study conducted on the most popular apps in India also observed that the privacy policies were drafted to protect the service providers from liability, rather than to help the consumers.[68]

The draft Personal Data Protection Bill (2018) contains provisions that go beyond just the requirements of the IT Rules. The Bill specifies a notice and consent framework with explicit consent in the case of sensitive personal data. Explicit consent is understood as consent that is informed, clear, and specific along with being free free and capable of being withdrawn.[69] Additionally the Bill also requires privacy policies to be easily comprehensible and in multiple Indian languages. However, as the Bill has not been passed by the Parliament, the SPD/I Rules and the IT Act are the only guidelines for privacy policies. As stated earlier the SPD/I Rules are the bare minimum standards and data controllers should strive to go above and beyond them.

The internet has become a diverse place which provides information to people with various degrees of ability, be it financial, physical, linguistic, technological etc. and the companies need to ensure that not only their services keep this diversity in mind, but also their privacy

---

[63] Patrick Gage Kelley et al., A “Nutrition Label” for Privacy, PROC. 5TH SYMP. ON USABLE PRIVACY AND SECURITY (SOUPS), July 2009, https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.
[64] McDonald, A. M., and Cranor, L. F. “The cost of reading privacy policies”. I/S –A Journal of Law and Policy for the Information Society 4(3), 2008.
[65] Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 471-478). ACM. See also Federal Trade Commission. 2012. Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers.
[66]Kulkarni A,Narayan S and Punia S, Users' Perspectives on Privacy Policy and Data Protection, Cuts International Retrieved from:http://snip.ly/2dfaj0#http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf
[67] Kulkarni A,Narayan S and Punia S, Users' Perspectives on Privacy Policy and Data Protection, Cuts International Retrieved from:http://snip.ly/2dfaj0#http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf
[68] Bailey R, Parsheera S, Rahman F, Sane R, Disclosures in privacy policies: Does “notice and consent” work? NIPFP Working paper series Retrieved from:https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf
[69]Section 18 of the draft Personal Data Protection Bill 2018 Retrieved from :https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

policies.[70] This situation has worsened with users interacting with increasingly complex data collection practices and accessing services through devices such as smartphones which make reading privacy policies harder.[71] The fact that no Fintech company that this research studied complied with all the provisions even of the SPD/I Rules is telling. It, then, indicates the limitations of the 'notice-and-choice' model of data privacy. While information that is provided to data subjects is necessary to be better designed, neither the SPD/I Rules, nor the the PDP Bill take into account the manner in which data flows operate in the context of Fintech business models.

Annexure 1

Clear and Accessible statements of its practices and policies

Whether the privacy policy is accessible through the main website of the body corporate?

Whether the privacy policy is mentioned or included in the terms and conditions of publicly available documents of the body corporate that collect personal information?

Whether the privacy policy can be comprehended by persons without legal knowledge?

Collection of personal or sensitive personal data/information

Type

Whether the privacy policy mentions all categories of personal information including SPD/I being collected?

Whether the privacy policy explicitly specifies the type of SPD/I being collected?

Option

Whether the Privacy Policy specifies that the user has the option to not provide information?

Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?

[70] Naidu S, Design Concerns in Creating Privacy Notices, Centre for Internet and Society, Retrieved from:https://cis-india.org/internet-governance/blog/design-concerns-in-creating-privacy-notices
[71] Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., Wetherall, D. "A Conundrum of Permissions: Installing Applications on an Android Smartphone". In Proceedings of USEC2012: Financial Cryptography and Data Security Workshop on Usable Security, March 2012.

Grievance Officer

Whether the privacy policy mentions the existence of a grievance officer?

Whether the privacy policy provides the contact information of the grievance officer?

Purpose of Collection and usage of information

Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?

Whether the privacy policy makes explicit provisioning regarding the retention of users' information?

Whether the privacy policy outlines a mechanism allowing users to review, correct and amend the information provided by the user?

Disclosure of Information

Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties?

Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?

Reasonable Security practices and procedures

Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?