PRIVACY ON THE LINE

What people in India think about their data protection and privacy

Dalberg + CGAP + FUTURE OF FINANCE
A DVARA RESEARCH INITIATIVE

INTRODUCTION

Foreword
Summary
Key Questions

Foreword

There is a growing consensus on the need for a Data Protection bill for India. With the rise in smartphone adoption, ubiquity of internet, proliferation of digital services and the introduction of Aadhaar, a unique identity for all Indians, data trails are being generated everywhere. While there is substantial documentation of benefits of capturing real time data to help businesses and government, there is little research on consumer perceptions around data protection and privacy.

Between September and November 2017, a multidisciplinary team of strategists, lawyers, designers and researchers from Dalberg, Future of Finance Initiative at Dvara Research and CGAP set out to understand 'how do ordinary citizens of India think and act on their privacy and data protection?' Some of the key questions we wanted to understand were - How aware are people about data usage? What types of data do they value? Does consent matter? What risks and harms do they perceive? How do they make trade-offs and decisions? What are their expectations from the government and service providers?

This document is a collection of insights, design principles and stories from face-to-face interviews with close to 50 people and experts spread across 4 regions of India (Maharashtra, Delhi, Tamil Nadu and Uttarakhand). The interviews used Human Centred Design (HCD) research methods that help to understand not just what people say, but how they think, act and feel. They help uncover what factors drive their decision-making and how they might make trade-offs under different scenarios. The methodology also uses co-design where people are a part of the creating solutions.

While by no means exhaustive, we believe that it provides rich insights into how people, particularly those with limited means, perceive their data protection and privacy. The document also includes guidelines, design principles and potential ideas for how policy makers and providers may consider safeguarding people from harms, and creating better awareness around data protection and privacy.

Summary

Before we embarked on the research, the overwhelming perception surrounding us was that people in India “don’t really care” about privacy. It was felt that, culturally, the concept of ‘privacy’ holds limited relevance in the Indian context and that people are more than willing to trade their data for benefits.

The research has shown us to the contrary. People value privacy for itself. People cared so deeply about their personal data such as photos, messages or browsing history that at times they did not want to share it even with trusted family members. Their personal data was only theirs to see. It could not be traded, no matter the price. Even data that consumers were more willing to share, such as transaction data or personal preferences for products like music, came with conditions. In instances where consumers were sharing data, they wanted providers to seek their consent prior to data collection and wanted a guarantee that no harm would come to them through any malicious use of their data.

People did not always understand what they were consenting to and did not have the cognitive capabilities to process them fully, routinely overlooking important clauses. However, they believed that it was a must for them to be aware of what they were signing themselves up for. Many people who could not read or write wanted more visual, verbal or video forms of consent that they could easily understand without relying on others. A one-time consent however, was not enough for people. Consumers feel that over time, they should have the right to withdraw consent or alter the form of consent, if providers use their data in additional ways, such as passing it onto third-parties.

Most people had experienced fraud (especially via phone impersonators), and did not know how to protect themselves or seek redressal. Where they had inadvertently or carelessly given away their data and suffered financial loss, they held themselves responsible. Women, in particular, were highly vulnerable to reputational harms, and self-censored themselves (for example not sharing phone number or photos) as the only way to protect themselves.

There was high trust placed in public banks and the government. Consumers had an equal measure of disbelief that these institutions or private service providers could betray this trust and share their data without their knowledge or explicit consent. In cases where harm was caused to them as a result of a data breach, they wanted providers to incur liability, government to protect their right to seek redressal, and be compensated fully.

Our conclusion is that people strongly favour a rights-based approach to data protection. In addition to rights and safeguards, they want to know how their data will be used and to give consent for collection as a means to exercise their agency. There was a strong expectation from people that the government should create laws that automatically safeguard their privacy and their data whenever it is used. Finally, they want a humanized redressal system to be in place that is affordable, trustworthy, responsive, and effective.

Key Questions

1 Do people care about privacy and data protection?

2 Are people aware of how their data is collected, stored and disseminated?

3 What do people perceive as risks and harms when it comes to their data?

4 How do people value different types of data?

5 What factors drive people’s decision and trade-offs regarding their data?

6 Do people expect to give consent to data sharing? How can it be informed?

7 To what extent do people expect to control their data?

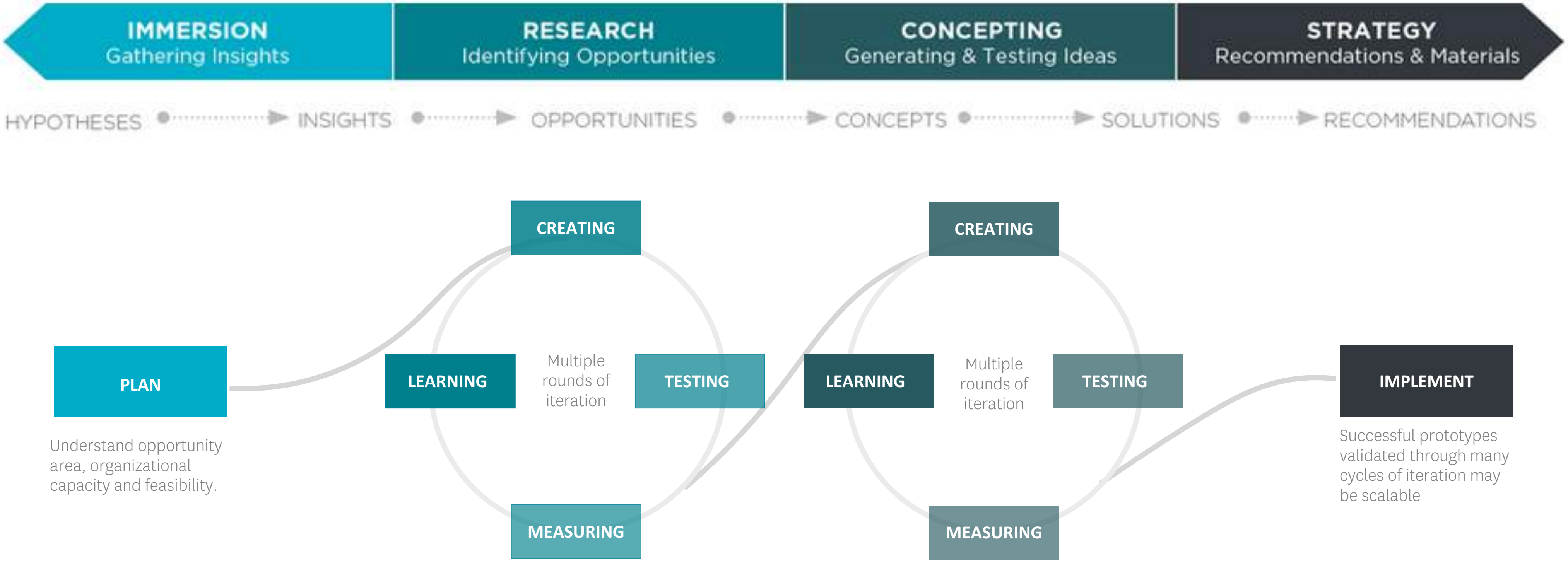
8 What do people expect from government and providers to safeguard their data?

RESEARCH METHODS

Human Centred Design
Research Locations
Research Methods
Research Tools

Human Centred Design

Human Centred Design (HCD) research enables us to gain deep empathy for users, to question core assumptions, and inspire new solutions. Our goal is to uncover insights through in-context observations of users, and learning from what they say, think, feel and do.



IMMERSION
Gathering Insights

RESEARCH
Identifying Opportunities

CONCEPTING
Generating & Testing Ideas

STRATEGY
Recommendations & Materials

HYPOTHESES → INSIGHTS → OPPORTUNITIES → CONCEPTS → SOLUTIONS → RECOMMENDATIONS

PLAN

Understand opportunity area, organizational capacity and feasibility.

CREATING

LEARNING

Multiple rounds of iteration

TESTING

MEASURING

CREATING

LEARNING

Multiple rounds of iteration

TESTING

MEASURING

IMPLEMENT

Successful prototypes validated through many cycles of iteration may be scalable

People we met

Total interviewees: 50

- Gender: 30 Men, 20 Women
- Location: 25 Urban, 25 Rural
- Age: 18 – 80 years old
- Income levels: 1-10 USD* a day
- Education: Illiterate, high school and college educated
- Mobile Ownership: Mix of none, basic and smart

In addition to demographic characteristics, each interviewee was chosen based on behaviours. Examples include:

- Village leader
- Shopkeeper accepting digital payments
- Victim of fraud
- Avid social media user
- Migrant worker

* Excluding three expert interviews

50 people 4 regions

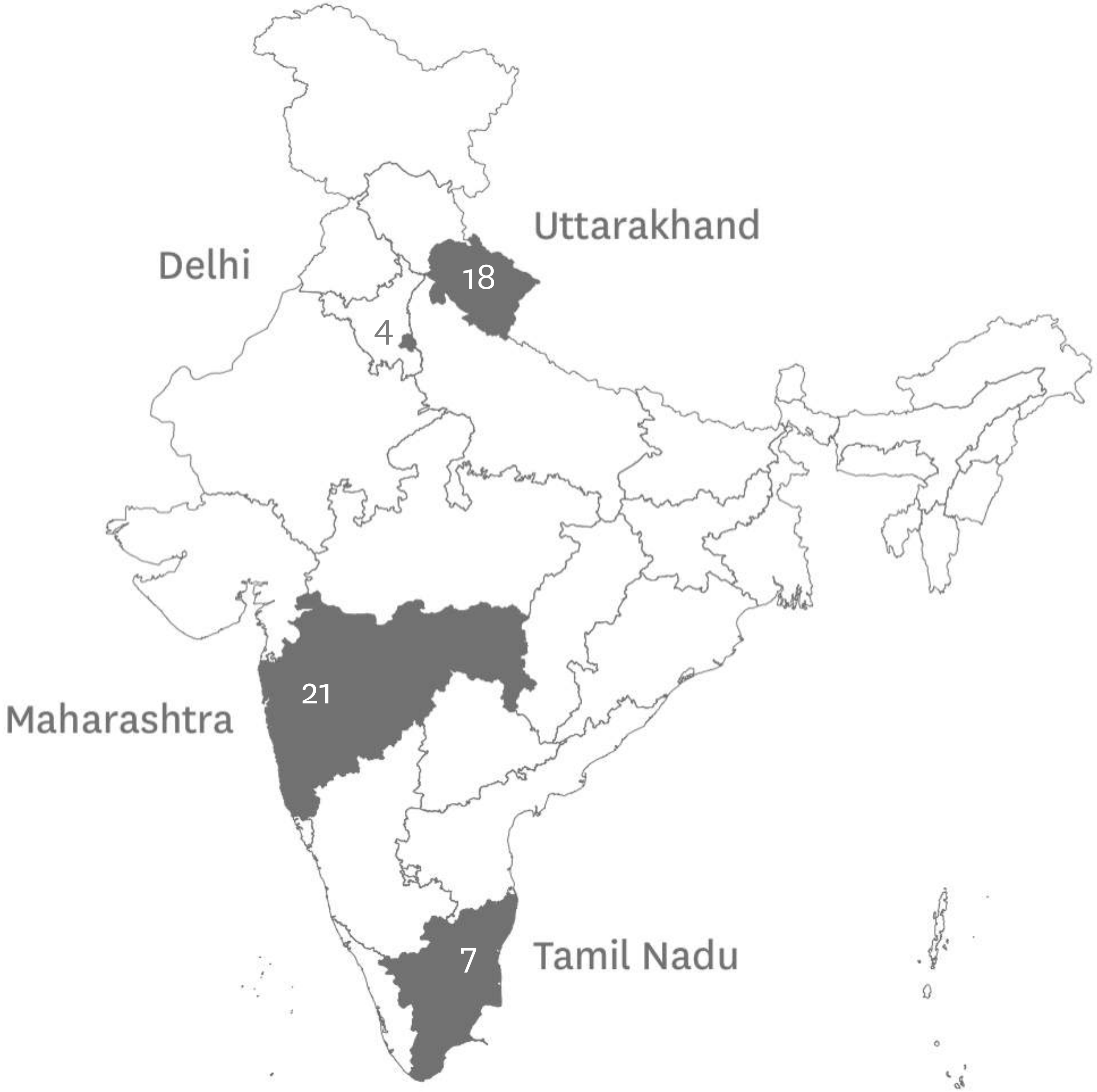
Young. Old.

Men. Women.

Literate. Illiterate.

With mobile. Without mobile.

All living on less than 10 USD* a day.



* Excluding three expert interviews

Key Research Methods

Group interviews

120 minute group interviews and co-design to test policy directions and data protection concepts.

Intercepts

15-30 minute interviews in public locations to get a wider range of perspectives on a few key questions.

In-depth interviews

90-120 min interviews with participants recruited on predefined criteria, using HCD research tools.

Observations

Shadowing key data giving locations such as banks, CSCs, Aadhaar enrolment centres, etc.

Expert Interviews

Interviews to better understand key questions that the research could answer.

Snapshot of Research Tools

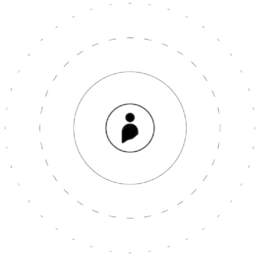
1 Customisation vs. Segmentation

2 Denial of Service

3 Data Valuation

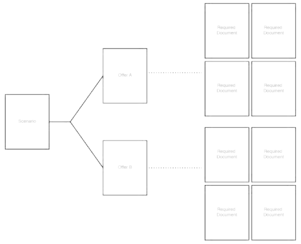
4 Same data, different contexts

5 Ecosystem trust map

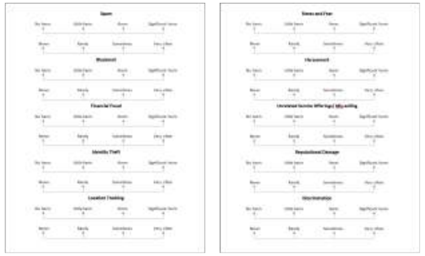


6 Shareability of Data

7 Data in Product Choice

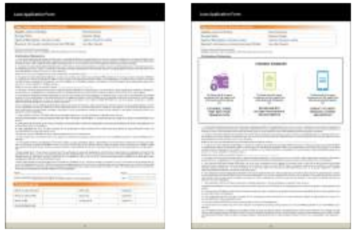


8 Mental model of harms

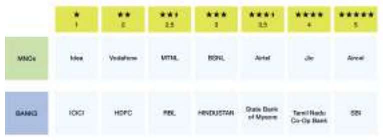


9 Data Portal

10 Consent Format

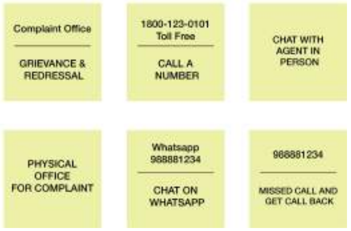


11 Five-Star Rating



	★ 1	★★ 2	★★½ 2.5	★★★ 3	★★★½ 3.5	★★★★ 4	★★★★★ 5
MNOs	Idea	Vodafone	MTNL	BSNL	Airtel	Jio	Aircel
BANKS	ICICI	HDFC	RBL	HINDUSTAN	State Bank of Mysore	Tamil Nadu Co-Op Bank	SBI

12 Grievance & Redressal



Complaint Office
GRIEVANCE & REDRESSAL

1800-123-0101 Toll Free
CALL A NUMBER

CHAT WITH AGENT IN PERSON

PHYSICAL OFFICE FOR COMPLAINT

Whatsapp 988881234
CHAT ON WHATSAPP

988881234
MISSED CALL AND GET CALL BACK

WHAT WE LEARNT

Insights
Design Principles
Ideas

Key Themes

1 PRIVACY

2 AWARENESS

3 CONSENT

4 CONTROL

5 TRUST

6 DATA SHARING

7 FRAUD

8 REPUTATIONAL HARM

9 VALUED DATA

10 REDRESSAL

1

PRIVACY

Privacy is valued in itself

People were highly protective of their personal data, at times even from trusted family members. Personal data included browsing history, WhatsApp and phone messages, call records, personal photos and videos, and GPS location data. People expected this kind of data to be kept private not always because they didn't trust others, although at times this was the case; but out of a strong sense of 'mine', 'this belongs to me', 'not someone else's business'. People did not want to be watched or seen without their permission, and were willing to go to any lengths to safeguard themselves. Privacy in relation to this kind of personal data was not a commodity to be traded. It was priceless.

“Certain kinds of data are not tradeable. Even if you give me a 100% discount, I won’t share my browsing history.”

- Sushma, Delhi

> “I do not want anyone seeing my data, especially my personal data… that is only mine to see.”

- Shakuntala, Mumbai

> “I use Appslock, which allows me to keep a separate media gallery on my phone. If the police want to access my gallery, they won’t be able to access Appslock.”

- Saddam, Mumbai

> “How is that possible? They can’t have it… What is ours will belong to us.”

- Parameshwari, Chennai

"I didn't open my Facebook account, my friend opened it for me. He put in everything, but I typed the password."

- Ganesh, Mumbai

"I used to use Whatsapp to make Video Calls to my friends, but I heard that the company stores your videos. I switched over to Facebook Messenger because I heard that was safer."

- Sapna, Mumbai

"Somethings are just personal, like shayari (poetry). I don't even want to share it with my family."

- Santosh, Uttarakhand

Make privacy the default

Privacy should be an enforceable right, where citizens can have peace of mind that they or their personal data is not watched by the state or other actors where no clear legitimate interest can be proven. Providers should be restrained about personal data collection – where it is needed, consumers should be provided with easy to understand notice of the nature and scope of collection prior to collection.

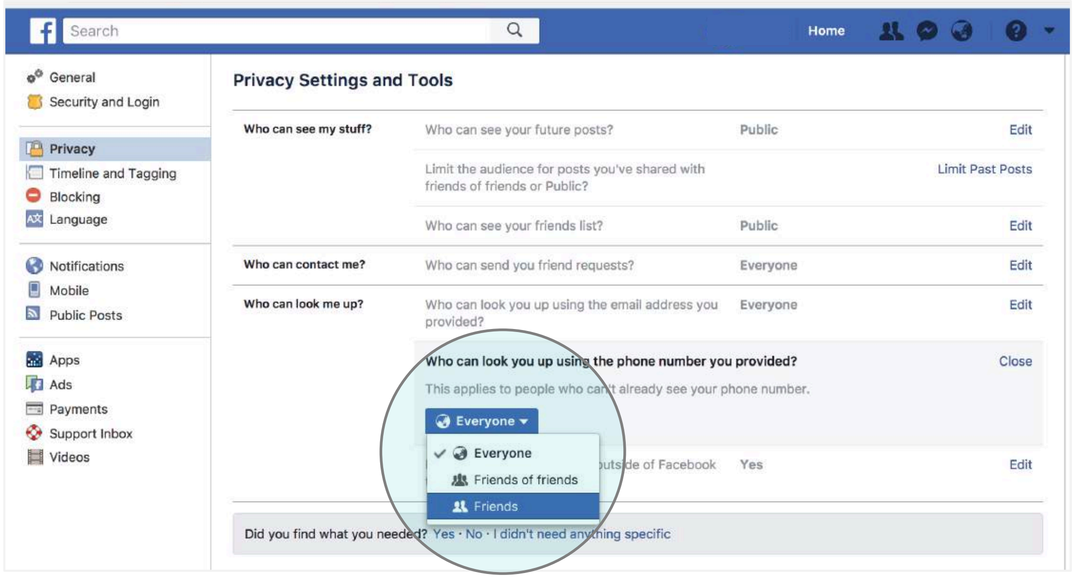
Social media websites such as Facebook can make some modifications to make privacy settings more accessible to consumers. For example, Facebook's current default setting is 'public' or 'everyone' and the option to change this is nested deep in the menu structure. Below is an illustrative example of how this could be modified to better protect privacy of the users.

ILLUSTRATIVE EXAMPLE

1. Default privacy setting

The default option for sharing personal data (such as email and phone numbers) on platforms like Facebook should be set to no one.

CURRENT | Facebook privacy interface



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Public	Edit
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
	Who can see your friends list?	Public	Edit
Who can contact me?	Who can send you friend requests?	Everyone	Edit
Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?		Close

This applies to people who can't already see your phone number.

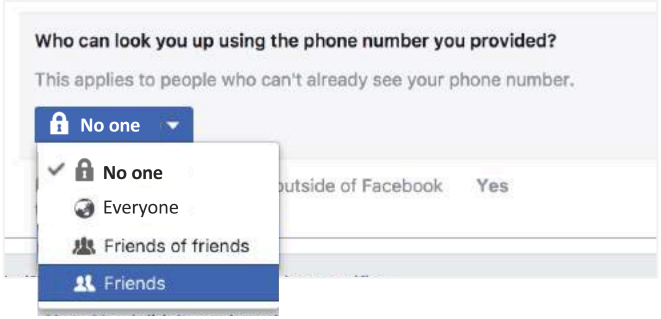
Everyone ▾
- ✓ Everyone
- Friends of friends
- Friends

...utside of Facebook Yes Edit

Did you find what you needed? Yes · No · I didn't need anything specific

'Everyone' is the default option for sharing phone number and email address

RECOMMENDED | Facebook privacy interface



Who can look you up using the phone number you provided?

This applies to people who can't already see your phone number.

No one ▾
- ✓ No one
- Everyone
- Friends of friends
- Friends

...utside of Facebook Yes

'No one' should be the default option for sharing phone number and email address

2 AWARENESS

Data is a black hole

People had little awareness of why certain types of data was demanded of them, what happened once they gave it, who else it was shared with, where it was stored, how long it was kept for and how it could be retrieved. They also had little awareness of data privacy settings beyond the mobile phone lock and password protection. Many felt they could not question a provider if asked for their data, and were unable to imagine the idea that it might be shared with third parties without their knowledge or consent. Misconceptions were also a cause of knee-jerk reactions amongst people. Amongst those who were aware, or made aware of the practice of data monitoring and sharing, there was concern as to what providers could do with their data.

“I have no idea why they ask me for this data. What do they do with it?”

- Champa, Uttarakahand

“For SIM cards, they are taking fingerprints. These must be going in the computer. But I don’t know what happens after that.”

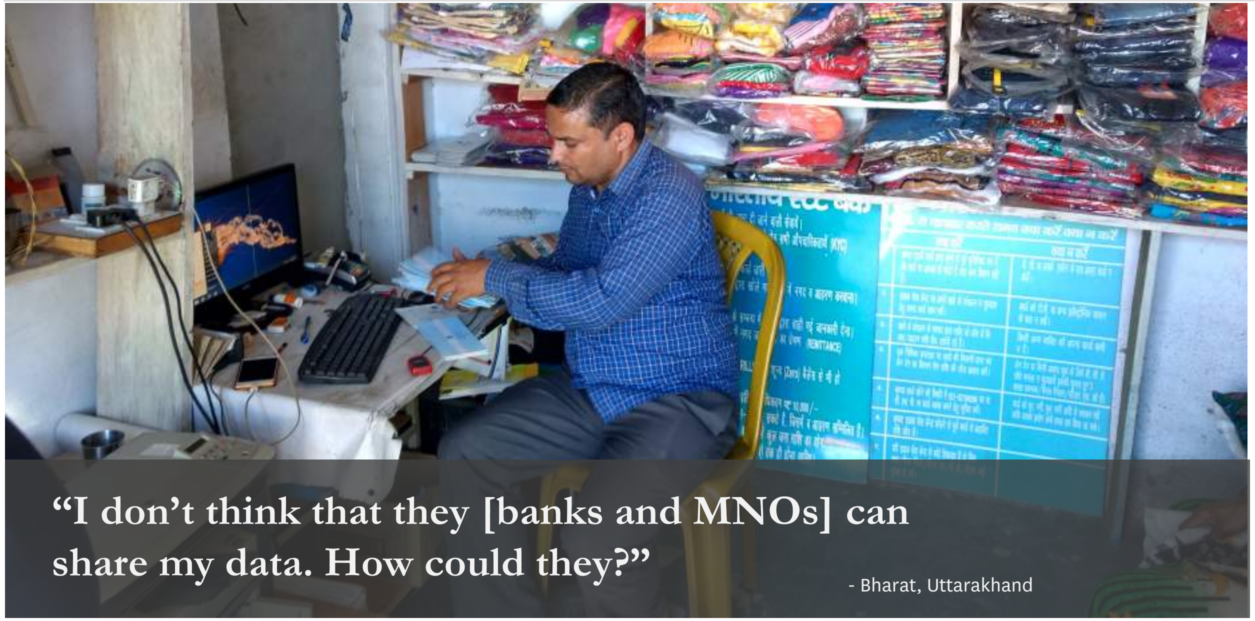
- Subhash, Uttarakhand

“Focus on education. People will protect their own data.”

- Sunil, Maharashtra

“When other banks started making offers, I started wondering about where they got my data from”

- Milind, Mumbai



"I don't think that they [banks and MNOs] can share my data. How could they?"

- Bharat, Uttarakhand

"The Government needs to spread awareness. They can easily discuss these issues at the Gram Panchayat meetings, everyone will be present, and paying attention."

- Tikam Singh Ji, Uttarakhand

> "I'm certain that banks cannot share my data. I would know, I am a Chartered Accountant, I cannot share my customer's data under any circumstances."

- Shaheda, Mumbai

Make data visible

Allow people to see how and where their data travels. Give them the right to know what happens to their data throughout its lifecycle (point of collection, service provision, transaction data, storage, sharing, etc.).

Food delivery services like Swiggy and e-commerce companies such as Amazon provide consumers with information along the course of the service/ delivery through a transparent and accurate system of notification. This staggered notification system is an analog for how providers dealing with data can also think about keeping consumers up to date about how their data is travelling and is being used.

ILLUSTRATIVE EXAMPLES

1. Missed call and SMS

Consumer could just give a missed call to receive SMS or WhatsApp that notifies them of the flow of their data across various services.

2. Swiggy/Amazon style data accountability

Consumers could view a dashboard on a mobile app or a website to view the flow of their data across various services.

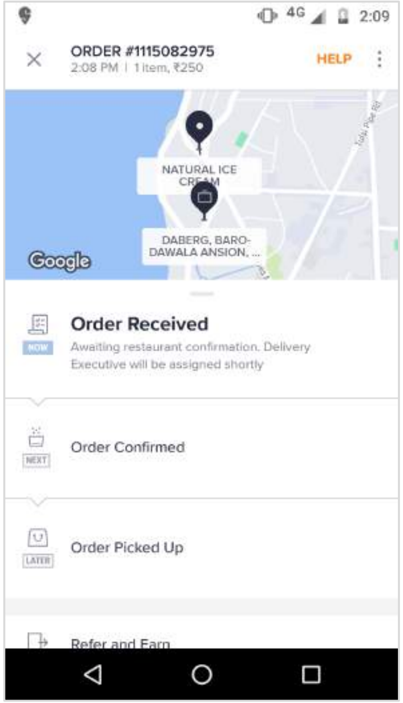
3. Safety card

Infographic like they have for flight safety explaining a basic data lifecycle to consumers across the country. Could be printed or available digitally.

4. Community awareness drives

Create awareness drives at the community level through meetings, phone messages and TV ads that educate people on how to protect themselves and their information from unauthorised use.

SWIGGY Food mobile app



ORDER #1115082975
2:08 PM | 1 item, ₹250

Order Received
Awaiting restaurant confirmation. Delivery Executive will be assigned shortly

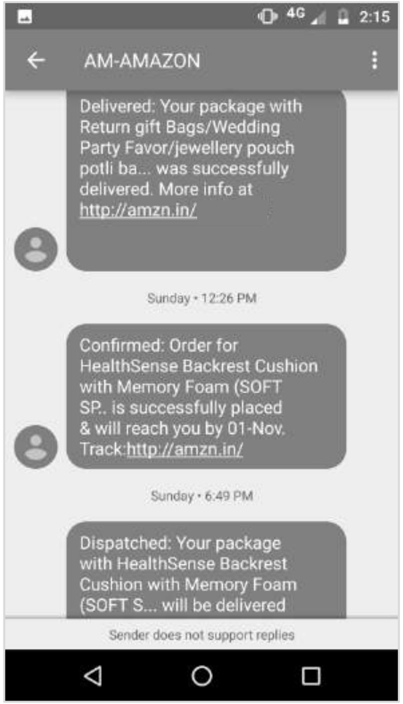
Order Confirmed

Order Picked Up

Refer and Earn

Swiggy has a mobile app as well as a website which allows consumers to track their order status. It sends email and SMS updates as well.

AMAZON E-commerce service



AM-AMAZON

Delivered: Your package with Return gift Bags/Wedding Party Favor/jewellery pouch potli ba... was successfully delivered. More info at http://amzn.in/

Sunday • 12:26 PM

Confirmed: Order for HealthSense Backrest Cushion with Memory Foam (SOFT SP.. is successfully placed & will reach you by 01-Nov. Track:http://amzn.in/

Sunday • 6:49 PM

Dispatched: Your package with HealthSense Backrest Cushion with Memory Foam (SOFT S... will be delivered

Sender does not support replies

Amazon sends SMS updates on the status of goods purchased and even shows exchange and refund status. It also has a mobile app and website.

3 CONSENT

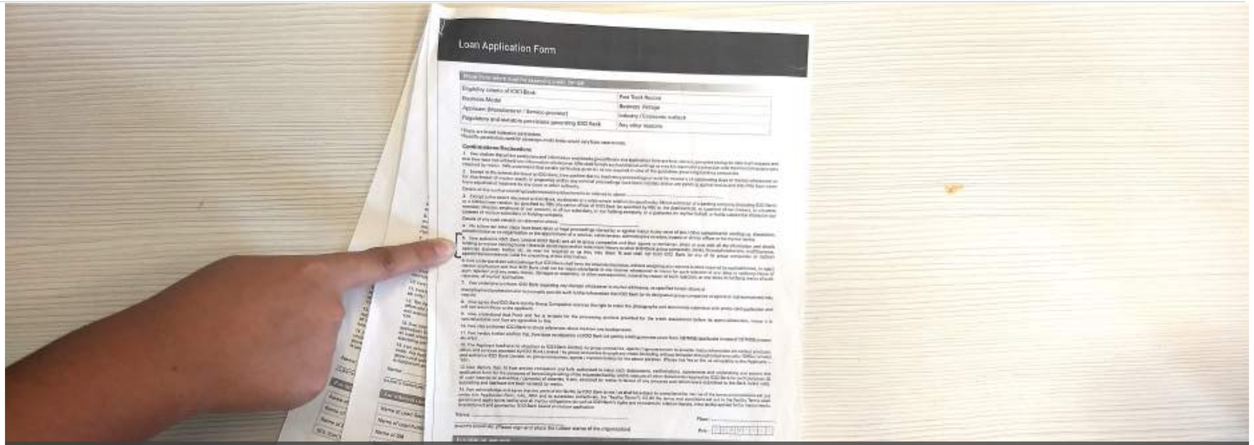
Consent is broken, but a must

Consent was perceived as necessary. People were unaware that they were giving organisations consent to use their data when they signed a terms and conditions sheet. People felt that they didn't have the knowledge, capacity or agency to engage with the lengthy, detailed and text heavy consent clauses that are currently used. Indeed, hardly anyone read consent clauses, no matter how educated. People who couldn't read or write felt that they didn't stand a chance against pages of fine print. If at all, they relied on others heavily to communicate to them what they were consenting to. The cognitive costs of consent seemed too high for people to consistently give informed consent. However, there was a natural understanding and expectation that they would be asked before any of their data would be used. Consumers expressed a unanimous wish to provide consent prior to sharing personal data, even if other safeguards and rules were to be in place. People wanted to be aware of what they were consenting to and responded enthusiastically to visual and verbal styles of consent.

> “The format of consent should be like a ‘2 minute Maggie’ video.”
>
> - Kalyani, Maharashtra

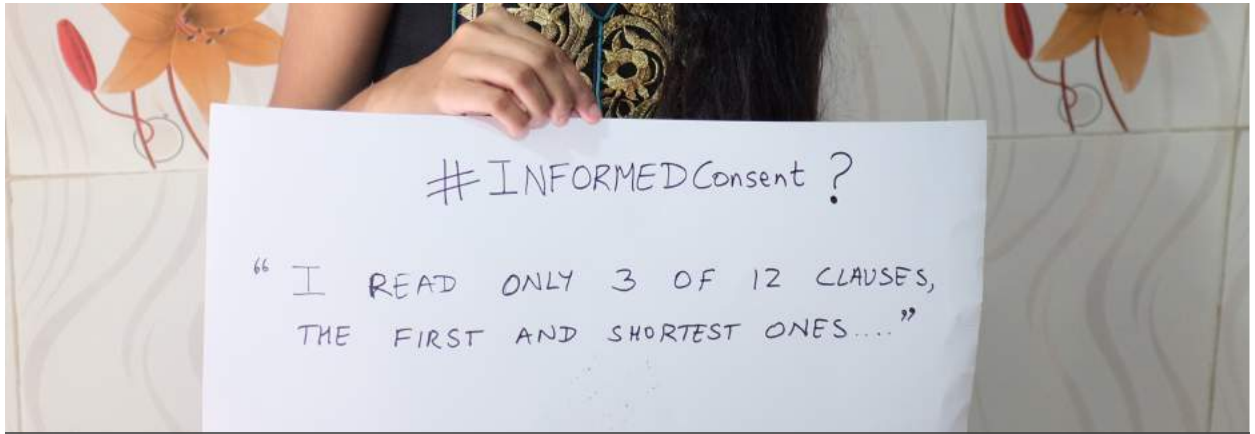
“Chhota akshar danger hota hai [The fine print is dangerous].”

- Raju, Mumbai



“If even 1% of the people actually read the terms and conditions, I did be surprised.”

- Sanjay, Uttarakhand

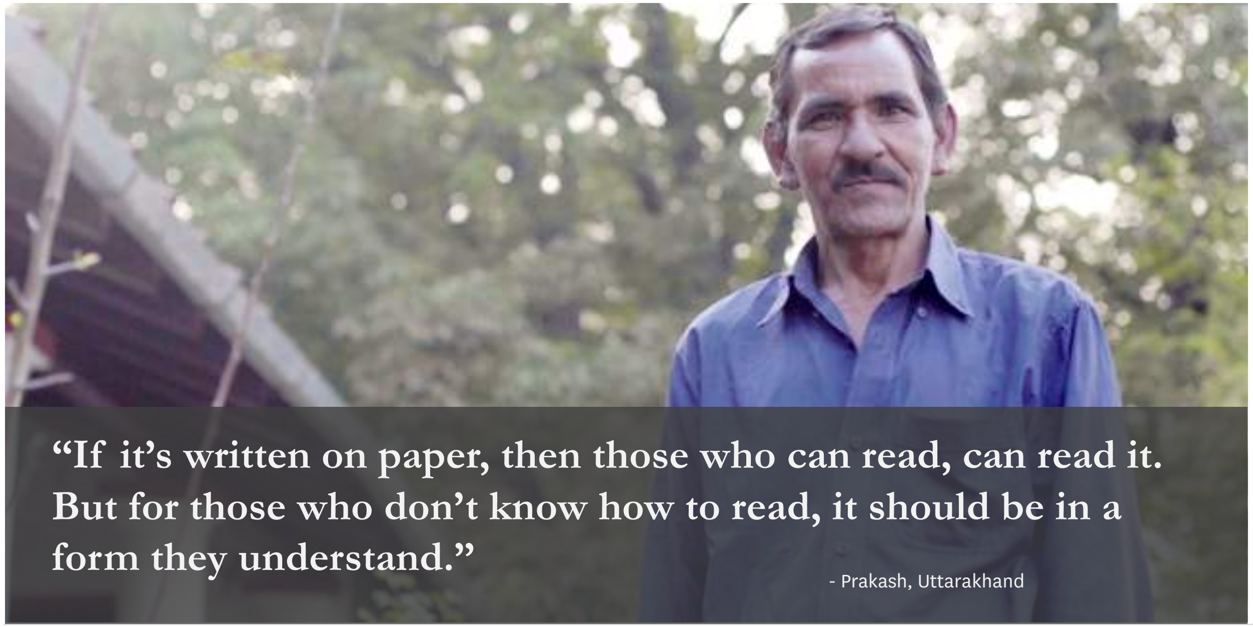

#INFORMEDConsent ?
“I READ ONLY 3 OF 12 CLAUSES, THE FIRST AND SHORTEST ONES....”

“I read the first line, because it’s probably the most important, and the shortest two lines. I skipped everything else.”

- Varsha, Mumbai

“Option should be given to everyone and it should be communicated well.”

- Mohamed, Mumbai



“If it’s written on paper, then those who can read, can read it. But for those who don’t know how to read, it should be in a form they understand.”

- Prakash, Uttarakhand

“Those who aren’t educated ask me to fill in their LIC forms for them. How will they protect themselves and provide consent?”

- Yashpal, Uttarakhand

Make consent understandable at a glance

Providers should be held to rigorous standards to design consent in a simple way that consumers, even the ones who cannot read or write, understand at a glance. The language of consent should fit that of the person giving consent.

Prototype consent forms developed by Dalberg resonated highly with respondents. While short, clear, video-based consent explanations were preferred by most people, their larger underlying ask was for consent to come in a more understandable form.

ILLUSTRATIVE EXAMPLES

1. Pictorial consent forms

Have graphic representations of things people are consenting to.
The short captions could be in regional languages.

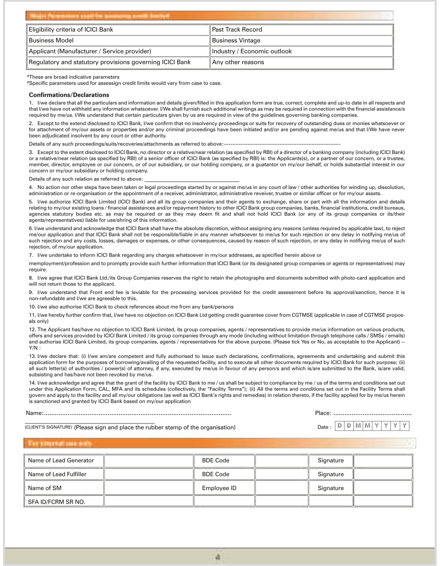
2. Video consent

Video consent, created in the style of an advertisement, holds high potential as it is a format that is easy to understand across consumer segments and is also more easy to scale than having a dedicated personnel to explain terms and conditions.

3. Verbal/phone based consent

Having a representative at the point of data collection/ contact the consumer, who is responsible for clearly explaining the utilisation of data.

CURRENT Loan application form



Major Parameters used for assessing credit limits#

Eligibility criteria of ICICI Bank	Past Track Record
Business Model	Business Vintage
Applicant (Manufacturer / Service provider)	Industry / Economic outlook
Regulatory and statutory provisions governing ICICI Bank	Any other reasons

#These are broad indicative parameters
#Specific parameters used for assessign credit limits would vary from case to case.

Confirmations/Declarations

1. I/we declare that all the particulars and information and details given/filled in this application form are true, correct, complete and up-to date in all respects and that I/we have not withheld any information whatsoever. I/We shall furnish such additional writings as may be required in connection with the financial assistance/s required by me/us. I/We understand that certain particulars given by us are required in view of the guidelines governing banking companies.

2. Except to the extend disclosed to ICICI Bank, I/we confirm that no insolvency proceedings or suits for recovery of outstanding dues or monies whatsoever or for attachment of my/our assets or properties and/or any criminal proceedings have been initiated and/or are pending against me/us and that I/We have never been adjudicated insolvent by any court or other authority.

Details of any such proceedings/suits/recoveries/attachments as referred to above:---

3. Except to the extent disclosed to ICICI Bank, no director or a relative/near relation (as specified by RBI) of a director of a banking company (including ICICI Bank) or a relative/near relation (as specified by RBI) of a senior officer of ICICI Bank (as specified by RBI) is: the Applicants(s), or a partner of our concern, or a trustee, member, director, employee or our concern, or of our subsidiary, or our holding company, or a guatantor on my/our behalf, or holds substantial interest in our concern or my/our subsidiary or holding company.

Details of any such relation as referred to above: ___________________________________

4. No action nor other steps have been taken or legal proceedings started by or against me/us in any court of law / other authorities for winding up, dissolution, administration or re-organisation or the appointment of a receiver, administrator, administrative reveiver, trustee or similar officer or for my/our assets.

5. I/we authorize ICICI Bank Limited (ICICI Bank) and all its group companies and their agents to exchange, share or part with all the information and details relating to my/our existing loans / financial assistances and/or repayment history to other ICICI Bank group companies, banks, financial institutions, credit bureaus, agencies statutory bodies etc. as may be required or as they may deem fit and shall not hold ICICI Bank (or any of its group companies or its/their agents/representatives) liable for use/shring of this information.

6. I/we understand and acknowledge that ICICI Bank shall have the absolute discretion, without assigning any reasons (unless required by applicable law), to reject me/our application and that ICICI Bank shall not be responsible/liable in any manner whatsoever to me/us for such rejection or any delay in notifying me/us of such rejection and any costs, losses, damages or expenses, or other consequences, caused by reason of such rejection, or any delay in notifying me/us of such rejection, of my/our application.

7. I/we undertake to inform ICICI Bank regarding any charges whatsoever in my/our addresses, as specified herein above or

memployment/profession and to promptly provide such further information that ICICI Bank (or its designated group companies or agents or representatives) may require.

8. I/we agree that ICICI Bank Ltd./its Group Companies reserves the right to retain the photographs and documents submitted with photo-card application and will not return those to the applicant.

9. I/we understand that Front end fee is leviable for the processing services provided for the credit assessment before its approval/sanction, hence it is non-refundable and I/we are agreeable to this.

10. I/we also authorise ICICI Bank to check references about me from any bank/persons

11. I/we hereby further confirm that, I/we have no objection on ICICI Bank Ltd getting credit guarantee cover from CGTMSE (applicable in case of CGTMSE proposals only)

12. The Applicant has/have no objection to ICICI Bank Limited, its group companies, agents / representatives to provide me/us information on various products, offers and services provided by ICICI Bank Limited / its group companies through any mode (including without limitation through telephone calls / SMSs / emails) and authorise ICICI Bank Limited, its group companies, agents / representatives for the above purpose. (Please tick Yes or No, as acceptable to the Applicant) -- Y/N :

13. I/we declare that: (i) I/we am/are competent and fully authorised to issue such declarations, confirmations, agreements and undertaking and submit this application form for the purposes of borrowing/availing of the requested facility, and to execute all other documents required by ICICI Bank for such purpose; (ii) all such letter(s) of authorities / power(s) of attorney, if any, executed by me/us in favour of any person/s and which is/are submitted to the Bank, is/are valid, subsisting and has/have not been revoked by me/us.

14. I/we acknowledge and agree that the grant of the facility by ICICI Bank to me / us shall be subject to compliance by me / us of the terms and conditions set out under this Application Form, CAL, MFA and its schedules (collectively, the "Facility Terms"); (ii) All the terms and conditions set out in the Facility Terms shall govern and apply to the facility and all my/our obligations (as well as ICICI Bank's rights and remedies) in relation thereto, if the facility applied for by me/us herein is sanctioned and granted by ICICI Bank based on my/our application

Name:.. Place: ....

(CLIENT'S SIGNATURE) (Please sign and place the rubber stamp of the organisation) Date : D D M M Y Y Y Y

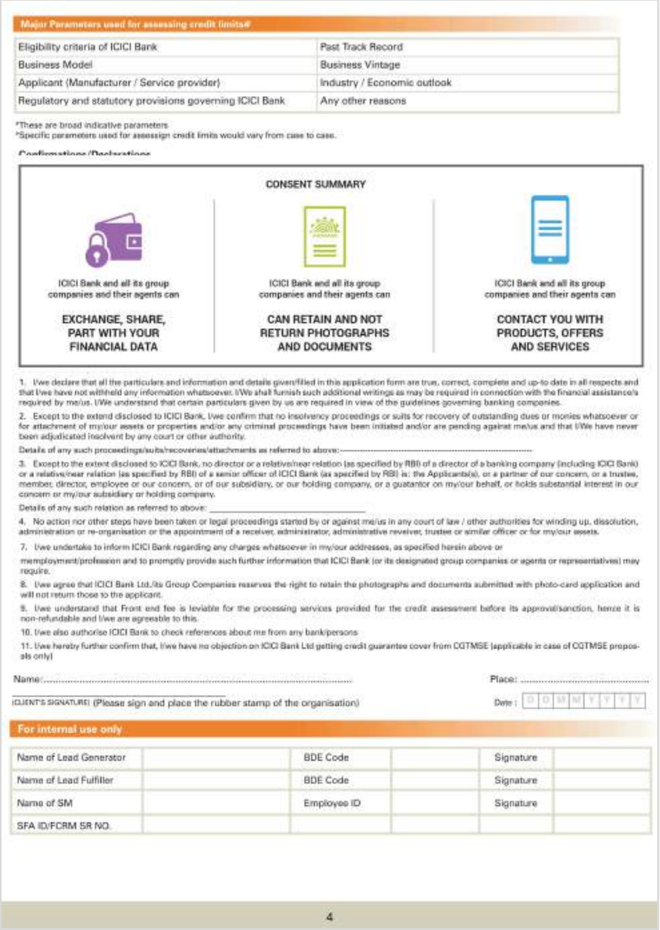
For internal use only

Name of Lead Generator		BDE Code		Signature	
Name of Lead Fulfiller		BDE Code		Signature	
Name of SM		Employee ID		Signature	
SFA ID/FCRM SR NO.					

4

Fine print, long clauses, technical language and lack of awareness by consumers contribute to almost no one understanding or reading consent forms.

RECOMMENDED Pictorial loan application form



Major Parameters used for assessing credit limits#

Eligibility criteria of ICICI Bank	Past Track Record
Business Model	Business Vintage
Applicant (Manufacturer / Service provider)	Industry / Economic outlook
Regulatory and statutory provisions governing ICICI Bank	Any other reasons

#These are broad indicative parameters
#Specific parameters used for assessign credit limits would vary from case to case.

Confirmations /Declarations

CONSENT SUMMARY

ICICI Bank and all its group companies and their agents can
EXCHANGE, SHARE, PART WITH YOUR FINANCIAL DATA

ICICI Bank and all its group companies and their agents can
CAN RETAIN AND NOT RETURN PHOTOGRAPHS AND DOCUMENTS

ICICI Bank and all its group companies and their agents can
CONTACT YOU WITH PRODUCTS, OFFERS AND SERVICES

1. I/we declare that all the particulars and information and details given/filled in this application form are true, correct, complete and up-to date in all respects and that I/we have not withheld any information whatsoever. I/We shall furnish such additional writings as may be required in connection with the financial assistance/s required by me/us. I/We understand that certain particulars given by us are required in view of the guidelines governing banking companies.

2. Except to the extend disclosed to ICICI Bank, I/we confirm that no insolvency proceedings or suits for recovery of outstanding dues or monies whatsoever or for attachment of my/our assets or properties and/or any criminal proceedings have been initiated and/or are pending against me/us and that I/We have never been adjudicated insolvent by any court or other authority.

Details of any such proceedings/suits/recoveries/attachments as referred to above:---

3. Except to the extent disclosed to ICICI Bank, no director or a relative/near relation (as specified by RBI) of a director of a banking company (including ICICI Bank) or a relative/near relation (as specified by RBI) of a senior officer of ICICI Bank (as specified by RBI) is: the Applicants(s), or a partner of our concern, or a trustee, member, director, employee or our concern, or of our subsidiary, or our holding company, or a guatantor on my/our behalf, or holds substantial interest in our concern or my/our subsidiary or holding company.

Details of any such relation as referred to above: ___________________________________

4. No action nor other steps have been taken or legal proceedings started by or against me/us in any court of law / other authorities for winding up, dissolution, administration or re-organisation or the appointment of a receiver, administrator, administrative reveiver, trustee or similar officer or for my/our assets.

7. I/we undertake to inform ICICI Bank regarding any charges whatsoever in my/our addresses, as specified herein above or

memployment/profession and to promptly provide such further information that ICICI Bank (or its designated group companies or agents or representatives) may require.

8. I/we agree that ICICI Bank Ltd./its Group Companies reserves the right to retain the photographs and documents submitted with photo-card application and will not return those to the applicant.

9. I/we understand that Front end fee is leviable for the processing services provided for the credit assessment before its approval/sanction, hence it is non-refundable and I/we are agreeable to this.

10. I/we also authorise ICICI Bank to check references about me from any bank/persons

11. I/we hereby further confirm that, I/we have no objection on ICICI Bank Ltd getting credit guarantee cover from CGTMSE (applicable in case of CGTMSE proposals only)

Name:.. Place: ....

(CLIENT'S SIGNATURE) (Please sign and place the rubber stamp of the organisation) Date : D D M M Y Y Y Y

For internal use only

Name of Lead Generator		BDE Code		Signature	
Name of Lead Fulfiller		BDE Code		Signature	
Name of SM		Employee ID		Signature	
SFA ID/FCRM SR NO.					

4

Recommended direction for pictorial consent form – succinct and in simple steps.

4

CONTROL

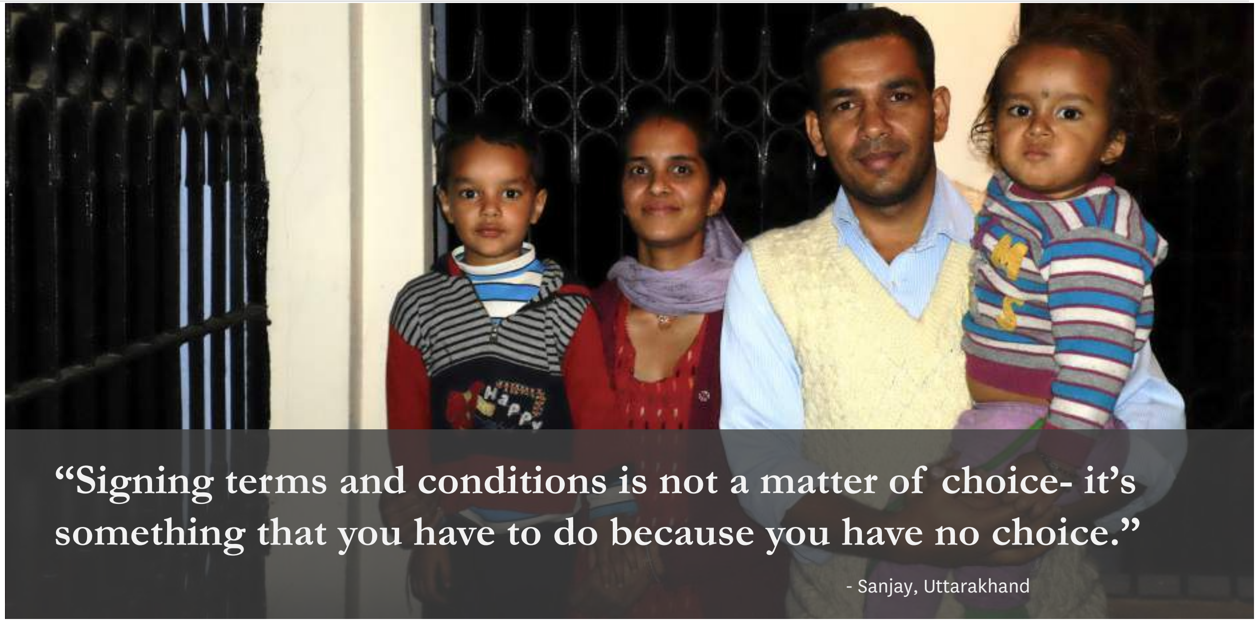
Control was desired even after consent

People did not want to provide blanket consent and hold the expectation that consent will be asked for at each step along the way. They wanted consent to be to-the-point and clearly linked to the service provision moment. People expressed the desire to have some bargaining power in the form of even a partial or limited service option rather than a complete denial of service in the absence of complete consent. Furthermore, giving consent did not indicate to people a loss of ownership over their data. Consent was seen as the first step to a transaction or the beginning of a relationship with the provider. Consumers want control and continued engagement after this initial consent, with the ability to modify their information and retrieve it in the event of discontinued service such as switching to another provider.

> “Data should be used in a ‘step-to-step’ basis… only when required.”
>
> - Varsha, Mumbai

> "I should have control over my data or it should be allowed by law."

- Shaheda, Mumbai



> "Signing terms and conditions is not a matter of choice- it's something that you have to do because you have no choice."

- Sanjay, Uttarakhand

> "I should have the right to withdraw and alter my consent."

- Yashpal, Uttarakhand

"Data should not be stored once the service is completed."

- Milind, Mumbai

"How can they share my data? They need to ask me first."

- Parameshwari, Chennai

"Personal information should not be retained by companies after the service is discontinued."

- Anand, Uttarakhand

Allow people ongoing control of their data

Make it easy for people to view who has what type of their data, for how long they've had it. Give people the right to withdraw or rectify their data from providers or services they're no longer using. Give people comfort through rules that data will be held only as long as needed.

Smartphone applications on Android operating systems ask for consent to access data only at the moment that it is required, including an option to revoke permission that is already given. This can be replicated on a multiple channels, not just on smartphones.

ILLUSTRATIVE EXAMPLES

1. 'Just in time' consent

Ask consumers for consent right before they are going to perform an action which involves sharing of their data using SMS, phone call or mobile app notification.

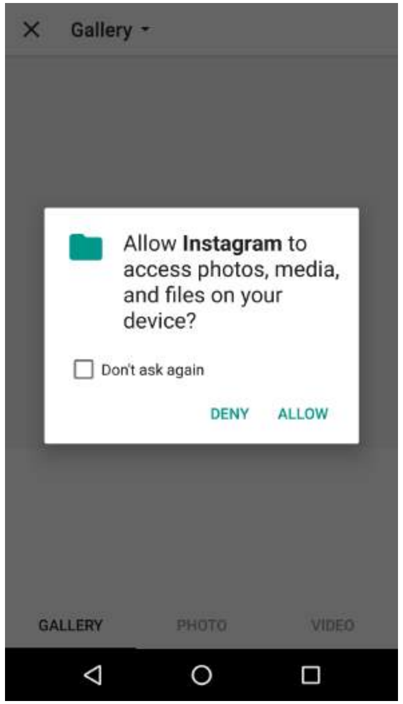
2. Modify data sharing privileges

Allow consumers to go back at any point and revoke or modify data sharing privileges granted to a service using an SMS or mobile app/website.

3. Data dashboard

Provide consumers a dashboard that displays all the data that they have consented to give, giving them the option to revoke their consent, highlighting known risks and providing tips and tricks to stay protected.

INSTAGRAM mobile app



Gallery

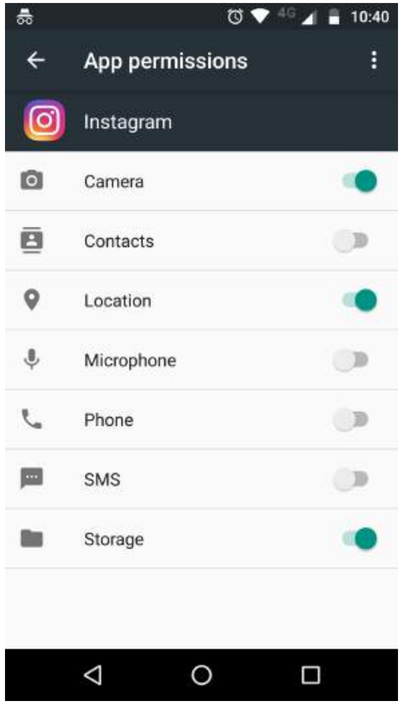
Allow **Instagram** to access photos, media, and files on your device?

□ Don't ask again

DENY ALLOW

'Just in time' consent on Instagram app through a pop-up, asking permission from the user right before posting a photo/video using the app.

ANDROID app permissions



10:40

App permissions

Instagram

Camera ●

Contacts ○

Location ●

Microphone ○

Phone ○

SMS ○

Storage ●

App permissions for Instagram where a consumer can revoke data sharing privileges for different types of data at anytime.

5 TRUST

Guarantee trumps benefit

While 'data that only belongs to me' was sacred and untradeable, there were other types of data (such as contact details, transaction data, or social media preferences, etc.) where people wanted a guarantee, more than any benefit. They wanted 100% assurance of the credibility of the person and/ or institution behind it, that it will not be misused, and no harm will be caused to them. They wanted a clear rationale for why the data was being demanded of them. Small costs or benefits didn't matter as much as trustworthiness. Government was often the most trusted institution followed closely by public banks and then by private banks or MNOs – social media companies were trusted the least. People expected that those they placed the most trust in would never betray them by doing things that were not in their interest.

> “If the company people are not keeping my data safe and sharing it, then I will avoid the company.”

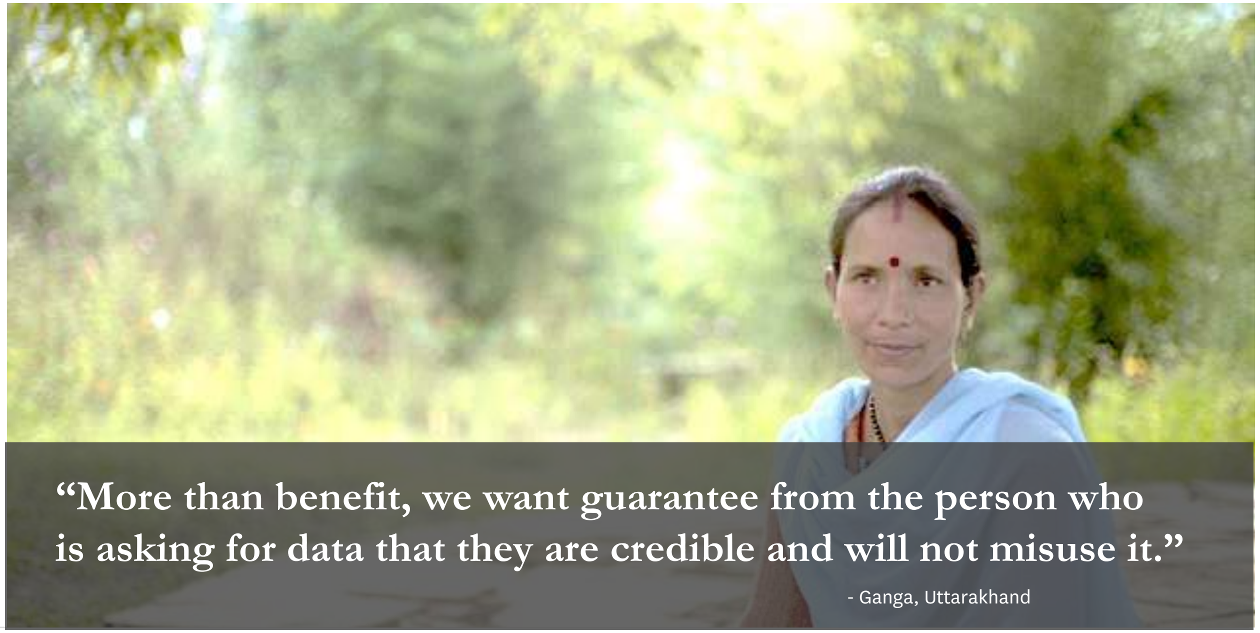
- Rubina, Mumbai

“If provided safety and guarantee I am willing to pay a small premium.”

- Kokila, Chennai

“I trust the Government, but not the politicians.”

- Sunita, Uttarakhand



“More than benefit, we want guarantee from the person who is asking for data that they are credible and will not misuse it.”

- Ganga, Uttarakhand

“If banks take responsibility for protecting my data, I am willing to share it.”

- Parameshwari and Palaniyandi, Chennai

“My data could also be misused, the bank or mobile company should not be allowed to do anything wrong, and should be responsible for anything that does go wrong.”

- Tikam Singh Ji, Uttarakhand

> “If someone asks me for my documents, I will ask them for theirs.”

- Kamla, Uttarakhand

Create a trust code or rating system

People trust the government to set rules around data practices to protect them. In addition, it would help to set up a code of conduct or rating system for providers to allow consumers to easily differentiate between those with good data practices (such as secure data storage, stringent third-party sharing norms, etc.) and those without. This will allow consumers to make more informed choices in provider selection, accounting for individual preferences on privacy and data protection.

Smartphone applications on Android operating systems ask for consent to access data only at the moment that it is required, including an option to revoke permission that is already given.

ILLUSTRATIVE EXAMPLES

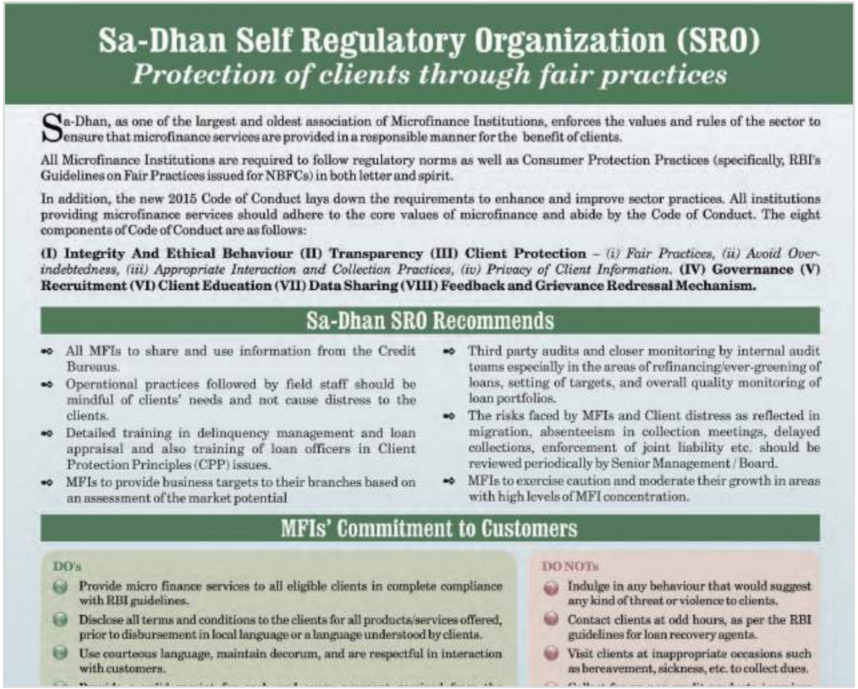
1. Code of conduct

Incentivise industry players like banks, MNOs and social media companies to develop and publicize a trust code for consumer data protection.

2. Rating system

Pass a legislation to mandate industry players like banks, MNOs and social media companies to come up with a '5 star rating' system on data protection which will be monitored by third party auditors.

SA-DHAN for code of conduct



Sa-Dhan Self Regulatory Organization (SRO)

Protection of clients through fair practices

Sa-Dhan, as one of the largest and oldest association of Microfinance Institutions, enforces the values and rules of the sector to ensure that microfinance services are provided in a responsible manner for the benefit of clients.

All Microfinance Institutions are required to follow regulatory norms as well as Consumer Protection Practices (specifically, RBI's Guidelines on Fair Practices issued for NBFCs) in both letter and spirit.

In addition, the new 2015 Code of Conduct lays down the requirements to enhance and improve sector practices. All institutions providing microfinance services should adhere to the core values of microfinance and abide by the Code of Conduct. The eight components of Code of Conduct are as follows:

(I) Integrity And Ethical Behaviour (II) Transparency (III) Client Protection – *(i) Fair Practices, (ii) Avoid Over-indebtedness, (iii) Appropriate Interaction and Collection Practices, (iv) Privacy of Client Information.* **(IV) Governance (V) Recruitment (VI) Client Education (VII) Data Sharing (VIII) Feedback and Grievance Redressal Mechanism.**

Sa-Dhan SRO Recommends

- All MFIs to share and use information from the Credit Bureaus.
- Operational practices followed by field staff should be mindful of clients' needs and not cause distress to the clients.
- Detailed training in delinquency management and loan appraisal and also training of loan officers in Client Protection Principles (CPP) issues.
- MFIs to provide business targets to their branches based on an assessment of the market potential
- Third party audits and closer monitoring by internal audit teams especially in the areas of refinancing/ever-greening of loans, setting of targets, and overall quality monitoring of loan portfolios.
- The risks faced by MFIs and Client distress as reflected in migration, absenteeism in collection meetings, delayed collections, enforcement of joint liability etc. should be reviewed periodically by Senior Management / Board.
- MFIs to exercise caution and moderate their growth in areas with high levels of MFI concentration.

MFIs' Commitment to Customers

DO's

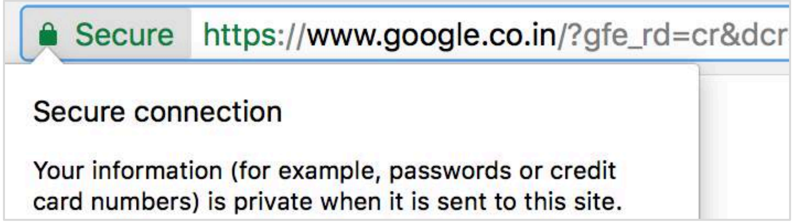
- Provide micro finance services to all eligible clients in complete compliance with RBI guidelines.
- Disclose all terms and conditions to the clients for all products/services offered, prior to disbursement in local language or a language understood by clients.
- Use courteous language, maintain decorum, and are respectful in interaction with customers.

DO NOT's

- Indulge in any behaviour that would suggest any kind of threat or violence to clients.
- Contact clients at odd hours, as per the RBI guidelines for loan recovery agents.
- Visit clients at inappropriate occasions such as bereavement, sickness, etc. to collect dues.

Sa-dhan is an RBI recognized self regulating organisation for MFIs that has formulated its own code of conduct for consumer protection.

'GREEN PADLOCK' rating system



Secure https://www.google.co.in/?gfe_rd=cr&dcr

Secure connection

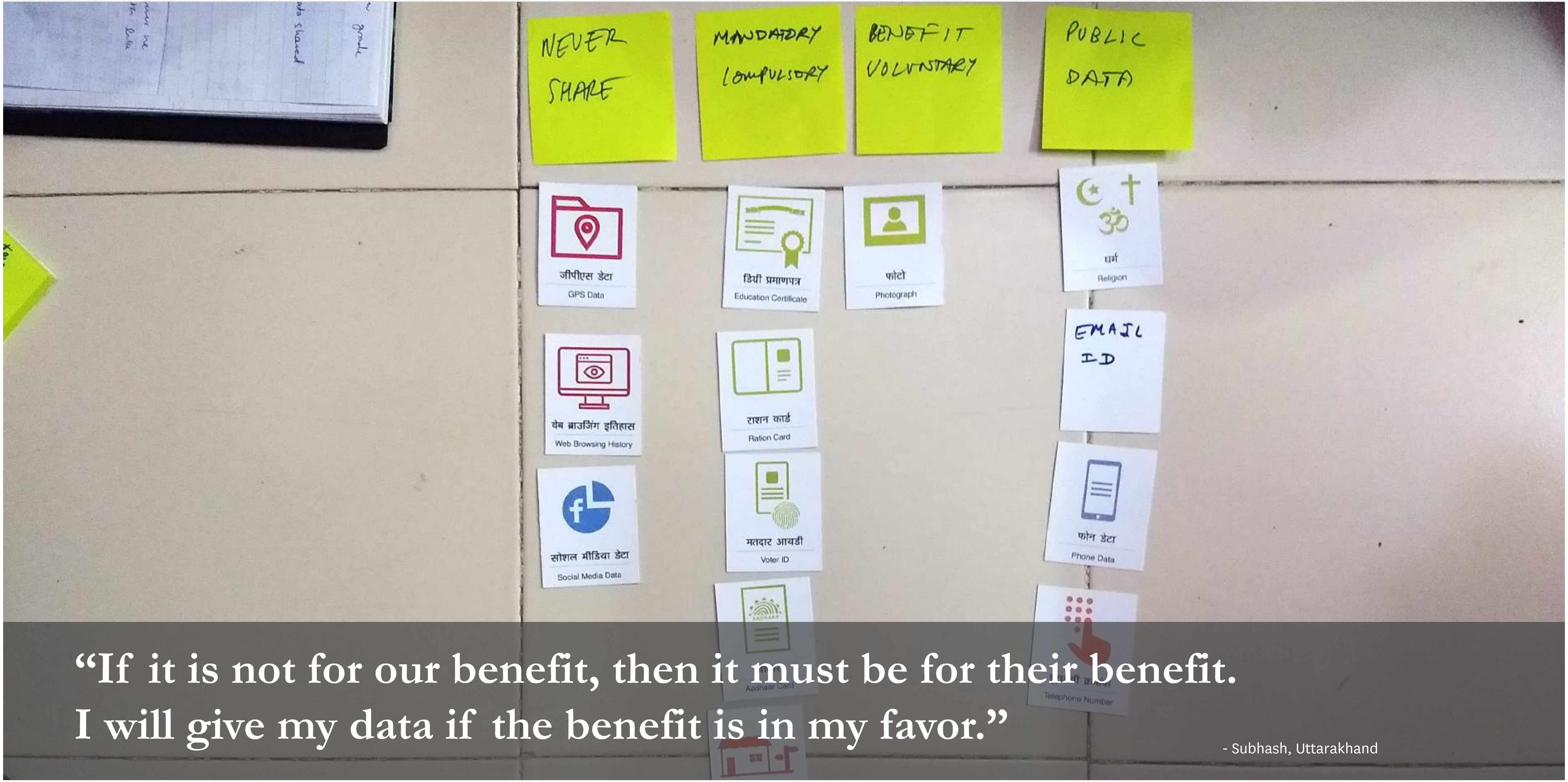
Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

'Green padlock' icon with 'Secure' text signifies that data will be encrypted and kept private to the website being used.

6 DATA SHARING

Show me the benefit if you want my data

If a guarantee was in place, some people were willing to consider the benefits of third party data sharing, as long as it was clear what those benefits were and the trade-offs they were making. The shareable data in this case included things such as their contact details, transaction data, social media preferences etc. Sometimes these benefits were individual (more personalised offers, better discounts, etc.), but at times they were collective in nature (for example for providers to be able to identify a SIM card owner easily in case of fraud). It's important to note people wanted customised offers, not generic ones in exchange for their data. They did not want to be bombarded by telemarketers selling them things they did not need. There was a clear line between feeling 'valued' as a customer and a 'target for spam' with unnecessary offers.



> "If it is not for our benefit, then it must be for their benefit. I will give my data if the benefit is in my favor."

- Subhash, Uttarakhand

“If I receive a benefit from sharing my data, I am willing to do so.”

- Sushma, Delhi

“If Myntra (online shopping platform) sells my data to other parties and benefits from it, that’s ok. Data sharing for customized marketing purposes is a beneficial thing for me.”

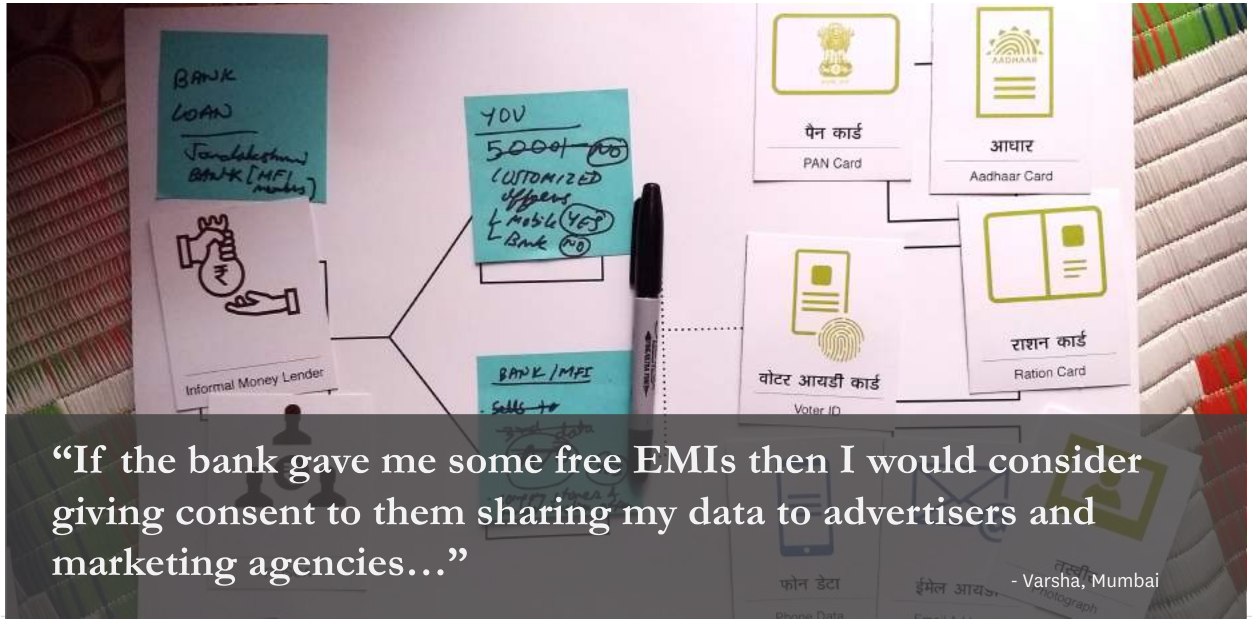
- Kalyani, Maharashtra

“Data usage for justifiable business practice is okay. Companies should keep record of data only when it is mandatory.”

- Sunil, Maharashtra

“Aadhar will result in an increase in tax collection for the country, which will help everyone.”

- Sunita, Uttarakhand



“If the bank gave me some free EMIs then I would consider giving consent to them sharing my data to advertisers and marketing agencies…”

- Varsha, Mumbai

“If there is no benefit why would I give my data? Only if the company tells me upfront, I am okay with it, however that rarely happens.”

- Prashant, Mumbai

Make benefits and risks of data sharing tangible

People want to have a clear understanding of who is benefiting and how. They want to know how they're benefiting versus the community or the providers or the government as a result of their data sharing. Providers who requested data beyond legitimate interest (what is needed for effective service provision or mandated by the law) need to be able to clearly articulate costs versus benefits to the users.

Mechanisms to clearly communicate risks and benefits to consumers, such as the Schumer box, which mandates norms for clear disclosure, have been introduced in the USA as well as the UK.

ILLUSTRATIVE EXAMPLES

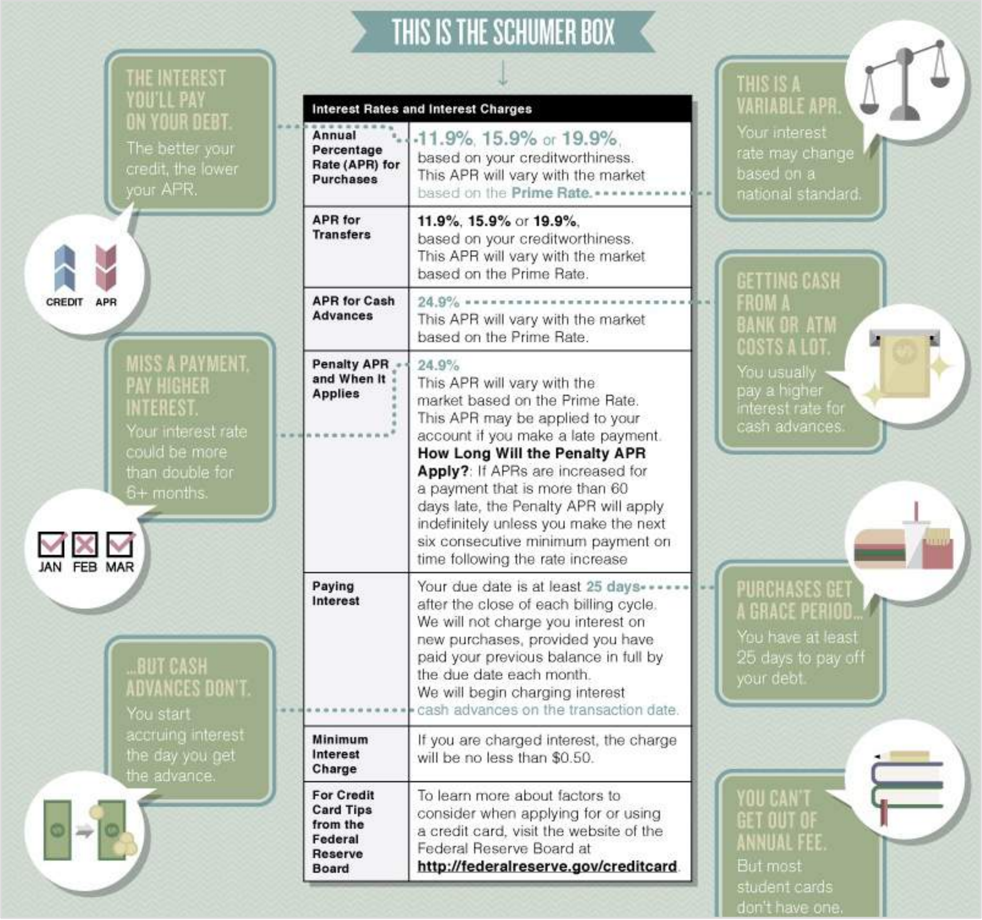
1. ‘Schumer box’ for India

Banks, MNOs, social media companies should mandatorily display their data sharing risks and benefits to consumers in the style of a Schumer Box and make it available as a printed and digital copy.

2. Awareness sessions

Government to conduct localized community level awareness sessions periodically at the village and town levels to make the benefits and risks of common services like bank account, loans, social media, sim cards, etc. clear to consumers.

SCHUMER BOX infographic



THIS IS THE SCHUMER BOX

Interest Rates and Interest Charges	
Annual Percentage Rate (APR) for Purchases	11.9%, 15.9% or 19.9%, based on your creditworthiness. This APR will vary with the market based on the **Prime Rate.**
APR for Transfers	**11.9%**, **15.9%** or **19.9%**, based on your creditworthiness. This APR will vary with the market based on the Prime Rate.
APR for Cash Advances	24.9% This APR will vary with the market based on the Prime Rate.
Penalty APR and When It Applies	24.9% This APR will vary with the market based on the Prime Rate. This APR may be applied to your account if you make a late payment. **How Long Will the Penalty APR Apply?**: If APRs are increased for a payment that is more than 60 days late, the Penalty APR will apply indefinitely unless you make the next six consecutive minimum payment on time following the rate increase
Paying Interest	Your due date is at least 25 days after the close of each billing cycle. We will not charge you interest on new purchases, provided you have paid your previous balance in full by the due date each month. We will begin charging interest cash advances on the transaction date.
Minimum Interest Charge	If you are charged interest, the charge will be no less than $0.50.
For Credit Card Tips from the Federal Reserve Board	To learn more about factors to consider when applying for or using a credit card, visit the website of the Federal Reserve Board at **http://federalreserve.gov/creditcard**.

THE INTEREST YOU'LL PAY ON YOUR DEBT. The better your credit, the lower your APR.

CREDIT APR

MISS A PAYMENT, PAY HIGHER INTEREST. Your interest rate could be more than double for 6+ months.

JAN FEB MAR

...BUT CASH ADVANCES DON'T. You start accruing interest the day you get the advance.

THIS IS A VARIABLE APR. Your interest rate may change based on a national standard.

GETTING CASH FROM A BANK OR ATM COSTS A LOT. You usually pay a higher interest rate for cash advances.

PURCHASES GET A GRACE PERIOD... You have at least 25 days to pay off your debt.

YOU CAN'T GET OUT OF ANNUAL FEE. But most student cards don't have one.

Schumer box highlighting the benefits and risks of applying for a credit card.

Credits: https://www.nerdwallet.com/blog/nerdscholar/read-schumer-box/

7 FRAUD

People assume fraud is inevitable

Nearly everyone we met had experienced some form of fraud or knew someone who had. We heard several cases of phone impersonators asking for bank accounts or ATM pin details. When asked where the impersonators might have gotten their numbers from, people shrugged and felt “they must have gotten it from somewhere.” Surprisingly very few people had complained about impersonation calls. There was a perception that with the rise of the digital economy, there is a greater risk of fraud committed by savvy hackers. Despite the recognition that they may be at risk of malicious third-party action, many consumers felt that ultimately they were responsible for any untoward outcome, particularly if they had given out their phone or bank account details. Where they had not, they felt it was the government’s job to protect them and private provider’s job to compensate them. A lack of trust in how their data is handled may also lead to a lower willingness from people to participate in services being offered.

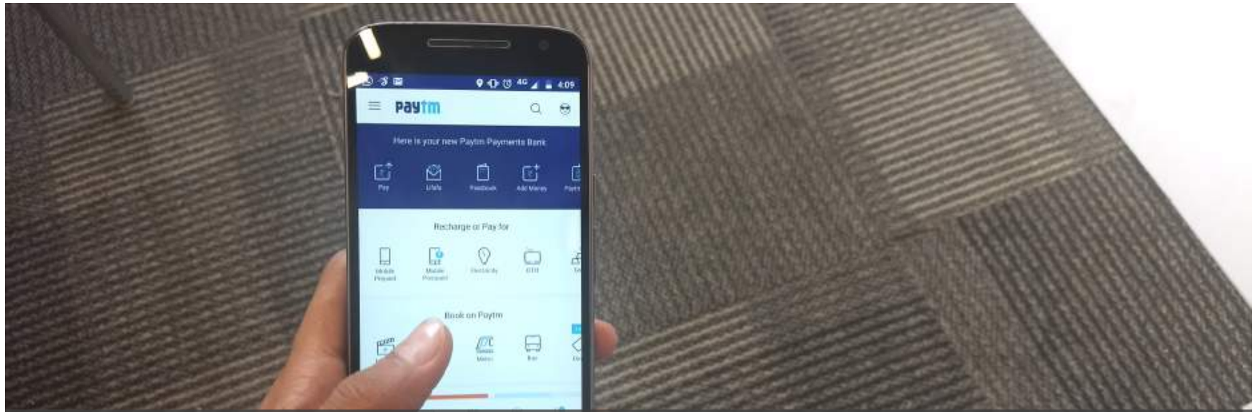
> “Ever since everything has become digital, fraud has increased.”
>
> - Naseer, Mumbai

“Lots of people keep calling to say, ‘put money in this bank account, you have won a lottery!’. My friend lost INR 40,000 this way”

- Saliya, Mumbai

“A lot of fraud is happening these days… I think it’s a big problem. I feel like I shouldn’t keep my money in the bank only.”

- Sapna and Shakuntala, Mumbai



“While using Paytm and online banking I am very careful about who I give my phone number and account number to. Anyone can hack my account.”

- Santosh, Uttarakhand

"Everyone knows someone who has lost money."

- Sumitra, Mumbai

"I got a call on my mobile asking for my account number and ATM pin. They took away money from my account."

- Subhash, Uttarakhand

"If I give my data outside without understanding, it is my mistake. But if someone steals my data, then how can it be my error?"

- Tikam Singh Ji, Uttarakhand

Shift the burden of liability to providers

Currently, consumers are bearing a disproportionate burden of the cost of any kind of fraud/ harm- going forward, providers and regulator should bear some liability. For example, in case of financial loss, consumers currently receive no compensation. While consumers could share some responsibility and even limited liability in exceptional cases, shifting the liability to providers gives them the right incentives to take steps to reduce the risk of fraud.

Legislation like the US Fair Credit Billing Act of 1974, and the RBI's circular limiting the liability of customers in unauthorised electronic banking transactions shifts most of the burden to the provider including financial compensation.

ILLUSTRATIVE EXAMPLES

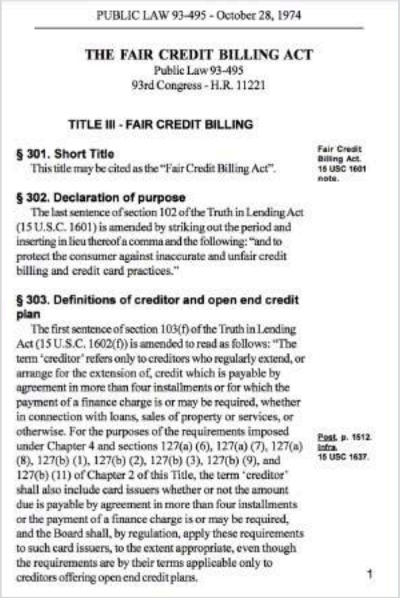
1. Legislation

Make it mandatory for Financial Service Providers (FSPs) to compensate the consumer in the event of a financial fraud and limit the amount a consumer has to bear. Also, incentivise the FSPs to create awareness and take preventive measures against frauds.

2. Third party audits

Government should set-up a body or have independent agencies with incentives to hold the FSPs accountable and fine them for lapses in consumer protection in event of a financial fraud.

FAIR CREDIT BILLING ACT



PUBLIC LAW 93-495 - October 28, 1974

THE FAIR CREDIT BILLING ACT
Public Law 93-495
93rd Congress - H.R. 11221

TITLE III - FAIR CREDIT BILLING

§ 301. Short Title
This title may be cited as the "Fair Credit Billing Act".

Fair Credit Billing Act. 15 USC 1601 note.

§ 302. Declaration of purpose
The last sentence of section 102 of the Truth in Lending Act (15 U.S.C. 1601) is amended by striking out the period and inserting in lieu thereof a comma and the following: "and to protect the consumer against inaccurate and unfair credit billing and credit card practices."

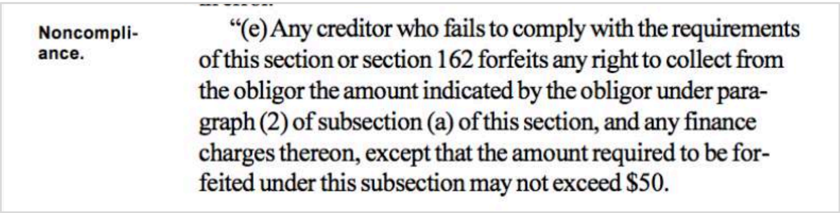
§ 303. Definitions of creditor and open end credit plan
The first sentence of section 103(f) of the Truth in Lending Act (15 U.S.C. 1602(f)) is amended to read as follows: "The term 'creditor' refers only to creditors who regularly extend, or arrange for the extension of, credit which is payable by agreement in more than four installments or for which the payment of a finance charge is or may be required, whether in connection with loans, sales of property or services, or otherwise. For the purposes of the requirements imposed under Chapter 4 and sections 127(a) (6), 127(a) (7), 127(a) (8), 127(b) (1), 127(b) (2), 127(b) (3), 127(b) (9), and 127(b) (11) of Chapter 2 of this Title, the term 'creditor' shall also include card issuers whether or not the amount due is payable by agreement in more than four installments or the payment of a finance charge is or may be required, and the Board shall, by regulation, apply these requirements to such card issuers, to the extent appropriate, even though the requirements are by their terms applicable only to creditors offering open end credit plans.

Post, p. 1512. Infra. 15 USC 1637.

1

This public law was introduced in 1974 in USA.

LIMITED consumer liability



Noncompliance.

"(e) Any creditor who fails to comply with the requirements of this section or section 162 forfeits any right to collect from the obligor the amount indicated by the obligor under paragraph (2) of subsection (a) of this section, and any finance charges thereon, except that the amount required to be forfeited under this subsection may not exceed $50.

In case of financial fraud, the Act limits consumer liability to USD $50 and most of the times it is waived off.

8 REPUTATIONAL HARM

High social costs inhibit women from sharing data

We heard many instances where women regulated and in some cases heavily self-censored their behavior to prevent misuse of their personal data (photos, social media messages, etc.). Many feared high personal consequences (such as marital discord, sexual harassment) and were afraid of social shaming as a result of it. They often relied on or were heavily guided by others (husbands, brothers, more educated people) on what they could do to protect themselves. At times, despite taking precautions they underwent harm and mental stress as a result of their social reputation having been damaged. Women appeared to be more privacy conscious because of the more immediate costs to them in society.

“I’ve decided not to share my picture with anyone, because of what can go wrong.”

- Kokila, Chennai

“Video calls can be misused by people to cause shame publicly. For this reason, I do not share it.”

- Sapna and Shakuntala, Mumbai

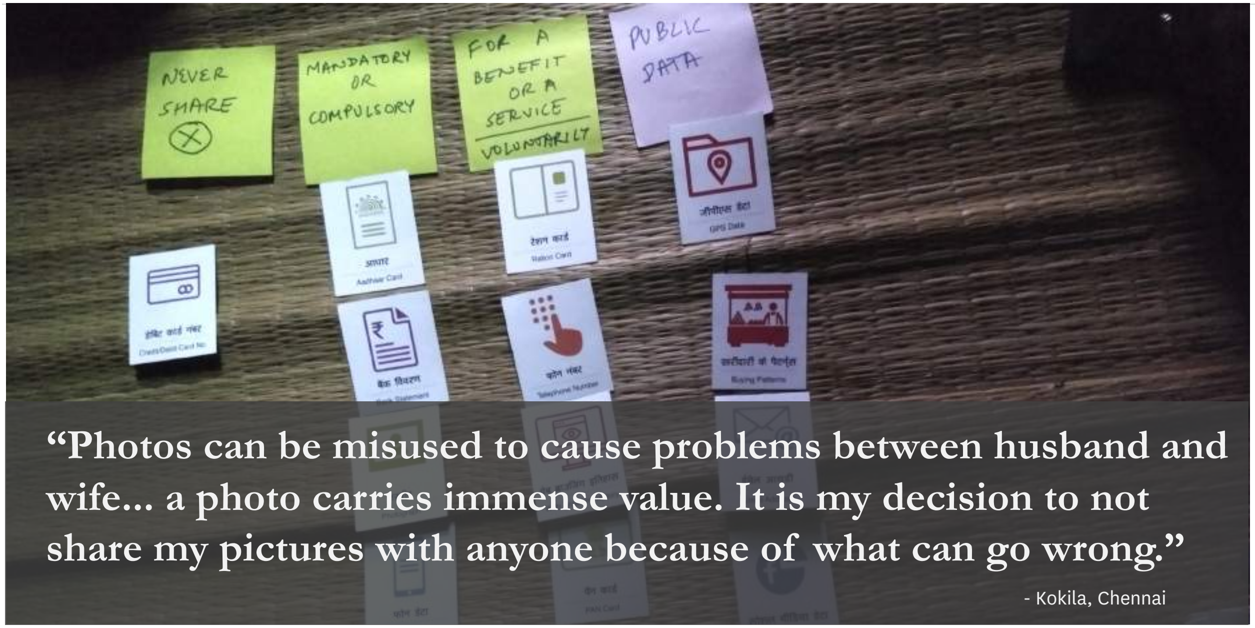
फायनेंशियल फ्रॉड (पैसे संबंधित धोखाधड़ी)
Financial Fraud
उत्पीड़न
Harassment
MISUNDERSTANDING W/ PARTNER

“Harassment over the phone happens very often. It’s the most common problem.”

- Varsha, Mumbai

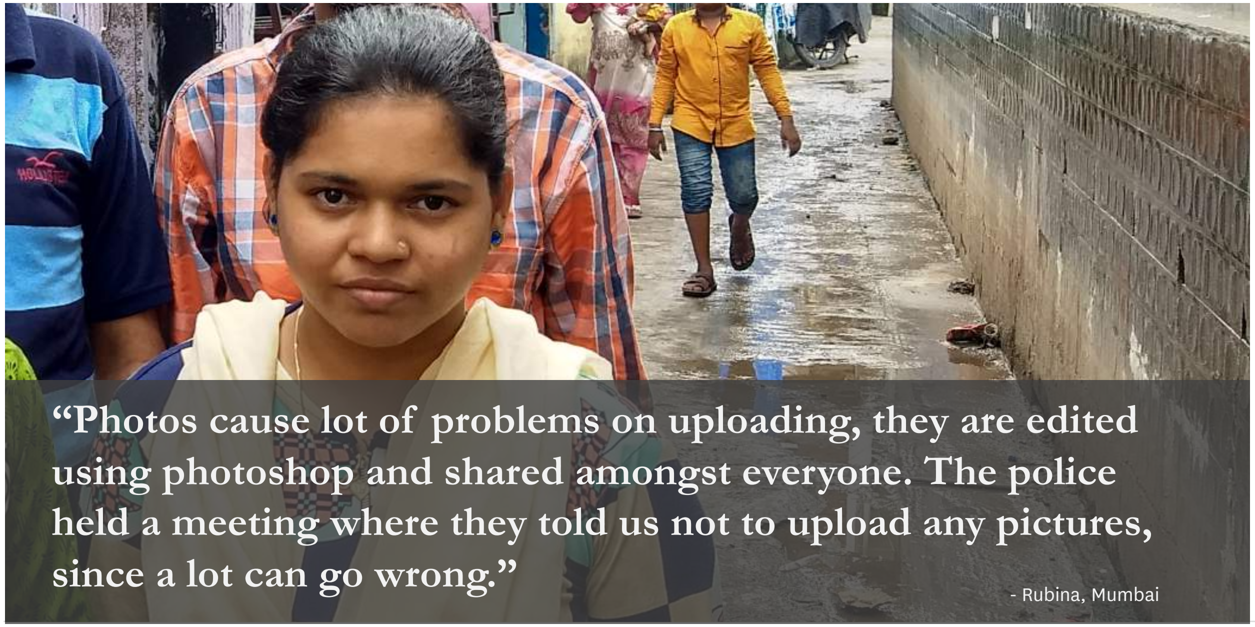
“The SHG women did not understand the terms and ended up defaulting on the loan, [bank employees told the entire village] which gave them a bad social name. They felt mentally stressed.”

- Deepa, Uttarakhand



"Photos can be misused to cause problems between husband and wife... a photo carries immense value. It is my decision to not share my pictures with anyone because of what can go wrong."

- Kokila, Chennai



"Photos cause lot of problems on uploading, they are edited using photoshop and shared amongst everyone. The police held a meeting where they told us not to upload any pictures, since a lot can go wrong."

- Rubina, Mumbai

"Pictures can be very dangerous, I saw on crime patrol that things can go very wrong, people change picture on the computer and share it with everyone"

- Sushma, Delhi

Make safeguards accessible for women

Women need support/ services to help them protect themselves online and offline. There is a need for additional awareness generation amongst women around the ways that they can protect themselves from personal, social or reputational harm. Privacy settings should be more clearly signposted and safeguards pre-designed into products and services by providers to protect women from harms that can be avoided.

Companies have introduced SOS features for their users to reach during emergencies at the press of a button. These measures were in response to reports of crime against women.

ILLUSTRATIVE EXAMPLES

1. SOS button and Hotline

In case of an emergency, an SOS button should be available to women across platforms like Facebook, WhatsApp, Instagram, Hike, etc.

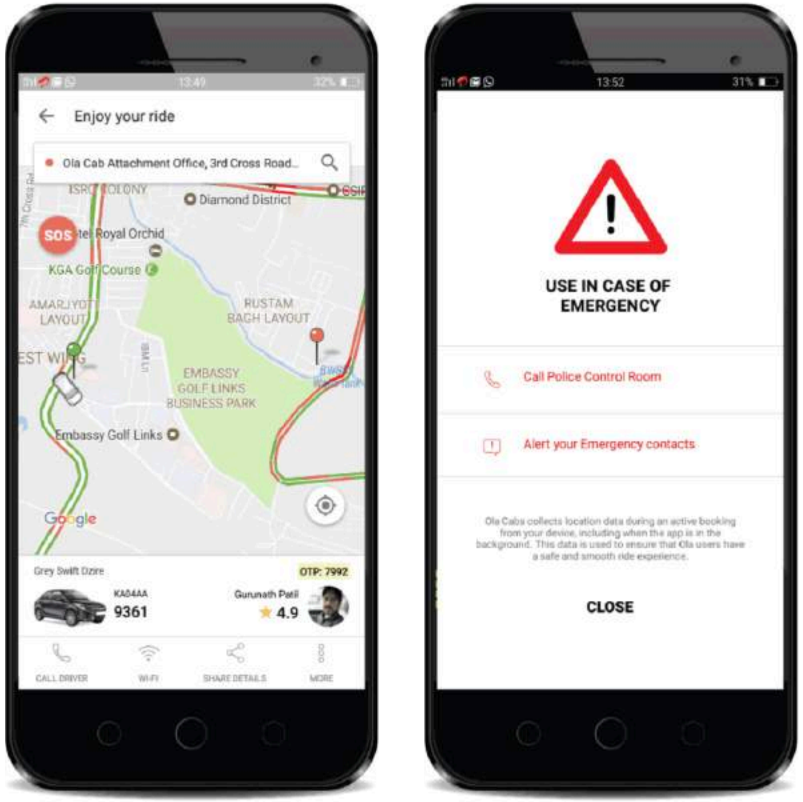
2. Auto configuration

When social media platforms detect female consumers, they automatically display tailored privacy options.

3. Group meetings

Government should conduct localized community level discussions where privacy options and rights of individual to privacy on availing Self Help Group (SHG) or MFI loans are explained and consumer doubts are cleared.

OLA CABS mobile app



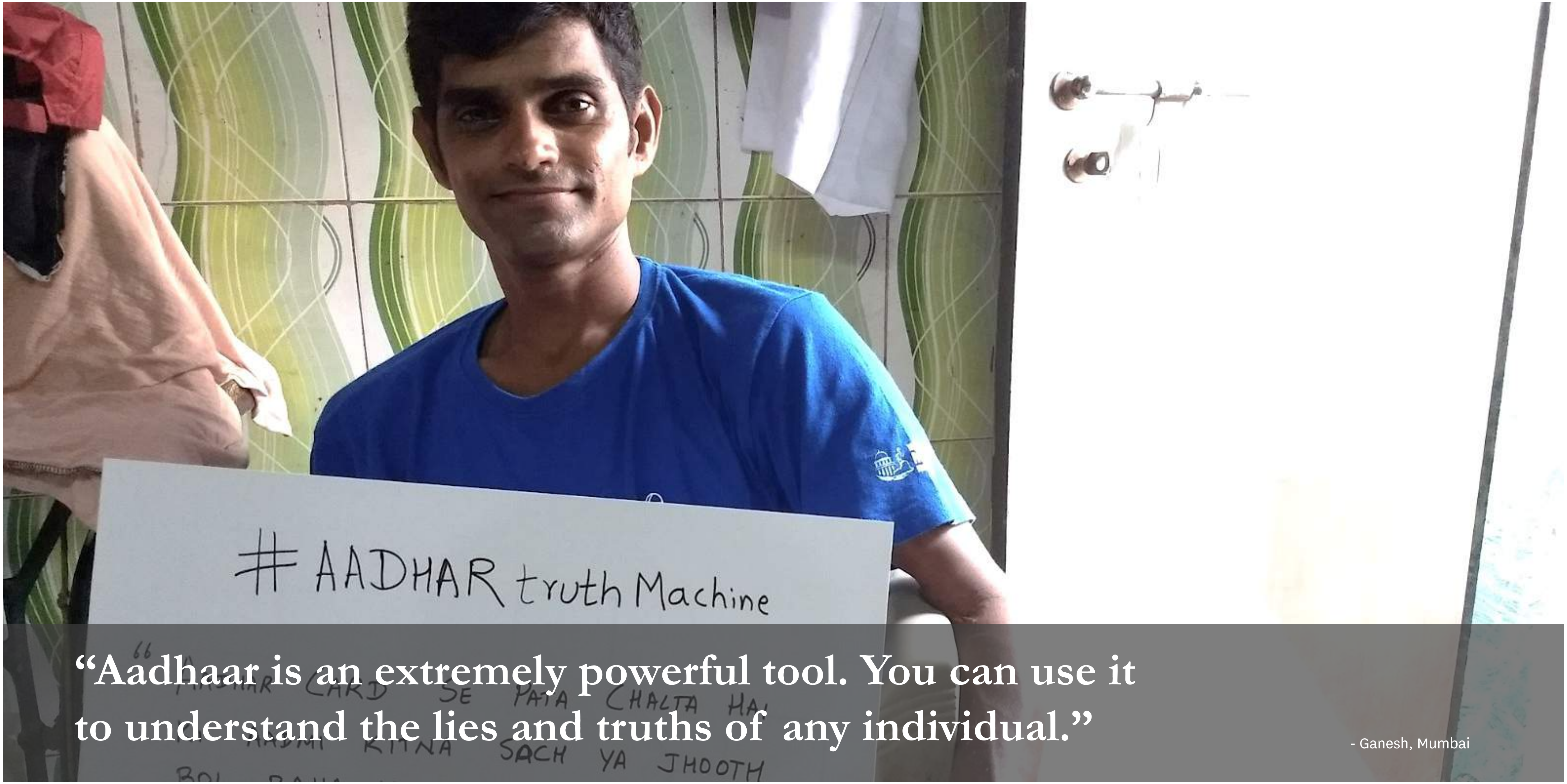
Ola Cabs collects location data during an active booking from your device, including when the app is in the background. This data is used to ensure that Ola users have a safe and smooth ride experience.

The red 'SOS' button on the mobile app allows consumers to alert the police control room or emergency contacts. Consumers can also share their taxi ride and tracking info with their friends and there is a physical red alarm button in every taxi.

9 VALUED DATA

Aadhaar is too precious to be misused

Aadhaar was consistently one of the most valued pieces of data. For the poor, it was a means to access various benefits. Most people felt Aadhaar was a good thing, as it allowed them access to multiple services with ease. They also felt it kept the ‘bad’ people accountable. However, they were equally concerned about the security of their Aadhaar and the dangers of it falling into the wrong hands. For example people said that they had seen SIM card providers issue multiple SIMs under the same Aadhaar identity by making people give their biometric multiple times. Others also felt it was a form of surveillance by the state that went beyond just securing people to watching every action of theirs.



> “Aadhaar is an extremely powerful tool. You can use it to understand the lies and truths of any individual.”

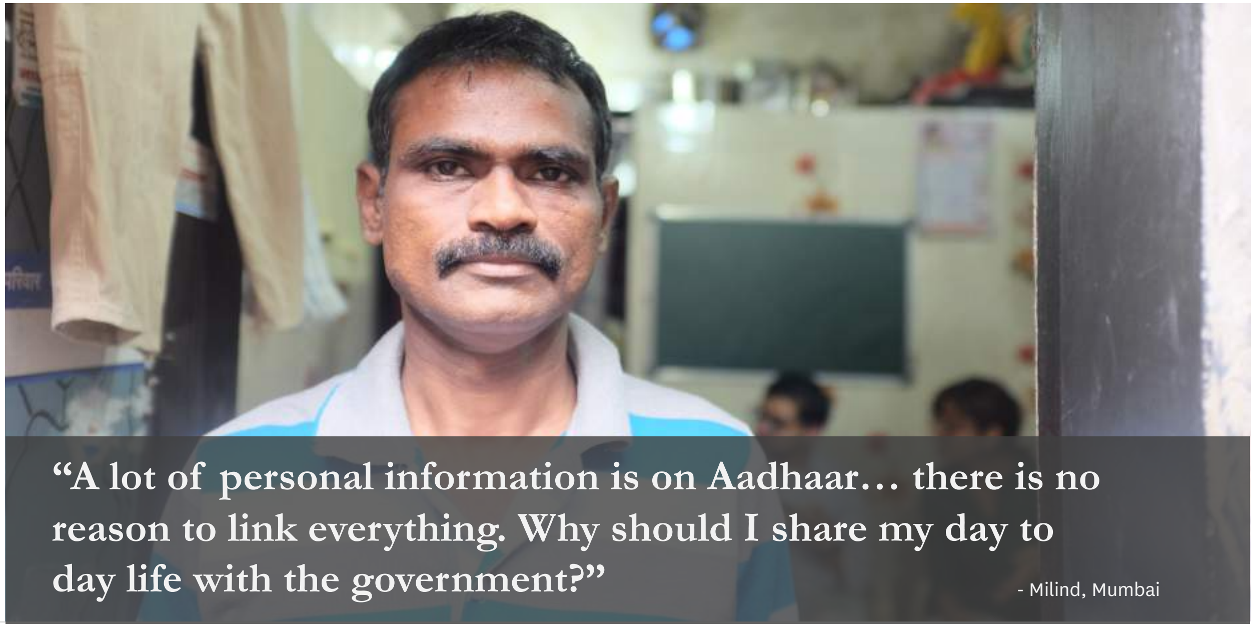
- Ganesh, Mumbai

> “If data sharing allows the government to catch those who break the law and a few people suffer due to it, that’s okay.”

- Sunil, Maharashtra

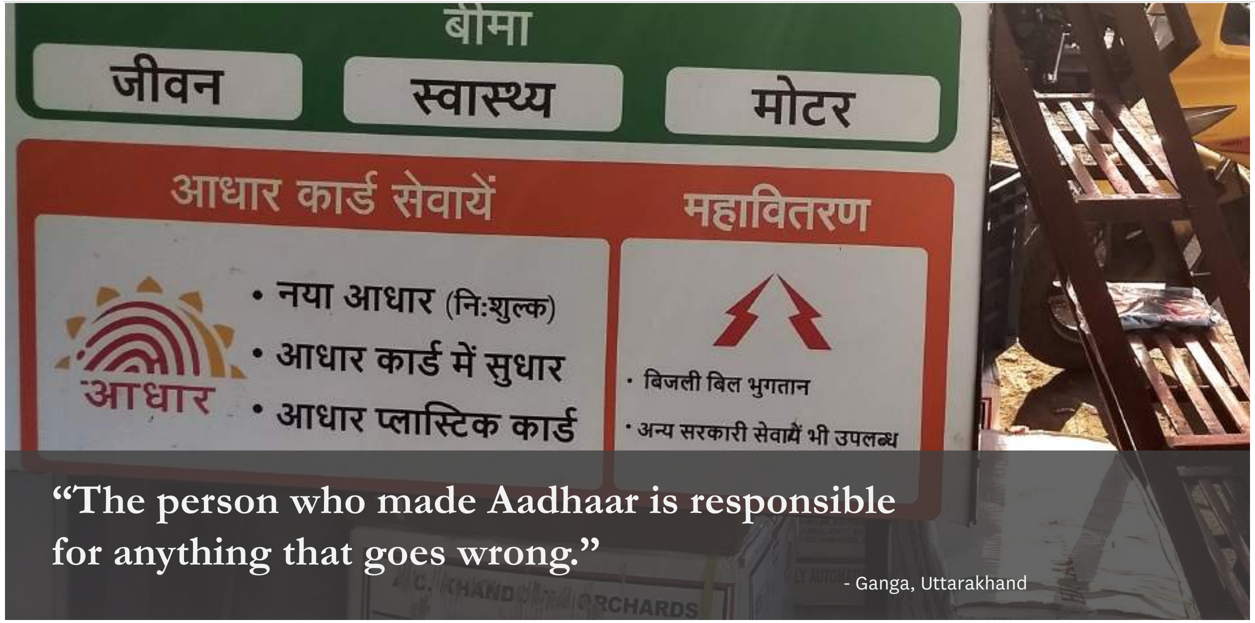
“I am the owner of my own Aadhaar card and no one else.”

- Sunita, Uttarakhand



“A lot of personal information is on Aadhaar… there is no reason to link everything. Why should I share my day to day life with the government?”

- Milind, Mumbai



"The person who made Aadhaar is responsible for anything that goes wrong."

- Ganga, Uttarakhand

"The government is responsible for keeping my Aadhaar safe. I am sure they have a security system in place"

- Santosh, Uttarakhand

"Terrorists can use Aadhaar to get SIM cards, it is important to keep the number safe."

- Prashant, Mumbai

Ensure highest security for the most valued data

It is vital for the state to ensure maximum security for what is increasingly the most valued and demanded piece of data. They should prevent its misuse and ensure the right redressal mechanisms in case of one.

Conducting hackathons or challenging people to break into databases or software can reinforce security in case flaws are found, and communicate security in case there are no breaches.

ILLUSTRATIVE EXAMPLES

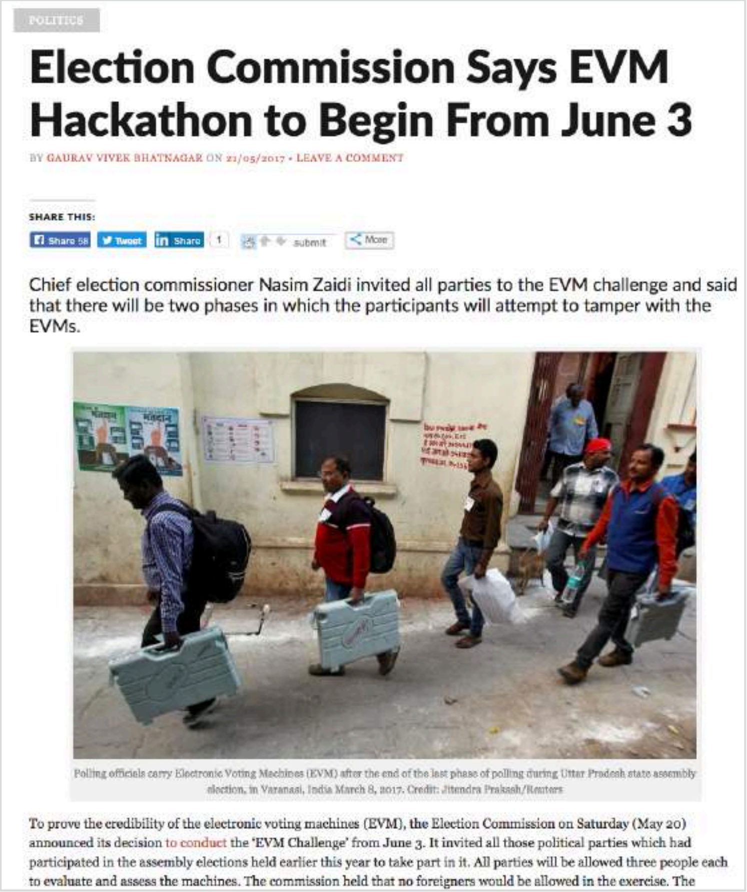
1. Hacking competition

Conduct a ‘Hack Aadhaar if you can’ competition with a big prize for any successful hacks. Also spread awareness about security measures employed by Aadhaar.

2. Regulatory oversight

The government should have strict regulations for MNOs to curb the issue of multiple sim cards being issued on a single person’s biometric without their knowledge. They should also crack down heavily on miscreants duplicating Aadhaar cards.

EVM HACKATHON news article



POLITICS

Election Commission Says EVM Hackathon to Begin From June 3

BY GAURAV VIVEK BHATNAGAR ON 21/05/2017 • LEAVE A COMMENT

SHARE THIS:

Chief election commissioner Nasim Zaidi invited all parties to the EVM challenge and said that there will be two phases in which the participants will attempt to tamper with the EVMs.

Polling officials carry Electronic Voting Machines (EVM) after the end of the last phase of polling during Uttar Pradesh state assembly election, in Varanasi, India March 8, 2017. Credit: Jitendra Prakash/Reuters

To prove the credibility of the electronic voting machines (EVM), the Election Commission on Saturday (May 20) announced its decision to conduct the ‘EVM Challenge’ from June 3. It invited all those political parties which had participated in the assembly elections held earlier this year to take part in it. All parties will be allowed three people each to evaluate and assess the machines. The commission held that no foreigners would be allowed in the exercise. The

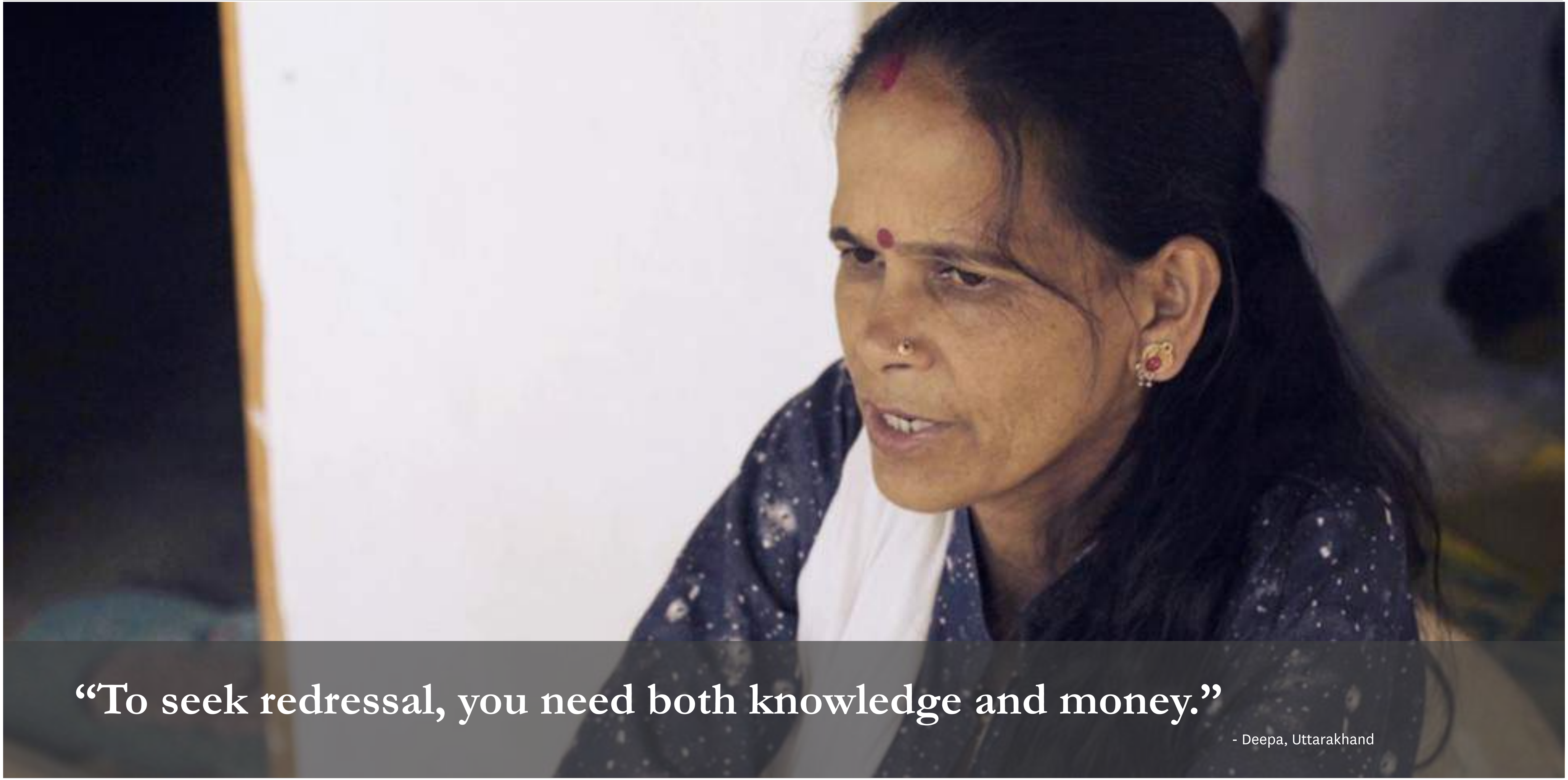
Article describing the Electronic Voting Machine (EVM) hackathon challenge

Credits: https://thewire.in/138190/evm-election-commission-hackathon/

10 REDRESSAL

There is low faith in redressal, but high demand

Traditional forms of redressal left people cynical and wary of its effectiveness. They had far too many experiences of being left hanging at the other end of the customer service line or filing complaints that never saw the light of day. At the same time they strongly felt that effective redressal options need to be immediate and tangible. They also wanted awareness of such mechanisms, and for them to be affordable for them to make use of it.



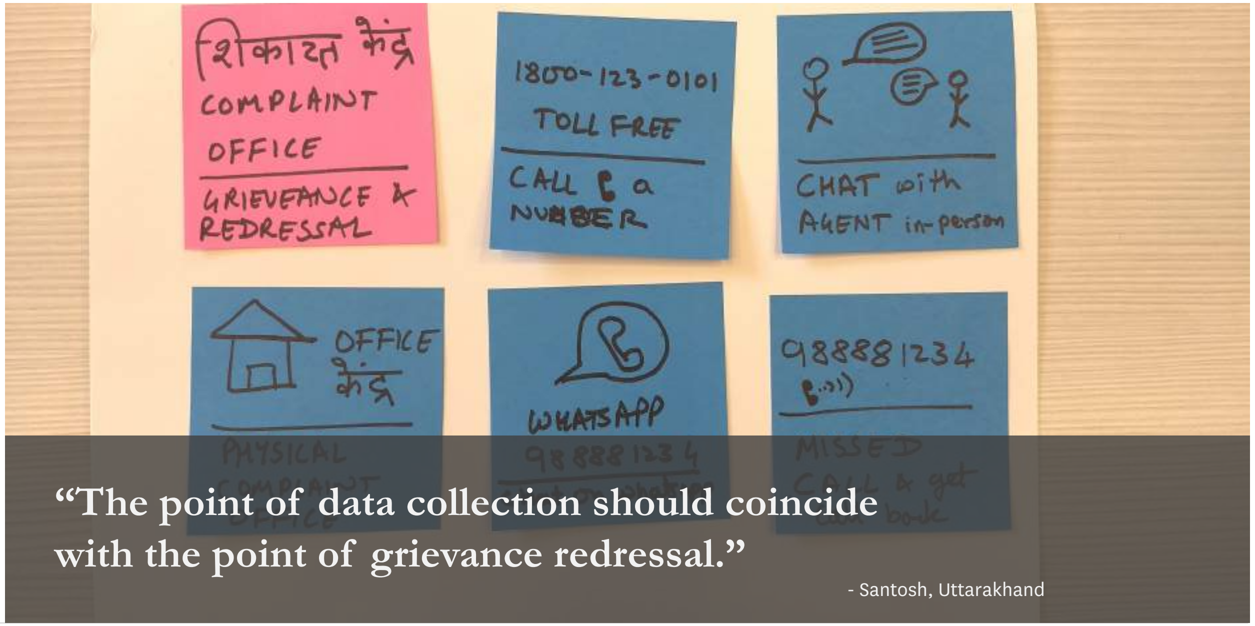
> “To seek redressal, you need both knowledge and money.”
>
> - Deepa, Uttarakhand

“I want to talk to someone who is knowledgeable, preferably from the Government or the police.”

- Mohamed, Mumbai

“It will be good if consent were explained verbally. Video consent with animation explaining consent conditions clearly will be good.”

- Anitha, Tamil Nadu



“The point of data collection should coincide with the point of grievance redressal.”

- Santosh, Uttarakhand

"Calling a toll free number to complain about data privacy violations will not work because it will always be busy."

- Saliya, Mumbai

"I want an agent to talk to when I am lodging complaints as I believe they can guide me better."

- Azad, Mumbai

"It should not be on the phone - I want to see the person's face when I'm making the complaint. I want to see if they understand what I'm saying."

- Nasser, Mumbai

Humanize redressal

People wanted redressal for data breaches to be immediate and at the point of sale or service. In case the service provider was unable to provide redressal they would approach other institutional agencies (police, gram pradhan, etc.) for redressal. They strongly felt that effective redressal is only possible if there is a person they can interact with face-to-face who is trustworthy and responsive.

Quasi-judicial formats such as those used by banks and customer service models used by mobile app services can be replicated specifically for incidents related to data breaches.

ILLUSTRATIVE EXAMPLES

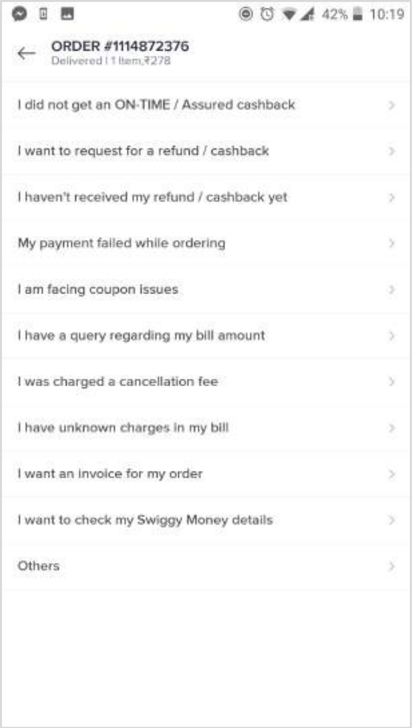
1. Better Ombudsman model

Have an ombudsman office for redressal of data protection and privacy issues. Learn from what did not work in the bank ombudsman model and avoid those pitfalls.

2. Follow new age digital services

For Urban Ladder, Swiggy, Amazon, Flipkart, etc. digital services, multichannel redressal methods have worked well. Avoid MNOs customer care or IVRS routes.

TYPICAL REDRESSAL screens for a mobile app

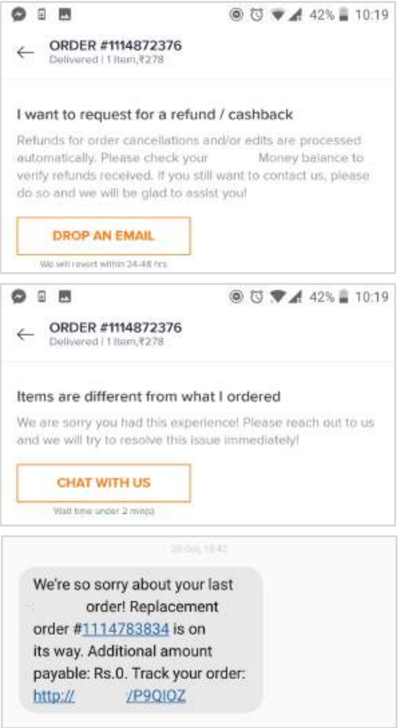


42% 10:19

ORDER #1114872376
Delivered | 1 Item,₹278

- I did not get an ON-TIME / Assured cashback
- I want to request for a refund / cashback
- I haven't received my refund / cashback yet
- My payment failed while ordering
- I am facing coupon issues
- I have a query regarding my bill amount
- I was charged a cancellation fee
- I have unknown charges in my bill
- I want an invoice for my order
- I want to check my Swiggy Money details
- Others

FAQ style menu for issues on resolving a digital transaction



42% 10:19

ORDER #1114872376
Delivered | 1 Item,₹278

I want to request for a refund / cashback

Refunds for order cancellations and/or edits are processed automatically. Please check your Money balance to verify refunds received. If you still want to contact us, please do so and we will be glad to assist you!

DROP AN EMAIL

We will revert within 24-48 hrs

42% 10:19

ORDER #1114872376
Delivered | 1 Item,₹278

Items are different from what I ordered

We are sorry you had this experience! Please reach out to us and we will try to resolve this issue immediately!

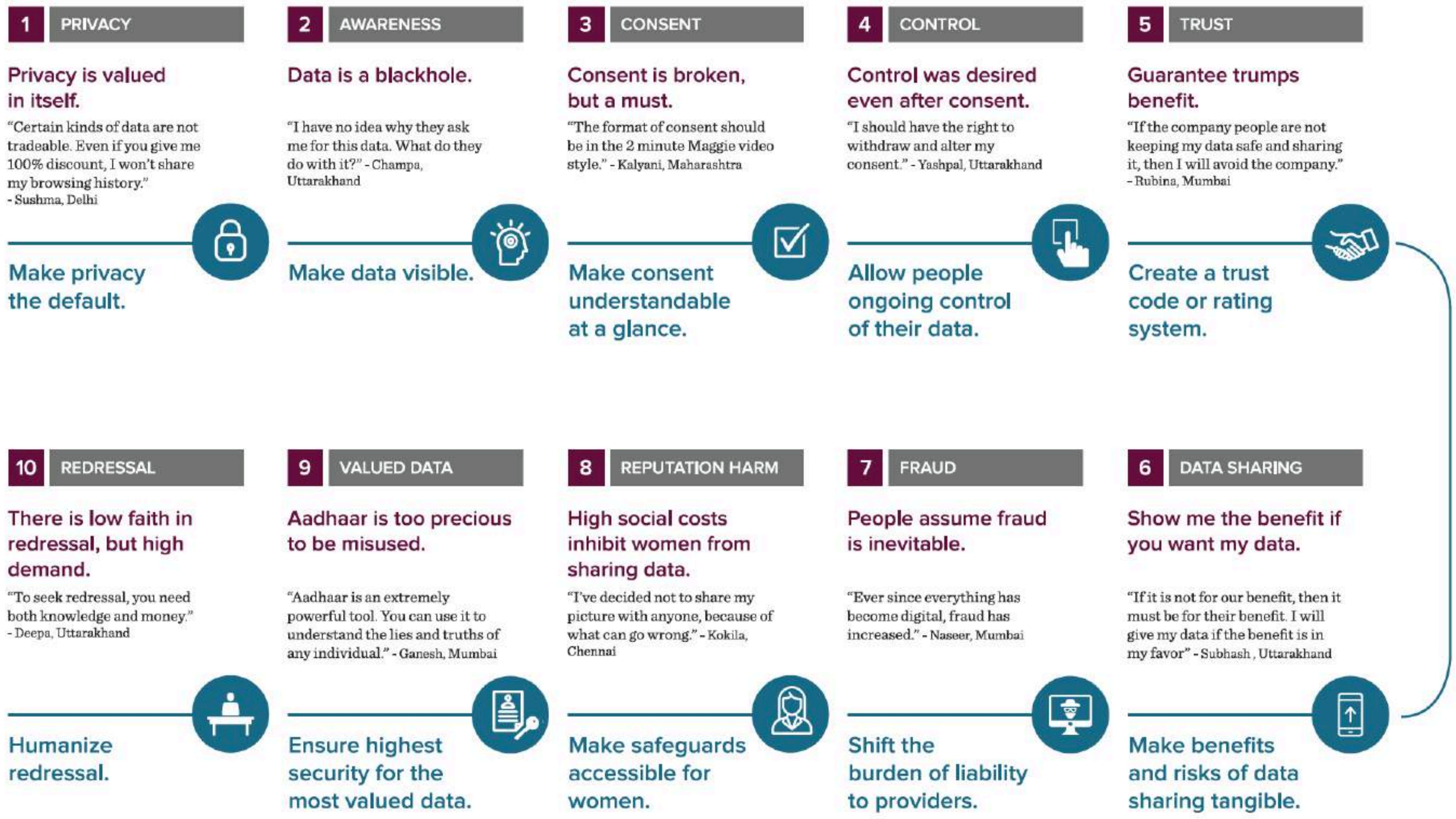
CHAT WITH US

Wait time under 2 min(s)

We're so sorry about your last order! Replacement order #1114783834 is on its way. Additional amount payable: Rs.0. Track your order: http:// /P9QIOZ

Options to call an agent or email to resolve the issue with a time guarantee of resolution. Also, an SMS is sent as reaffirmation.

■ INSIGHTS ■ DESIGN PRINCIPLES



1 PRIVACY

Privacy is valued in itself.

"Certain kinds of data are not tradeable. Even if you give me 100% discount, I won't share my browsing history." - Sushma, Delhi

Make privacy the default.

2 AWARENESS

Data is a blackhole.

"I have no idea why they ask me for this data. What do they do with it?" - Champa, Uttarakhand

Make data visible.

3 CONSENT

Consent is broken, but a must.

"The format of consent should be in the 2 minute Maggie video style." - Kalyani, Maharashtra

Make consent understandable at a glance.

4 CONTROL

Control was desired even after consent.

"I should have the right to withdraw and alter my consent." - Yashpal, Uttarakhand

Allow people ongoing control of their data.

5 TRUST

Guarantee trumps benefit.

"If the company people are not keeping my data safe and sharing it, then I will avoid the company." - Rubina, Mumbai

Create a trust code or rating system.

6 DATA SHARING

Show me the benefit if you want my data.

"If it is not for our benefit, then it must be for their benefit. I will give my data if the benefit is in my favor" - Subhash , Uttarakhand

Make benefits and risks of data sharing tangible.

7 FRAUD

People assume fraud is inevitable.

"Ever since everything has become digital, fraud has increased." - Naseer, Mumbai

Shift the burden of liability to providers.

8 REPUTATION HARM

High social costs inhibit women from sharing data.

"I've decided not to share my picture with anyone, because of what can go wrong." - Kokila, Chennai

Make safeguards accessible for women.

9 VALUED DATA

Aadhaar is too precious to be misused.

"Aadhaar is an extremely powerful tool. You can use it to understand the lies and truths of any individual." - Ganesh, Mumbai

Ensure highest security for the most valued data.

10 REDRESSAL

There is low faith in redressal, but high demand.

"To seek redressal, you need both knowledge and money." - Deepa, Uttarakhand

Humanize redressal.

THANK YOU

PRIVACY ON THE LINE

Dalberg

CGAP

FUTURE OF FINANCE
A DVARA RESEARCH INITIATIVE