CONSUMER AWARENESS WORKSHOP

on

Data Protection and Privacy & Impact of Personal Data Protection Bill (PDPB)

1 November, 2019

Kolkata
OBJECTIVE

- Engage with the consumer and civil society organisations (CSOs) in tier II locations to raise awareness and build their capacity that helps them engage with the common citizens productively on the issue of data protection and privacy.

- Understand the perspective of CSOs and help them put forth their perspective.
LEARNING OUTCOMES

● Hear about why data privacy and data protection is an important issue in India today
● Learn about the basic terminologies, and principles within the data protection and privacy ecosystem
● Understand the rights, duties and responsibilities of key stakeholders in protecting the privacy of an individual
● Understand the possible impact of Personal Data Protection Bill, 2018 on consumers
People who use technology to buy and sell products and services are known as digital consumers.

The **internet has made us digital consumers.** For the first time in history, a majority of the global population will be connected in 2019.

China and India will add more internet users over the next three years than what exists in the US today - the third largest internet base.
In the next three years, **half of India's population**—about 650M people—will become internet users.

Double-digit growth for 2019 is estimated— the number of Internet users will reach 627 million by the end of this year.

87% of the total user base, or **493 million Indians**, are defined as **regular users**, having accessed the internet in the last 30 days. Of this, 293 million active internet users reside in urban India, while there are **200 million active users in rural India**.
97% of users access the internet on their mobile device

The number of smartphone users in India is expected to rise by 84% to 859 million by 2022 from 468 million in 2017.

Indians have 1.2 billion mobile phone subscriptions and downloaded more apps -- 12.3 billion in 2018 -- than residents of any other country except China.

One of the network operators brought in more than 100 million subscriptions of 4G network in first six months of its launch.

Monthly mobile data consumption per user is growing at 152 per cent annually -more than twice the rates in the United States and China.
India will go from data poor to data rich nation in 5 Years ...

... allowing data driven decision making for scale and inclusion!
NEWS STORIES
India Ranked Third Worst For Data Privacy In Global Surveillance Index

The country ranks behind only Russia and China when it comes to surveilling citizens.

Why India scored low? Aadhaar, content monitoring (whatsapp), No data protection law still in place, recent circular (Sec 69 of the IT Act, 2000) allows 10 government agencies to decrypt and intercept data.
Aadhaar Database Suffered Multiple Breaches, Comprised Records of 1.1 Billion Citizens
PERSONAL DETAILS FOR ₹500?

- Grievance redress facility used for breach
- A news report said an ‘agent’ available on WhatsApp facilitated access by a login ID and password to particulars of any Aadhaar number
- The agent was paid ₹500 through a digital wallet
- Particulars such as name, address, pin code, photo, phone and email were accessed and an Aadhaar card printed, the report said

"UIDAI assures that there has not been any Aadhaar data breach. The Aadhaar data, including biometric information, is fully safe."

—UIDAI STATEMENT
Unsold Potatoes Dumped in front of Government Officials’ Houses by Farmers in UP
Data Surveillance: Police Tapped Over 10,000 Phones to Catch Two Men
### People whose Facebook information may have been improperly shared with Cambridge Analytica

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of Accounts</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>70,632,350</td>
<td>81.6%</td>
</tr>
<tr>
<td>Philippines</td>
<td>1,175,870</td>
<td>1.4%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>1,096,666</td>
<td>1.3%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>1,079,031</td>
<td>1.2%</td>
</tr>
<tr>
<td>Mexico</td>
<td>789,880</td>
<td>0.9%</td>
</tr>
<tr>
<td>Canada</td>
<td>622,161</td>
<td>0.7%</td>
</tr>
<tr>
<td>India</td>
<td>562,455</td>
<td>0.6%</td>
</tr>
<tr>
<td>Brazil</td>
<td>443,117</td>
<td>0.5%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>427,446</td>
<td>0.5%</td>
</tr>
<tr>
<td>Australia</td>
<td>311,127</td>
<td>0.4%</td>
</tr>
</tbody>
</table>

We do not know precisely what data the app shared with Cambridge Analytica or exactly how many people were impacted. Using as expansive a methodology as possible, this is our best estimate of the maximum number of unique accounts that directly installed the thisisyourdigitallife app as well as those whose data may have been shared with the app by their friends.
Allegations on Facebook: Personal Information Sold, Invasion of Privacy

### Facebook Users' Privacy Concerns

<table>
<thead>
<tr>
<th>Concern</th>
<th>Very Concerned</th>
<th>Somewhat Concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your personal information being sold to and used by other companies and organizations</td>
<td>55%</td>
<td>25%</td>
</tr>
<tr>
<td>Invasion of privacy</td>
<td>43%</td>
<td>31%</td>
</tr>
<tr>
<td>Internet viruses</td>
<td>36%</td>
<td>30%</td>
</tr>
<tr>
<td>Unsolicited messages or ads, sent through spam email or appearing on your Facebook page, usually sent to try to sell you something</td>
<td>33%</td>
<td>32%</td>
</tr>
<tr>
<td>Being attacked or shamed by others for things you say or do on Facebook</td>
<td>15%</td>
<td>13%</td>
</tr>
<tr>
<td>Spending too much time on Facebook</td>
<td>13%</td>
<td>17%</td>
</tr>
<tr>
<td>Getting upset or feeling bad about yourself because of things you see others post</td>
<td>9%</td>
<td>11%</td>
</tr>
</tbody>
</table>

Published on MarketingCharts.com in April 2018 | Data Source: Gallup

Based on telephone interviews conducted April 2-8, 2018 among 1,509 US adults ages 18 and older, of whom 785 are Facebook users. The remaining respondents answered “Not too concerned” or “Not concerned at all.”
Facebook Fined for Mishandling Users’ Personal Information

A record $5 billion fine is to be imposed on Facebook for privacy breach the FTC had started the investigations into Facebook after the Cambridge Analytica controversy and is expected to hit Facebook with a record-setting $5 billion fine.
Facebook agrees to pay UK fine over Cambridge Analytica scandal - had obtained personal data of 87 million Facebook users

Highest Penalties in Privacy Enforcement Actions

- States v. Uber: $148 M
- British Authority v. British Airways (proposed): $230 M
- CFPB and States v. Equifax: $275 M
- FTC v. Facebook: $5,000,000,000,000

Source: Federal Trade Commission | FTC.gov
Lack of transparency  
Data Privacy, data protection, and security  
Risk of data theft (financial loss, fraud)  
Complex liability  
Lack of complaint filing system and adequate grievance redressal mechanism  
Opaqueness with regard to quality of products and services  
Network downtime  
No dedicated laws  
Language barrier
Designing adequate laws

Awareness and education
RECENT PRIVACY MILESTONES IN INDIA

- SC’s Puttaswamy Judgement recognising right to privacy as a fundamental right
- Government appointed Srikrishna Committee released a white paper on ‘Data Protection Framework’ (for consultation on the topic by Srikrishna Committee, as formed by MeitY)
- Sector specific developments (in this realm):
  - DISHA by Ministry of Health & Family Welfare for health data
  - RBI circular on payments data storage
  - TRAI’s paper on Data Privacy for TSPs
  - Draft e-commerce policy framework
- Release of Srikrishna Committee recommendations and draft Personal Data Protection Bill, 2018
- Draft Intermediary Guidelines 2018 by MeitY
“The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.” – SC in KS Puttaswamy v. UOI. Decisions of the MP Sharma (1954) and Kharak Singh (1962) cases overruled to the extent they held that the Indian Constitution did not protect the right to privacy.

The RBI circular mandated all system providers to store the data relating to payment systems in India.

EU GDPR become effective.

PERSONAL DATA PROTECTION BILL, 2018

- Defines Personal Data
- Guidelines for use of Personal Data
- Framework for Regulating use of Personal Data
PERSONAL DATA PROTECTION BILL, 2018

- Data Fiduciary
  - Any person (including the State, a company, any juristic entity or any individual) who determines the purpose and means of processing of personal data.

- Data Processor
  - Any person (including the State, a company, any juristic entity or any individual) who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary.

- Data Principal
  - A natural person to whom the personal data relates.

- Personal Data
  - Data about a natural person in relation to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

- Sensitive Personal Data
  - Personal data revealing, related to, or constituting passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious political belief or affiliation, or any other category as may be specified by the Data Protection Authority of India (Authority).
RIGHTS OF DATA PRINCIPAL

ACCESS

RECTIFICATION

NAME: Phil
AGE: 33 29

Right to Data Portability
PERSONAL DATA PROTECTION BILL, 2018

Data Fiduciary Obligations

- Fair and Reasonable Processing
- Notice
- Collection Limitation
- Accountability
- Purpose Limitation
- Lawful Processing
- Data Quality
PERSONAL DATA PROTECTION BILL, 2018-A PEEK

- Restricts and imposes conditions on cross-border transfer of personal data
- Suggests setting up of Data Protection Authority of India to prevent any misuse of personal information
- Allows processing of personal data only for the purpose it is collected or for compliance of any law, employment and for any function of Parliament or any state legislature
- ‘Sensitive personal data’ comprises passwords, financial data, health data, sex life, sexual orientation, biometric data, genetic data, caste or tribe and religious or political belief or affiliation

It is a monumental law and we would like to have widest parliamentary consultation... We want Indian data protection law to become a model globally, blending security, privacy, safety and innovation

RAVI SHANKAR PRASAD | IT MINISTER
What do Internet users think, and know about Digital Technologies?

The benefits, expectation, confidence; risks, privacy, data protection, trust, safety and security; awareness, usage and experience as perceived by 2160 users were recorded through a survey conducted by CUTS International.
CUTS surveyed 2400 people across India of which 2160 were internet users.
High awareness of right to privacy with more need for capacity building expressed in digital space

Is ‘Right to data privacy’ a fundamental right?
- Yes: 90%
- No: 5.1%
- Not Sure: 4.9%

Is there a need for the government/ regulators to undertake awareness and capacity building programmes for users with respect to their data?
- Yes: 70%
- No: 8.2%
- Not Sure: 21.8%
High need for re-imagining & re-designing privacy policy as a consent mechanism

Reading Privacy Policies

Understanding

Why not reading

A chunk of users don’t realise importance of consent hence requiring capacity building

Is consent when not completely informed due to lack of readability is consent broken

<table>
<thead>
<tr>
<th>Lengthy</th>
<th>Language barrier</th>
<th>Too much legalese</th>
<th>Not necessary</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.4</td>
<td>33.4</td>
<td>23</td>
<td>15.5</td>
<td>6.3</td>
</tr>
</tbody>
</table>
User's are protective of their personal and sensitive information

While close to 90% users share and are comfortable sharing their general profile and contact details with online businesses they don’t seem to be as comfortable sharing their email IDs.

Many users do not think they share sensitive information and are not comfortable sharing it.

Users are least comfortable in sharing financial details and medical history.

Across all meta data types less than 40% think they are sharing meta data and even lesser are comfortable sharing it.

Users are not comfortable sharing their tastes & preferences with online businesses.

Despite not being comfortable in sharing personal photos and videos more than 60% are sharing them.
Awareness of third party sharing and legitimate use is low among users.

Most users think service providers use the data collected to provide better services and undertake targeted advertising. While most online businesses resort to third party sharing only 46% users are aware of this.

An element of mistrust is reflected when less than 37% users say that data collection is for disclosed legitimate purposes.

Users expect online businesses to follow the principle of Purpose Limitation while handling their data.

What do you think is the purpose for which such data is collected by the service providers?
Users are aware of risks associated with sharing data with online businesses. Users expect online businesses to follow the principle of Purpose Limitation while handling their data.

Unauthorized data collection is the highest risk perceived while unwanted advertisements is the lowest risk. Users’ capacity building is necessary to build awareness of risks.

Users are unaware of third party sharing and hence don’t consider it a major risk.

What according to you are the associated risks in sharing your data with service providers?
### Vulnerable groups less likely to realise risks of data sharing with service providers

Perception of different risks is different across different groups, businesses can tailor privacy policies as per your target group.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Male (%)</th>
<th>Female (%)</th>
<th>Urban (%)</th>
<th>Non-Urban (%)</th>
<th>Experienced (%)</th>
<th>Inexperienced (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised collection</td>
<td>64</td>
<td>56</td>
<td>52</td>
<td>54</td>
<td>54</td>
<td>50</td>
</tr>
<tr>
<td>Misuse of personal photos/videos</td>
<td>68</td>
<td>57</td>
<td>56</td>
<td>55</td>
<td>51</td>
<td>54</td>
</tr>
<tr>
<td>Hacking</td>
<td>51</td>
<td>54</td>
<td>54</td>
<td>51</td>
<td>55</td>
<td>52</td>
</tr>
<tr>
<td>Financial fraud</td>
<td>53</td>
<td>49</td>
<td>55</td>
<td>45</td>
<td>52</td>
<td>50</td>
</tr>
<tr>
<td>Data not protected</td>
<td>49</td>
<td>48</td>
<td>49</td>
<td>48</td>
<td>48</td>
<td>49</td>
</tr>
<tr>
<td>Undisclosed use</td>
<td>42</td>
<td>39</td>
<td>42</td>
<td>39</td>
<td>35</td>
<td>39</td>
</tr>
<tr>
<td>Misuse of data</td>
<td>43</td>
<td>39</td>
<td>43</td>
<td>39</td>
<td>37</td>
<td>35</td>
</tr>
<tr>
<td>Unauthorised data sharing</td>
<td>43</td>
<td>39</td>
<td>43</td>
<td>39</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>Unwanted advertisements</td>
<td>43</td>
<td>39</td>
<td>43</td>
<td>39</td>
<td>36</td>
<td>36</td>
</tr>
</tbody>
</table>

What according to you are the associated risks in sharing your data with service providers?

- More female respondents considered unwanted ads as a risk as compared to males.
- More non-urban respondents perceive hacking as a risk.
Users expect service providers to deliver on user rights

- Easy to use data control tools: 28%
- Service provider has strong data protection tools: 13%
- Purpose limitation, Privacy & Anonymisation highest expectations from service providers: 18%
- Flexibility in data sharing: 10.6%
- Provide data control tools: 11.4%
- Ensure data privacy: 4%
- Ensure data anonymisation: 9%
- Privacy by design: 6%

Expectation of Data Control Tools and associated provisions are low and want service providers to ensure data protection - Privacy by design.

What provides you comfort in sharing your data with service providers in order to avail their services?
Low usage of data protection tools by users due to capacity constraint

Capacity constraint is the biggest reason for users who are aware of data protection tools but still don’t use them. Many users do not find use of data protection tools necessary.

% respondents


- Don’t know how to use them
- Do not find it necessary
- Difficult and complicated to use
- Use is not effective

12
Reputation and related indicators highest enforcers of trust in data sharing

- Reputation: 64.6%
- Mobile app ratings & downloads: 50.6%
- Easy Privacy Policy: 45.7%
- Flexibility in providing data: 44.1%
- Anonymisation of data: 43.4%
- Appropriate consent & notice mechanism: 43.2%
- Knowledge of their data protection measures: 40.2%
- Tools offered for data protection: 37.1%

Reputation is the most important factor for users while sharing. Trust code/code of conduct ratings should be designed to inform users.

Mobile app ratings do not provide much confidence to inexperienced users.

While data anonymisation is expected by users in general, it does not appear to provide much confidence to many female users.

Data protection tools do not provide much confidence to users.

What gives you confidence to share your data with service providers?
Almost no experience of data privacy violation - onus should be on businesses to inform and provide redress mechanism.

- Perceived Experience of Data Privacy Violation: 98% No, 2% Yes
- Reporting Data Privacy Violation: 47% Yes, 53% No

- Don’t know how, and whom to report
- Did not find it necessary/important enough to report it
- Made a new account instead of reporting it
- Did not want to waste time on it
More **females, young, and rural users** are coming within the fold of digital technology than ever before.

Despite being uncomfortable, users reported to share their information. Around 16-18% reported **discomfort in sharing** their contact and address details, and around 14% for email and personal photos.

Around 60% users **fear unauthorised data collection**, but rely on the **Reputation** of the service provider to boost their **confidence** while sharing data.
Top 3 expectation of 59% users from service providers are purpose limitation, ensure privacy and anonymisation.

Only 11% users read privacy policies, and only a small percentage of that claim to understand them. Top 3 impediments were 3L’s- Length, language and legalese.

Despite being aware, most non-urban and inexperienced users don’t use Data Protection Tools due to capacity constraints, and find it unnecessary.

Almost 70% users feel the need to build capacity and awareness among users.
Inform users - Service providers need to better inform users of purposes of data collection, privacy, data protection and anonymisation practices to retain their trust and confidence in them.

Alleviate risks - Service providers need to make more efforts to prevent unauthorised data collection, data misuse, hacking and financial fraud.

Redesign protection - privacy policies and data protection tools need to be user friendly, and

Regulatory measures for ensuring accountability of service providers & strengthening Grievance redressal mechanism

Building capacity of users for using data protection tools, reading privacy policies, reporting violation.
Way Forward

- Analyse the impact of legal provisions on rights of consumers- by weighing the quantitative as well as qualitative pros and cons of the debate. Conducting a Cost-Benefit Analysis (CBA) would help map the benefits and challenges.
- Due process and transparency in policy making; meaningful, stakeholder consultations
- Measures to foster interoperability and harmonisation. It will help bridge the growing divide on the internet.
- Avoid unilateral actions that may stifle trade and curtail choice and access for consumers.
- Engage, educate, empower the consumers about the evolving privacy paradigm through educative/informative workshops
Thanks!

Swati Punia

CCIER, CUTS International

swp@cuts.org

CUTS Centre for Competition, Investment & Economic Regulation (CUTS CCIER)
D–217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: +91.141.2282821; Fx: +91.141.2282485
Email: c-cier@cuts.org; Web: http://www.cuts-ccier.org/