BEYOND CONSENT

Why New Approaches to Data Protection and Privacy for the Digital Age Are Needed

9-10 a.m. (US ET), June 13

David Medine, Renuka Sane
Speakers

David Medine
Senior Financial Sector Specialist
CGAP

Renuka Sane
Associate Professor
National Institute of Finance and Policy
India
June 13, 2019
Rethinking Notice and Consent – Global Experiences
David Medine, CGAP
Notice and Consent Doesn’t Fully Work

Indians install between 5 and 207 apps on their phones; average number of apps per phone: 51
https://techarc.net/techinsight-india-app-engagement-is-on-the-rise/

- In US, average is 80
Third-party sharing authorized per app’s privacy notice in US is 3, therefore:
  - 153 third parties authorized to get access to data in India (240 in US)
  - With little or no knowledge by app users

Hard or impossible for anyone to keep up with their privacy policies
This does not include privacy policies:
  - Web sites, home/IoT devices, automobiles, loyalty programs

Virtually no one reads privacy notices
As NIPFP has demonstrated in its study:
  - Those who read notices largely don’t fully understand them.
Unfair Burden

Putting the burden on individuals to manage their privacy is unfair
- Too many choices
- Often written in legalese
- Drafted to give companies the broadest possible use of data

Add challenges in developing countries
- Literacy
- Familiarity with technology
- Percentage of non-smart phones
- Language differences.
Consent Still Has a Role

Consent doesn’t work well to control:
- Use
- Disclosure to third parties
- Retention
- Security

Consent works better:
- Which information is given to providers
  - Either up front or during the relationship
  - Digital locker is an example of control through consent
Response

Shift responsibility from individuals to providers:

**Legitimate purposes**
- Limit use of information to specified bases
  - including relating to the purposes for which the information was collected
  - Cannot be overridden by consent

**Fiduciary duty**
- Handle data to serve the interests of the customer

**Learned intermediary**
- Person with expertise who can
  - Evaluate and test algorithms for accuracy and bias
  - Advise individuals about provider data protection practices.
Thank you

To learn more, please visit
www.cgap.org
DISCLOSURE IN PRIVACY POLICIES
Does Consent Work?

Renuka Sane
National Institute of Public Finance and Policy

July 13, 2019
Objective of Research

- Is the current method of consent on data privacy broken?
- Can consent be made to work?

Approach:
- Evaluate the quality of privacy policies (pre-EU’s GDPR version) of popular online services
- Evaluate how much users typically understand the policies in products and services they sign up for
- What can this tell us about whether consent is broken or has a chance?
Which services evaluated
Chosen for popularity, importance in sector, mix of foreign and domestic firms

WhatsApp has 98% of instant messaging market in India
Top VE app in India in terms of reach

Google is the search engine leader
with over 97% market share in India

5 million rides per week in India.
In fierce battle with Indian rival Ola

Flipkart is India’s leading e-commerce marketplace
with about 100 mln registered users

India’s leading payment gateway
First to reach over 100mln downloads in 2017
Criteria for assessing their data policies

Access to Privacy Policies:
- Number of clicks? Deeper it is embedded in website, harder in terms of time and patience it is to reach
- Length: The longer the policy, the more difficult to read
- Languages: Few than a quarter of Indians speak English as their first language
- Readability: Flesch-Kincaid (FK) grade level and reading ease tested. In the FK test, higher scores indicate material that is easier to read.

Visual Presentation: Use of highlights, section notes etc.

Substantive Content: Clear, specific provisions on privacy principles
# Results: Access and readability

<table>
<thead>
<tr>
<th>Clicks</th>
<th>Pages</th>
<th>Words</th>
<th>Languages</th>
<th>Readability</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>10</td>
<td>3,352</td>
<td>English</td>
<td>Difficult (college)</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>2,890</td>
<td>English Indian</td>
<td>Very difficult (university)</td>
</tr>
<tr>
<td>2</td>
<td>11</td>
<td>3,355</td>
<td>English</td>
<td>Very difficult (university)</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>1,767</td>
<td>English</td>
<td>Difficult (college)</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>819</td>
<td>English</td>
<td>Very difficult (university)</td>
</tr>
</tbody>
</table>
Results: Visual presentation

Uber and Google offered the most features

- Multiple sections in bold font (Uber, Google, WhatsApp)

- Notes to summarize each section made it easier to understand at a glance (Uber)

- Additional pop-ups when user moves the cursor (Google)

- Separate overview page (Uber)

- Click-throughs for more information (Uber, Google)
Results: Terminology

Here are some examples:

- “We do not retain your messages in the **ordinary course** of providing our services to you…

- “We do not share data with **third parties** but may share with **affiliates** …

- “We may retain certain **popular videos or photos** on our servers to enable easy distribution …

- “We collect device specific information when you install, access, or use our Services. This **includes** information such as hardware model, operating system information, browser information....

Policies do not have a "definitions" section (except for Google). Implies that terms are understood, or users must locate them elsewhere.
Substantive Content: Privacy principles

- Collection
- Permitted use
- Sharing with third party
- Use by affiliated entities
- Sharing with government
- Data breach notification
- Access to own data
- Data retention
- Right to seek clarification
- Exporting of data
• All five companies collect as much information as possible.

• All policies use fairly broad terminology in explaining their usage of personal information. Terminology is ambiguous. Replete with illustrative lists.

• Information sharing among group of companies is fairly common.

• Personal information is shared with law enforcement authorities. Not clear whether this is legally compliant/enforceable or not is not mentioned (except for Paytm and Google).
Analysis: Substantive content

• Policies fairly ambiguous about their data retention practices

• Information retained includes that which is necessary for providing services and is already in the custody of third parties

• Little information provided to the user about when (or if at all) data will be deleted. Certain parts may be retained in perpetuity

• Four policies provide some contact details to enable users to connect with the company in case of queries, clarifications or grievances
How much do users understand?

We surveyed students on college campuses to assess the policies

- Target users:
  - Ability to read and understand English
  - College education
  - Familiarity with selected services
  - Law vs. non-law background

We randomly assigned one of the five policies and tested students on the contents.
The sample

• 155 respondents from colleges and universities in Delhi

• 33% from a law background, 67% from a non-law (mostly economics) background

• 59% post-grad students, 41% under-grad students

• Respondents took between 10 and 20 minutes to fill out the forms
The questionnaire

Three kinds of questions: easy, intermediate, difficult.

**Example 1**: Can Paytm automatically collect details about the model/make of your computer/smartphone? (easy)

**Example 2**: Gemtm, a subsidiary of Paytm, provides a customized jewelry manufacturing service. Gemtm is interested in getting the names and contact information of Paytm users who normally carry out transactions worth more than INR 50,000 on consumables. Can Paytm provide this information? (difficult)

We restricted their answers to the following choices: Yes, No, Policy does not specify, Can't say
## Results

<table>
<thead>
<tr>
<th>Overall Average</th>
<th>5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>By study area</strong></td>
<td></td>
</tr>
<tr>
<td>Non-law</td>
<td>5.3</td>
</tr>
<tr>
<td>Law</td>
<td>5.2</td>
</tr>
<tr>
<td><strong>By degree</strong></td>
<td></td>
</tr>
<tr>
<td>Undergraduate</td>
<td>5.1</td>
</tr>
<tr>
<td>Post graduate</td>
<td>5.3</td>
</tr>
<tr>
<td><strong>By company policy</strong></td>
<td></td>
</tr>
<tr>
<td>Flipkart</td>
<td>5.3</td>
</tr>
<tr>
<td>Google</td>
<td>5.4</td>
</tr>
<tr>
<td>Paytm</td>
<td>5.5</td>
</tr>
<tr>
<td>Uber</td>
<td>5.9</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>4.6</td>
</tr>
</tbody>
</table>
Number of correct answers by question type

- More than 60% of respondents answered the easy questions correctly.
- The least correct responses were for the difficult questions, followed by the intermediate ones.
Conclusion: Quality of privacy policies

- Policies not accessible; not available in local languages
- Primarily written with a view to protect firm from liability claims
- Various rights considered essential in modern privacy law are not included in policies (data breach notification, data retention)
- No information on where data will be processed or stored, or by whom (except Google/WhatsApp which say it may be processed in the US)
- Policies assume that the user has a knowledge of legal terms
Conclusions from survey

- Average score low - even the easy questions do not have a 100% score
- Trade-off to make between length of policy and user fatigue
- When certain features are not specified, understanding is lessened
- Legal terms such as “third party” and “affiliate” are confusing and inhibit understanding
Thank you

To learn more, please visit
https://blog.theleapjournal.org/2019/02/disclosures-in-privacy-policies-does.html
Q&A

Please submit your comments and questions using the chat box. Be sure to send them to “All Participants”. Thank you

David Medine
Senior Financial Sector Specialist
CGAP

Renuka Sane
Associate Professor
National Institute of Finance and Policy
India
Thank you

To learn more, please visit www.cgap.org