STATE OF DATA PRIVACY OF INDIAN MOBILE APPS & WEBSITES

The Arrka Study 2021
As I pen this foreword on the 73rd Republic Day of India, the lines echoing in my head are those that a beloved Social Sciences teacher had made me recite decades ago – the Preamble to the Constitution:

“We, The People Of India, having solemnly resolved to constitute India into a SOVEREIGN SOCIALIST SECULAR DEMOCRATIC REPUBLIC and to secure to all its citizens:
JUSTICE, social, economic and political;
LIBERTY of thought, expression, belief, faith and worship;
EQUALITY of status and of opportunity;
and to promote among them all FRATERNITY assuring the dignity of the individual and the unity and integrity of the Nation;”

At that time, I did not really understand the purport of these lines. However, as we stand today at the cusp of a new era in Data Privacy in India with our own Data Protection law round the corner, the wealth of meaning these words carry is reinforced given how critical Privacy is to ensure the above. Along with the conviction that the much needed guardrails the law is set to establish will serve to provide the necessary wind beneath our wings as we in India continue making great strides on the technology and data fronts.

At such a moment in history, it fills all of us at Arrka with great pride to contribute our bit to the Privacy Landscape of India with this fifth edition of our Annual Privacy Study. Some interesting nuggets, some surprises, some resigned sighs of ‘things seem to be getting worse’, a few rays of hope – this is how I would summarise the findings this year.

With this edition, we have also made a switch from releasing this study in the December of every year to January 28th of every year – to coincide the release with World Data Privacy Day.

As always, we look forward to your inputs and feedback.

With Best Regards,

Shivangi Nadkarni
Co-Founder & CEO, Arrka
Jan 26th 2022
Key Highlights

Who did we study?

Mobile Apps (IOS + Android) & Websites of 201 Organizations. Of these:

- 100 were Indian Organizations across 25 Industry Sectors. We have been tracking these 100 over the last five years
- 72 were Organizations in the US & EU
- 29 were Organizations with Children's Apps

What did we study?

- What kind of Personal Data the Apps & Websites collected
- How did they share Personal Data further on
- How Transparent have they been to their users.
- How do Children’s Apps fare with respect to Privacy
- How do Indian Apps compare with US & EU Apps

Interesting Factoids on the Kind of Personal Data Apps & Websites Collected:

On Mobile Apps:

**Android Apps:**
- 74% Apps have access to your exact precise Location;
- 68% have access to your Camera;
- 54% have access to your Microphone

**IOS Apps:**
- 56% take access to your location even when the App is not in use;
- 69% have access to your Camera;
- 41% have access to your Contacts

On Websites:

- 96% Websites have at least one tracker embedded
- 21 Third Party trackers are embedded in a website on an average. Out of this 8 are Third Party cookies
- 98% websites’ embedded 3rd parties were involved in Advertising & Tracking
Interesting Nuggets on Data being shared further:

- Google is the single largest 3rd party with whom data is being shared.
- In Android Apps, 42% of the identified trackers belong to Google while 52% is the corresponding number for Websites.
- Facebook is a distant second...
  - ...with 25% of identified trackers on Android and 10% of trackers on Websites belonging to Facebook.

How Transparent are Organizations via their Privacy Notices:

- This is the Average Readability Score of an Indian Organization's Notice - which is categorized as 'Difficult to Read'.
- This is Half the acceptable International Readability Standard Score!
How Do Indian Apps & Websites Compare with those in the US & EU?

54% Indian Android Apps access your microphone compared to just 34% in the US and 30% in the EU

On the other hand, US websites were found to deploy 15 3rd Party Cookies compared to 8 in Indian Websites and 2 in EU Websites

Indian Children’s Apps:

21% had access to camera,
28% had access to phone details and
55% contained In-App Ads

87% Children’s Apps accessed at least one dangerous permission

The Arrka Privacy Index:

The Arrka Privacy Index has shown marginal improvement and stands at 53/100 this year.
Study Methodology & Approach
What Do We Study?

Data Privacy is all about Personal Data – and how much of control can an individual exercise over her Personal Data. The Arrka Study focuses on understanding some aspects of this in the context of Digital Properties of Organizations – i.e. Mobile Apps and Websites.

Specifically, we study: ‘Below The Surface’ Personal Data that Mobile Apps and Websites have access to

- What kind of Data is being collected via Permissions, Trackers and Cookies?
- Is Data being shared with external (3rd) Parties?
- Is more data than required being possibly collected?
- How transparent are organizations being via their Privacy Notices?
- Children’s Apps and some aspects therein that are critical.
- How Indian Digital Properties compare with those in the US & EU

**Note:** Personal Data is any data that can, directly or indirectly, potentially identify an individual. Why is ‘Below-the-Surface’ data important? “I may not know your name, but I know exactly what kind of person you are – your likes, your behaviour, where you live, your waking hours, your attitudes, your political leanings, etc”. Below the surface data enables this – basically enabling the building of detailed behavioural profiles of individuals which are used to target advertisements, tailor content & info and shape ideas & opinions of the target individuals.
Who Do We Study?

Overall 201 organizations and their 3 Digital properties (Android Apps, iOS Apps & Websites) were covered as part of the Study.

- 100 Indian organizations across 25 sectors
- 72 Organizations in the US & EU for Benchmarking
- 29 Children’s Apps as a separate focussed category
- 100 Indian organizations across 25 sectors

Indian Organizations

We have been tracking the same 100 organizations since 2017. Hence we do a trend analysis over the years on some key parameters as well.
How do we Study?

The Study covers 3 Key Areas related to Privacy in organizations – specific to their digital properties:

1. Personal Data Collection
2. Personal Data Sharing with 3rd Parties
3. Transparency of Practices

Note:
The data used for analysing websites is from external sources like DuckDuckGo and PrivacyScore.org. For Mobile Apps, the data used is from the testing done at the Arrka Privacy Lab. Privacy Notices have also been analysed at the Arrka Privacy Lab.
Key Findings
A. Mobile Apps

A.1: Top Dangerous Permissions Accessed

Mobile Apps collect a lot of Personal Data about a user via Permissions. ‘Dangerous Permissions’ are those via which the data collected is highly sensitive, the misuse of which can cause harm to the user.

### Top Permissions

**Android**
- 74% have access to your Exact location
- 68% have access to your Camera
- 54% have access to Microphone
- 46% can read your Contacts
- 33% can read your SMS
- 22% can use your Fingerprint *

**iOS**
- 78% have access to your Location
- 69% have access to your Camera **
- 49% have access to Microphone
- 41% can read your Contacts
- 62% can read your Photos ***
- 29% can use your Calendar

### Notes

- * Term used by Android
  * Fingerprint that is used to unlock the device
  ** Only “While using the App”
  *** Apps have “Read and Write” access to your Photos

Note: Usage of permissions can be highly contextual. In some cases, they are a ‘must have’ to provide certain features and functionalities while in some cases, they are a ‘good to have’ or are not really needed for the kind of features/functionalities provided by the app.

iOS Apps – Of the 16 Permissions we reviewed for iOS Apps, some are common with Android (e.g.: Contacts, Camera) while some are different. Moreover, certain permissions (i.e. Location, Camera) can be configured such that they can be accessed in one of two modes – ‘While Using the App’ or ‘Always’. We have also analysed the number of Apps “Always” accessing Location and accessing location only “while using the App” further in our study.
A.2: Top Categories that access Maximum Number of Dangerous Permissions

<table>
<thead>
<tr>
<th>Android</th>
<th>No. of Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>17</td>
</tr>
<tr>
<td>Mobile Wallets</td>
<td>16</td>
</tr>
<tr>
<td>Banks *</td>
<td>13</td>
</tr>
<tr>
<td>Travel Booking</td>
<td>13</td>
</tr>
<tr>
<td>iOS</td>
<td>No. of Permissions</td>
</tr>
<tr>
<td>Health &amp; Fitness</td>
<td>8</td>
</tr>
<tr>
<td>Entertainment (Ticket Booking)</td>
<td>7</td>
</tr>
<tr>
<td>Communication</td>
<td>7</td>
</tr>
<tr>
<td>News and Magazine</td>
<td>7</td>
</tr>
</tbody>
</table>

* ‘Banks’ is the new category that has found its way into this list in 2021

A.3: The Curious Case of Location Permissions

- **Android Apps**
  - Only Approximate Location: 7%
  - Only Exact Location: 9%
  - Both: 66%

- **iOS Apps**
  - Both Options “While using the App” & “Always”: 53%
  - Only While using the App: 19%
  - Never, While using the App: 3%
  - Never, Always: 3%

- More Apps access ‘Exact’ location than ‘Approximate’ location
- Apps were requesting access to both Approximate and Exact location

- 53% Apps request Access to Locations and provide users the option to choose when the App can access their Location “While using the App” OR “Always”.
A.3: Year-on-Year Trends

Given this is the 5th edition of this study, we have done some trend analysis to see how Privacy in India has been evolving.

A.3.1. Android Apps - Access to Camera and Microphone Continues to Increase

<table>
<thead>
<tr>
<th>Year</th>
<th>Accessing Camera</th>
<th>Accessing Microphone</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>45%</td>
<td>28%</td>
</tr>
<tr>
<td>2018</td>
<td>50%</td>
<td>27%</td>
</tr>
<tr>
<td>2019</td>
<td>58%</td>
<td>33%</td>
</tr>
<tr>
<td>2020</td>
<td>62%</td>
<td>46%</td>
</tr>
<tr>
<td>2021</td>
<td>68%</td>
<td>54%</td>
</tr>
</tbody>
</table>

A possible reason for this could be that organizations are providing newer services/features based on these permissions (For eg: Voice Enabled services & Facial Recognition Services)
A.3.2. Android Apps - Stabilization in SMS & Call related permission access:

There was a dramatic decrease in the SMS & Call related permissions groups in 2019 owing to stringent policy controls being imposed by the Google Playstore. This is showing a slight increase now.

A.3.3. Android Apps: Access to Location:

- More Apps are requesting access to Location over 2020.
- No significant uptrend or downtrend observed over the last 5 years.
A.3.4. Android Apps - Slight Reduction in access to Contact Data:

This is positive news to see a reversal in the trend of access to Contact Data in 2021.
B. Websites

The Website Tracker Landscape

Websites collect **Personal Data** of users from their devices via Trackers.

1. **Cookies – One Type of Tracker**
   - **1st Party Cookies**
     - Belong to the organization itself
   - **3rd Party Cookies**
     - Belong to an external organization

2. **Other Types of Trackers**
   - **1st Party Trackers**
     - Belong to the organization itself
   - **3rd Party Trackers**
     - Belong to an external organization

**Mechanisms used to share user data with 3rd Parties**

**B.1: First Party Cookies**

- 2019: 12
- 2020: 12
- 2021: 12

**Key Findings**
- **12** – Avg. number of First Party Cookies
- No change in the number of First Party Cookies in the last 3 years
B.2: 3rd Party Trackers – Cookies & Other Trackers

96% Websites studied had 3rd Party Trackers embedded.
14 of the 3rd Party Trackers are known* Advertisers
8 – Average Number of 3rd Party Cookies per Website

Top Categories embedding 3rd Party Trackers (including 3rd Party Cookies)

- Finance Stocks (91)
- News and Magazines (72)
- Finance – Mobile Wallets (31)

B.3: 3rd Party Cookies

8 – Avg. number of First Party Cookies
We have observed a 20% reduction in the number of 3rd Party Cookies over 2020

*3rd parties are known trackers or advertisers, as determined by matching them against a number of blocking lists: AdBlock Plus: the EasyList, EasyPrivacy and Fanboy’s Annoyance List (which covers social media embeds).
Are Apps Collecting More Data than required?

Like every earlier year, as part of the Study, we did a 'compare & contrast' of Apps within specific industry sectors. For this, we looked at the number and types of permissions Apps within the same sector take and looked at the differences. We categorized the permissions being taken into 3 categories:

- **Most Accessed** Permissions (>85% Apps access these),
- **Moderately Accessed** Permissions (30-85% category apps access these) and
- **Least Accessed** Permissions (< 30% Apps from the category access these).

This comparison shows us how there is variance in permissions being taken by Apps in the same sector. This leads us to wonder if those taking many more permissions compared to their counterparts are offering additional features and functionalities or is it ‘good to have’ data for other purposes.
1. Travel- Booking

- Least Accessed
  (<30% Apps access these permissions)
- Moderately Accessed
  (30-85% Apps access these permissions)
- Most Accessed Permissions
  (>85% Apps access these permissions)

- Number of Permissions being accessed by an Android Travel Booking App
  Min: 4
  Max: 21

- Number of Permissions being accessed by an iOS Travel Booking App
  Min: 2
  Max: 8
2. Banks

- **Least Accessed**
  (<30% Apps access these permissions)

- **Moderately Accessed**
  (30-85% Apps access these permissions)

- **Most Accessed Permissions**
  (>85% Apps access these permissions)

### Android Banking App

- Read and Write Calendar
- Bluetooth
- Receive and Read SMS
- Microphone
- Access to Accounts on device
- Write Contacts
- Fingerprint
- Location (Approximate and Exact)
- Camera
- Read Contacts
- Read and Write to External Storage
- Send SMS
- Read Phone Details

### iOS Banking App

- Contacts
- Photos
- Camera
- Location Services - "Always"
- Calendars
- Bluetooth Sharing
- Microphone
- Location Services "While Using the App"

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Permissions being accessed</td>
<td>18</td>
<td>8</td>
</tr>
</tbody>
</table>

- Min
- Max
3. Entertainment - Streaming

- **Least Accessed**
  (<30% Apps access these permissions)
- **Moderately Accessed**
  (30-85% Apps access these permissions)
- **Most Accessed Permissions**
  (>85% Apps access these permissions)

### Permissions

**Android Streaming App**
- Call Phone
- READ AND Write Calendar
- READ, Receive and Send SMS
- BLUETOOTH
- Microphone
- CAMERA
- READ Phone Status
- Access Exact and Approximate Location
- Read Contacts
- Access to Accounts on device
- Bluetooth
- Photos
- Microphone
- Camera
- Location Services – ‘Always’
  ‘While using the App’
- Read and Write to External Storage

**iOS Streaming App**
- Number of Permissions being accessed by an Android Streaming App
  - Min: 6
  - Max: 20
- Number of Permissions being accessed by an iOS Streaming App
  - Min: 3
  - Max: 6
4. News and Magazines

- **Least Accessed**
  (<30% Apps access these permissions)

- **Moderately Accessed**
  (30-85% Apps access these permissions)

- **Most Accessed Permissions**
  (>85% Apps access these permissions)

**Android News and Magazines App**
- Access Approximate Location
- Camera
- Read and Write Calendar
- Read Contacts
- Read Phone Details
- Bluetooth
- Access to Accounts on Device
- Reminders
- Bluetooth Sharing

**iOS News and Magazines App**
- Location Services "While Using the App"
- Location Services "Always"
- Photos
- Camera
- Contacts
- Calendars
- Microphone

Number of Permissions being accessed by an Android News and Magazines App:
- **Min:** 2
- **Max:** 16

Number of Permissions being accessed by an iOS News and Magazines App:
- **Min:** 0
- **Max:** 8
Who is your Personal Data being shared with?

The study analyzed the traffic flowing out of each App & Website to understand where data was headed out to. We looked for answers to the following questions:

1. Which entities are your data’s Top Recipients?  
2. Which functional categories do the entities belong to?

A. Android Apps

A.1 Which entities are your data’s Top Recipients?
- Google (42%) is the leading recipient of your data with Facebook (25%) coming a distant second
- We observed a long tail of small recipients, each contributing to less than 2% of the overall trackers identified. E.g. InMobi, Segment

A.2 Which functional categories do the entities belong to?
- 68% of 3rd Parties are related to Advertising and Analytics
B. Websites

B.1 Which entities are your data’s Top Recipients?
- Google (52%) is the leading recipient of your data with Facebook (10%) coming a distant second
- Google Trackers are present in 97% Websites and Facebook in 55%
- 90% of Websites use Google Analytics. The other top tracker is DoubleClick
- We observed a long tail of small recipients, each contributing to less than 3% of the overall trackers identified. E.g., Criteo, Microsoft, Twitter, Cloudflare, etc

![Proportion of 3rd parties](image)

![Presence in Websites](image)

B.2 Which functional categories do the entities belong to?
98% of Trackers are related to Advertising and Analytics.

![Categories of Trackers](image)

Note: Data on 3rd Parties for websites was extracted from DuckDuckGo. The term Google covers all properties of Google. 3rd Parties in the Development category are used to add functionality to Apps whereas Content Delivery networks ensure delivery of content in the fastest possible time.
How transparent are Organizations being with you?

To test how easy organizations were they making it for users to understand their practices, we tested Privacy Notices on ease of their Readability.

To analyze Notice Readability, we used the Industry Standard “Flesch Reading Ease Scale”. The Flesch Reading Ease scores are being used as a standard readability formula by many US Government Agencies.

Standard Acceptable scores on the Flesch Reading Ease Scale are **60-70** (on a scale of 0-100).

### Key Findings

- The Privacy Notice of an average Indian Organization is rated as **31/100** on the Readability Scale. This is **50%** of the Internationally Accepted Readability Score which applies to any document.
- The Avg. Readability Score of Indian organizations has not changed in the past 3 years.
- **39%** of Privacy Notices are at “Very Confusing” score level.

---

**Categories with the lowest Notice Readability Scores are**

- Finance - Banks (22)
- Sports (26)
- Entertainment - Ticket Booking (27)

Readability scores for Banks saw a significant drop of **15%** from 2020.
Special Focus Area: Children’s Privacy

Children are a particularly vulnerable category. Hence, one area we specifically studied over and above the 100 base Apps were Android Apps from India targeting children. Along with studying Personal Data Access, we also reviewed aspects specific to Children’s Apps.

87% Apps accessed at least one Dangerous Permissions

- 21% access to your Camera
- 14% access to Microphone
- 10% can read your Contact
- 7% have access to your Exact location
- 62% had access to Files on Storage
- 28% had access to Phone Details
- 55% provided In-App purchase
- 55% served In-App ads

Although Children’s Apps access & share significantly lesser Personal Data as compared to Regular Apps, there is scope for further improvement. Significant increase in Apps accessing Camera as compared to 2020. 55% Apps serve In-App ads.
Indian Organizations in comparison with EU & US Organizations

To understand how Indian Organisations stack up in comparison to US and EU Organisations in terms of Personal Data accessed, we studied 35 EU and 37 US Organisations to study the patterns. There is a significant difference in certain types of Personal Data accessed.

A. Android Apps

Our study finding indicates that significantly higher number of Indian Apps request access to specific permissions as compared to their Global counterparts. US Apps come a distant second and the EU Apps take the least permissions.

A combination of Google Playstore Policy Changes and stringent Privacy regulations like GDPR appear to be changing App behaviour in the EU and, to a lesser extent, in the US.

Comparison with International Apps
Indian Websites fare much better as compared to the US.

- Significantly higher Trackers are deployed by US Websites as compared to Indian Websites.
- We also observed a significantly higher use of Google Analytics by Indian Websites as compared to US and EU Websites.

### 3rd Party Trackers Embedded

<table>
<thead>
<tr>
<th></th>
<th>INDIA</th>
<th>US</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>22</td>
<td>25</td>
<td>10</td>
</tr>
</tbody>
</table>

### 3rd Party Cookies

<table>
<thead>
<tr>
<th></th>
<th>INDIA</th>
<th>US</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>8</td>
<td>15</td>
<td>2</td>
</tr>
</tbody>
</table>

### Use of Google Analytics

<table>
<thead>
<tr>
<th></th>
<th>INDIA</th>
<th>US</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>90%</td>
<td>33%</td>
<td>41%</td>
</tr>
</tbody>
</table>
The Arrka Privacy Index

- Provides a Unified Privacy Score across Mobile Apps & Websites
- Covers 9 Privacy Principles
- Evaluates using 57 Parameters
- Assimilates the Contextual nature of Privacy like Sectoral differences
- Scores can fall between 0-100. Higher the score better the Privacy

India Privacy Score

53/100
<table>
<thead>
<tr>
<th>#</th>
<th>Category</th>
<th>Privacy Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sports</td>
<td>65%</td>
</tr>
<tr>
<td>2</td>
<td>Games</td>
<td>64%</td>
</tr>
<tr>
<td>3</td>
<td>Finance - Stocks</td>
<td>62%</td>
</tr>
<tr>
<td>4</td>
<td>Education</td>
<td>61%</td>
</tr>
<tr>
<td>5</td>
<td>Classifieds</td>
<td>60%</td>
</tr>
<tr>
<td>6</td>
<td>Government</td>
<td>58%</td>
</tr>
<tr>
<td>7</td>
<td>Entertainment - Streaming</td>
<td>58%</td>
</tr>
<tr>
<td>8</td>
<td>Music &amp; Audio</td>
<td>57%</td>
</tr>
<tr>
<td>9</td>
<td>Communication</td>
<td>57%</td>
</tr>
<tr>
<td>10</td>
<td>Jobs</td>
<td>57%</td>
</tr>
<tr>
<td>11</td>
<td>Finance - Fintech Market Place</td>
<td>56%</td>
</tr>
<tr>
<td>12</td>
<td>Dating</td>
<td>56%</td>
</tr>
<tr>
<td>13</td>
<td>Finance - Banks</td>
<td>53%</td>
</tr>
<tr>
<td>14</td>
<td>Shopping</td>
<td>52%</td>
</tr>
<tr>
<td>15</td>
<td>House &amp; Home</td>
<td>52%</td>
</tr>
<tr>
<td>16</td>
<td>Food &amp; Drink</td>
<td>51%</td>
</tr>
<tr>
<td>17</td>
<td>Travel - Maps &amp; Information</td>
<td>50%</td>
</tr>
<tr>
<td>18</td>
<td>Finance - Mobile Wallets</td>
<td>50%</td>
</tr>
<tr>
<td>19</td>
<td>Vehicles</td>
<td>50%</td>
</tr>
<tr>
<td>20</td>
<td>News &amp; Magazines</td>
<td>49%</td>
</tr>
<tr>
<td>21</td>
<td>Travel - Booking</td>
<td>49%</td>
</tr>
<tr>
<td>22</td>
<td>Medical</td>
<td>44%</td>
</tr>
<tr>
<td>23</td>
<td>Entertainment - Ticket Booking</td>
<td>42%</td>
</tr>
<tr>
<td>24</td>
<td>Travel - Taxi &amp; Ride Sharing</td>
<td>40%</td>
</tr>
<tr>
<td>25</td>
<td>Health &amp; Fitness</td>
<td>37%</td>
</tr>
</tbody>
</table>

NOTE: As part of this Study, we are publishing an abridged version of the Privacy Index in which we have used a subset of 15 parameters covering areas like Personal Data Collection, Sharing, and Transparency Practices.
## Readiness for the upcoming India Data Protection Bill

<table>
<thead>
<tr>
<th>#</th>
<th>India DPB 2021 Requirements</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Fiduciary shall provide a Privacy Notice to Data Principals at the time of Data Collection</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>The Privacy Notice should provide Information to Data Principals about the Fiduciaries' Personal Data Processing Practices</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>The Privacy Notice shall be clear, concise and easily comprehensible to a reasonable person</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>The Privacy Notice shall be in multiple languages where necessary and practicable.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>Collection Limitation:</strong> The Personal Data shall be collected only to the extent that is necessary for the purposes of processing of such personal data</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>Children's Data:</strong> The data fiduciary shall be barred from targeted advertising directed at children</td>
<td></td>
</tr>
</tbody>
</table>

**Key Findings**

- All Organizations have documented a Privacy Notice on the App Store and Website
- From a Content perspective, organizations are sharing partial information regarding Personal Data processing when compared to the bill's requirements
- Privacy Notices are largely “Difficult to Read” as per the Readability Scale and are at **50%** of Internationally Acceptable Standards of readability
- Organizations have only drafted the Privacy Notices in English. This may make it less accessible to the lay user
- Indian Apps may be collecting more Personal Data than required based on:
  - Comparison with Global Apps
  - Higher granularity of data requests (E.g. More Apps seek Exact location to Approximate Location)
  - High Intra Category variation in permission requests
- **55%** of the Children's Apps allowed In-App advertising which is in violation of the India DPB 2021
Conclusion

As we spent 2021 in and out of our homes, technology continued to be our lifeline. In the midst of this, we waited the whole year for the Joint Parliamentary Committee to publish its report and the updated version of the Data Protection Bill. The much-awaited report came towards the end of December 2021.

Meanwhile, India Inc seems to have continued on its trajectory of paying scant attention to Data Privacy, with the unstated paradigm being ‘let the law come’. This is evident from the data in this study where most privacy-specific parameters seem to have only gotten worse.

However, the year 2022 certainly holds out hope. Hope that the Data Protection Law will soon become a reality. Hope that Indian Organizations will start taking baby steps towards privacy. And, thereby, hope that the data we find next year shows a reversal in the trends seen thus far.
All the testing for this study was carried out at the Arrka Privacy Testing Lab. A one-of-its-kind lab in India, it is dedicated exclusively to privacy testing of mobile apps, websites and other digital properties & technology infrastructure.
Arrka: India’s Privacy Specialist
Empowering Organizations to get Privacy Compliant via smart automation since 2012

www.arrka.com
privacy@arrka.com
@arrka2
www.linkedin.com/company/Arrka
https://www.facebook.com/arrkaconsulting/

Arrka empowers organizations to assess, design, implement and manage their Data Privacy Programs across multiple laws & jurisdictions. Arrka’s Privacy Management Platform (APMP) - the first of its kind from India - enables automation. This is complemented by the Arrka Lab and Arrkademy. To know more visit www.arrka.com

All brand names, logos and digital properties referred to in this report are the property of the respective organisations. This material and the information contained herein has been prepared by Arrka Infosec Private Limited (“Arrka”). It is intended to provide general information on the subjects under consideration and is not an exhaustive treatment of the said subjects. The information is not intended to be relied upon as the sole basis for any decision which may affect you as an individual or your business. Arrka shall not be responsible for any loss whatsoever sustained by any person who relies on this material.

©2022 Arrka Infosec Private Limited