Index

- Foreword 3
- Executive Summary 4
- Setting the Context 6
- Methodology and Approach 7
- Personal Data Collection: 9
  - What Personal Data is being collected and How?
  - Are Apps Collecting more Personal Data than needed?
- Personal Data Sharing: Who is your Personal Data being shared with? 14
- Cross Border Movements: Which Countries outside India is your Personal Data travelling to? 16
- Are Organizations being transparent with you? 17
- Special Focus: Are Children’s Apps safe? 18
- How do Indian Apps compare with Global Apps on Privacy? 19
- The Arrka Privacy Index 21
- Conclusion 22
- Authors 23
Foreword

‘It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair…”

- Charles Dickens in ‘A Tale of Two Cities’, circa 1859

160 years after these famous opening lines, the world seems to be back at the same juncture - at least, the world of Data Privacy in India. The world is watching with bated breath what law India is going to adopt for Personal Data Protection. At stake is the data of the second largest digital population in the world.

Meanwhile, the global scene has been busy this year. Amongst things directly impacting digital properties like Mobile Apps and Websites in India, giants like Google, Apple and Facebook have made some significant policy changes. The results are seen in this year’s study when compared to last year.

In this volatile environment, it has been interesting for us at Arrka to undertake this 2019 study. From its inception in 2017, we have been adding onto the scope of the study. In 2017, it was just Android Apps. Last year, 2018, we added on their iOS counterparts and their associated Websites, along with some global benchmarks and a special ‘Children’s Apps’ section.

During the course of this year, the Arrka team has been working on developing the Arrka Privacy Index for organizations. Taking a leaf out of this yet-to-be-launched Index, we are excited to publish a Privacy Index for only Mobile Apps and Websites with this study.

We look forward to this third edition of the ‘State of Data Privacy of Indian Mobile Apps & Websites - 2019’ report equipping various stakeholders with some valuable data points for India.
Executive Summary

Study Coverage
- 100 Indian Organizations
- 25 Industry Categories
- 300 Indian Android Apps, iOS Apps and Websites
- 50 EU & US Organizations

Personal Data Collection

Android Apps:
- 75% Apps have access to your Exact Location
- 58% Apps have access to your Camera
- Mobile Wallets access the highest number of Dangerous Permissions – 11 Permissions
- Google Play store policy now restricts access to SMS & Call Related permissions. The impact of these revisions has been observed in our study. There has been a 45% decrease in Apps reading SMS.
- 39% Permissions accessed in Android Apps are Excessive.
- 50% Apps seeking Location permission in Android Apps did not need it

iOS Apps:
- Apple Store guidelines around “requesting Permissions only when the App needs it” had a significant impact on the access to Personal Data
- Only 50% Apps seek any permission at launch
- iOS Apps access only 3 types of permissions Service during launch as compared to 14 types of Permissions in 2018
- 48% iOS Apps access Location Services during Launch of which 12% Apps access Location even when the App is not in use

Websites:
- 93% Websites have known 3rd Parties embedded that were involved in Advertising & Tracking
- On an avg. 15 Known 3rd Party Trackers embedded in a website. On an average 4 Excess Trackers were found to be embedded in Websites
- An avg. of 65 Trackers were found in websites belonging to the News & Magazines Category (Highest for a category)
- 78% Websites Deploy 3rd Party Cookies with an average of 10 Cookies per Website
- Setting Long Term Cookies is a favored Tracking mechanism over Short Term Cookies. No instance of Flash Cookies was observed

Personal Data Sharing
- More than 95% Mobile Apps and Websites share data with 3rd Parties
- On an average, Mobile Apps and Websites share data with 4 3rd Parties
- 40% reduction in 3rd Parties embedded in Android & iOS Apps as compared to 2018.
- Industry Consolidation, Vendor Rationalization & Privacy Awareness is leading to reduction in 3rd Parties
- Google is the largest 3rd Party with 39-50% of the Traffic across Apps and Websites being directed towards it
- Highest proportion of 3rd Parties (~60%) fall into the Development Tools category. We observed a sharp decline in proportion of Analytics Providers
Executive Summary

Cross Border Transfer
- 97% of the data traffic from Apps travels outside India.
- 86% of the traffic from Apps is headed to the USA.
- No instance of data transfer has been observed to Singapore and China in 2019.

Transparency
- Based on the Fleisch Reading Scale, the Privacy Notices for Indian organizations are "Difficult to Read". 40% Privacy Notices are "Very Confusing".
- No improvement in Readability has been observed over 2018 which is of concern.
- Readability Scores of Privacy Notices for Indian organizations are 50% less than the Accepted Global Standard.

Children's Apps
- Although Children’s Apps access & share significantly lesser Personal Data as compared to Regular Apps, there is scope for further improvement.
- 29% Apps have access to Phone Details and 7% have access to Camera, Microphone & Contacts.
- 78% Apps did not take Consent & 42% Privacy Notices did not address Children.
- 93% Apps were found to contain In-App ads with over half of these ads marketing irrelevant services.
- Although 57% Apps offered In-App Purchase options, only 38% Apps have Parental Control features to restrict access to Children.

Comparison with Global Apps
- A combination of Play store Policy Changes and stringent Privacy regulations like GDPR are changing App behavior in EU and to a lesser extent in the US.
- Significantly higher proportion of Indian Apps access Exact Location and read SMS as compared to US and EU Apps.
- 29% Indian Apps read SMS as compared to 4% Apps in the EU and US.
- 4% of EU Apps accessed Exact Location as compared to 75% Indian Apps.
- 0% of EU iOS Apps accessed Location services when App was not in use as compared to 12% Indian and 35% US Apps.

Arrka Privacy Index
- The Arrka Privacy Index was designed to understand Privacy Readiness & Maturity of Digital Properties in India and understand sectoral variations.
- The Arrka Privacy Index provides a composite score across Mobile Apps & Websites. It takes into consideration the Contextual nature of Privacy.
- Arrka Privacy Index covers 9 Privacy Principles and assesses Mobile Apps and Websites across 57 Parameters.
- Arrka Privacy Index for India is 52 (out of a maximum possible score of 100).

THE ARRKA STUDY 2019
A. Personal Data: Personal Data is any data that can, directly or indirectly, potentially identify an individual. Personal Data can be categorized into ‘Above-the-Surface’ data (visible to an individual) and ‘Below-the-Surface’ data (not easily visible to an individual). Our study focuses largely on “Below the Surface” data.

Why is ‘Below-the-Surface’ data important? “I don’t want to know who you are, but I would like to know what you do, online”. Below the surface data enables this – basically enabling the building of detailed behavioral profiles of individuals which are used to target advertisements, tailor content and info and shape ideas and opinions of the target individuals.

B. Privacy Principles: Privacy principles represent the core of privacy protection and they provide a holistic lens to analyze Privacy. They also form the underlying components around which Personal data protection or privacy laws across the world are based. In our study we have selected 3 principles to focus on: Collection Limitation, 3rd Party Disclosure and Notice. We selected these because we could test these externally without involving the target organization. We did not test for Security this time around as we believe organizations have reached a certain degree of maturity - based on our past 2 editions of the study.

Privacy Principles & User Concerns

- **Notice** - Are you clearly and unambiguously telling me all that you do with my Personal Data?
- **Consent** - Is my consent being taken on all that is being done with my Personal Data?
- **Collection Limitation** - Is the Personal Data being collected more than what is required?
- **Purpose and Usage Limitation** - Why are you collecting my Personal Data? What are you going to use it for? Are you going to use it to track me & build my profile?
- **Access and Correction** - Can I access my Personal Data & make corrections as and when required?
- **Disclosure/3rd Party Transfer** - Are you sharing my Personal Data with a 3rd party? Is my Personal Data being sent outside geographical boundaries?
- **Security** - Is my Personal Data adequately protected and safeguarded?

*The focus areas of the study*
Methodology and Approach

In this section, we detail the “What” and the “How” of the study. A. What - Apps we covered in the study and the Sampling methodology. B. How - Privacy Principles we selected and how we tested each principle.

A. Sampling Methodology
The study covered 100 organizations from India and 3 digital properties of each organization: An Android App, its iOS counterpart and the associated Website. The organizational categories have been defined based on Google Playstore definitions and industry nomenclature. We chose organizations across categories to ensure fair representation. Within each category, organizations were chosen based on popularity. For eg., more than 90% of the Android Apps chosen have had greater than one million downloads on Android and 58% of the Websites chosen were among the Top 500 Indian websites based on Alexa ratings. We have maintained the same stratification as our 2018 study to ensure consistency and promote trending.
B. Testing Approach & Areas Covered:
We cover 4 key Areas of Privacy practices in organizations: Personal Data Collection, Sharing with 3rd Parties, Data movement across borders and Transparency & Accountability. All these areas provide insights on the 3 Privacy principles of Collection Limitation, Disclosure to 3rd Parties and Notice. The data gathered and the technique involved varies based on Mobile Apps and Websites. For Websites, we have used external sources for data gathering, like the DuckDuckGo Browser Privacy Statistics and PrivacyScore.org statistics to gather insights into Tracker usage.

Permissions accessed by Apps at the time of Launch have been studied.

Based on our 2018 Study of Websites, Trackers are the primary source of Personal Data Collection as compared to Permissions. Hence our study this year has only focused on Trackers.

Mobile Apps have 3rd Party SDKs embedded which have access to Personal Data collected via permissions. Similarly Websites have 3rd Party Trackers. In Apps, we used Network Analysis to study 3rd Parties.

Cross Border Transfer in Apps was studied using Network Analysis by analyzing the IP address of 3rd Parties.

Organizations are becoming more Privacy aware and are placing Privacy Notices on their Mobile Apps and Websites. Hence this year, we have focused only on ease of readability of these Notices.

Note: *Apps and Websites can transfer data to 3rd Parties offline which cannot be tracked. We are only covering the online transfer of Data.
Personal Data Collection: What Personal Data is being accessed and How?

Mobile Apps and Websites obtain Personal Data of users from their devices via Permissions and Tracking Mechanisms. The types of Permissions and Tracking Mechanisms used are different for Mobile Apps and Websites. Further, there is a difference between the Android and iOS Permission groupings. The study analyzes all these areas.

Android Apps

The following table highlights the most accessed dangerous permissions by Apps. Access to Dangerous Permissions should ideally be driven by the functionalities provided by the App. But this does not always happen. Apps demand access to Permissions from users without providing any corresponding functionality. Hence access to permissions can be highly contextual depending on category of App and services provided.

### Top Dangerous Permissions

- **86%** Can write to your external Storage
- **75%** Have access to your Exact location
- **66%** Have access to Phone details including Phone number

### Other Key Dangerous Permissions

- **58%** Have access to your camera
- **40%** Can read your contact
- **33%** Have access to microphone
- **29%** Can read your SMS

### Categories using the most no. of Dangerous Permissions per App

- **Mobile Wallets (11)**
- **Classifieds (10)**
- **Communication (9)**
Key Trends and Comparison to 2018

1. Reduced Variation in Volume of Permission Access:
The gap between the Categories taking the maximum & minimum permissions has gone down by 30% as compared to 2018. This indicates a growing industry maturity in Privacy and subsequently judicious usage of permissions.

2. Dramatic Reduction in SMS & Call related permission access:
Decreases were observed in the access of SMS & Call related permission groups. This decrease could be attributed to the changes in Google Playstore policy which restricts the access to these permission groups due to their sensitive nature.

3. At the same time Access to Camera and Microphone Permissions saw a steady increase. This indicates that organizations are providing newer services/features based on these permissions (i.e. Increase in Voice Enabled services)

4. Steep Reduction in Permissions Taken observed in sectors like Communication, Medical. This could be attributed to overall awareness on Privacy among organizations and Google Play store policy restrictions.
iOS Apps

The Permission structure of iOS is a little different from that of Android. There are 16 Permissions in all, some of which are common with Android (eg: Contacts, Camera) while some are different (Apple Music, TV Account). Moreover, certain permissions (i.e. Location, Microphone and Camera) can be configured such that they can be accessed in one of two modes – ‘While Using the App’ or ‘Always’. As part of our Testing methodology, we record permissions taken during Launch

FINDINGS

We observed a marked change in App behavior over 2018 Study in the area of seeking permissions.

Only 50% Apps sought permission at Launch as compared to 100% in 2018

Apps seeking permission at Launch only accessed 3 types of permissions as compared to 14 Types in 2018

Location Services is the only significant Permission sought at launch. 36% of Apps seeking Location permission “only when App is in usage” whereas 12% of Apps “Always” track Location whether the App is in use or not

% Apps Accessing Permissions at Launch  No. of Permission Types accessed during Launch

2018 | 100% | 14
2019 | 52% | 3

Trends - Key iOS Permissions Accessed

<table>
<thead>
<tr>
<th>Permission</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photos</td>
<td>100%</td>
<td>88%</td>
</tr>
<tr>
<td>Camera</td>
<td>79%</td>
<td></td>
</tr>
<tr>
<td>Location Services</td>
<td>48%</td>
<td>72%</td>
</tr>
<tr>
<td>Calendar</td>
<td>3%</td>
<td>37%</td>
</tr>
<tr>
<td>Contacts</td>
<td>36%</td>
<td></td>
</tr>
<tr>
<td>Microphone</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>Bluetooth Sharing</td>
<td>25%</td>
<td></td>
</tr>
</tbody>
</table>

Conclusion

• We conclude that most Permissions are sought by Apps only at the time they need it (post login and in usage) Just In Time

• The key reason for this change in App behavior could be attributed to the revision in Human Interaction Guidelines for iOS Apps which states that Apps should:
  • Request permission at launch only when necessary for your app to function.
  • Request Personal Data only when your app clearly needs it (Just In Time).
Websites
The 2018 Study had Analyzed Permissions and Tracking mechanisms deployed by websites and had concluded that Trackers were the key mechanisms deployed by Websites. Hence this year we focused on studying trackers in detail. Cookies is one of the tracking mechanisms and we focused on Cookies set by both First Parties (Organizations that own the websites) and Third Parties. Third Party cookies are used to share data with 3rd Parties. As we have a separate section dedicated to Personal Data sharing, we will only focus on the volume & Type of 3rd Party Cookies in this section. We also distinguished between the cookie types: Short Term, Long Term, Flash Cookies.

## 3rd Party Trackers

<table>
<thead>
<tr>
<th>%</th>
<th>Websites studied had 3rd Party Trackers embedded</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>Websites had known 3rd Parties embedded that were involved in Advertising &amp; Tracking</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avg. #</th>
<th>3rd Party Trackers Embedded in a Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Avg. # of Known 3rd Party Trackers embedded in a website</td>
</tr>
</tbody>
</table>

### 3rd Party Trackers

- **Categories with Max Embedded 3rd Party Trackers**
  - **(65)** News and Magazines
  - **(58)** Finance – Stocks
  - **(39)** Entertainment – Ticket Booking

### Cookies in Websites

- **78%** of Websites studied deployed Third-Party Cookies
- **92%** of Websites studied deployed First Party Cookies

<table>
<thead>
<tr>
<th>Avg. # - 3rd Party Cookies</th>
<th>Avg. # - First Party Cookies</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>7</td>
</tr>
</tbody>
</table>

- **Short Term**
- **Long Term**

- **On an average, Websites deployed 10 Third Party Cookies**
- **On an average, Websites deployed 12 First Party Cookies**

  - No instances of Flash Cookies were observed either in First Parties or Third Parties
  - Setting Long Term Cookies is a favored Tracking mechanisms

---

Note: Details on trackers are based on Stats from PrivacyScore.org which is a publicly available tool to assess the security and privacy measures of websites.

*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).*
Personal Data Collection:
Are Apps & Websites collecting more Personal Data than needed?

Personal Data Collection by Apps through Permissions and Trackers is highly contextual and varies based on Categories and the functionality provided by the Apps. Hence determining whether Apps have taken more Personal Data than needed is a complex task. As part of the Study, we have identified a few indicators which evaluate Excessive Personal Data Collection in an objective manner.

**Android Apps**

**Indicator 1:** \% *Excess Permissions accessed by Apps without providing any corresponding functionality*

**Key Findings:**
1. 39% Permissions accessed by Android Apps are Excessive
2. 50% of the Apps which ask for Location access did not need it
3. 18% more excessive permissions are being accessed by Apps as compared to 2018

**2. Indicator 2: #Intra Category Variation in Permissions**

The variation in the number of permissions accessed by Apps in the same category is hard to justify as the functionality provided is approximately similar. This could indicate Excess Permissions.

**Key Findings:**
1. Apps taking the highest permissions in a category take 5/2.5X more Permissions than the App taking the lowest permissions
2. Travel-Booking is the category with the maximum Intra-category variation of 12 Permissions

---

**Websites**

**Indicator:** Number of Trackers Blocked by the Browser for a website without impacting site functionality is a good indicator of excess Trackers (and excess Personal Data Collection)

The more the number of trackers blocked, the worse the Privacy provided by the website as it could potentially operate without the trackers.

**Key Findings:**
1. On an average 4 Trackers were blocked for a Website
2. Vehicles is the worst performing category where an average of 8 Trackers were blocked

---

*How do we Test for Excess Permission: We turn off access to a permission and then test if the App still functions. If the App functions, we conclude that the Permission is not required, hence qualifying as an Excess permission

*How do we compute Intra-Category Variation: For Apps belonging to the same category, we compute Maximum Permissions taken – Minimum Permissions Taken

*The Number of Trackers blocked by Browser data for Websites are based on DuckDuckGo Browser stats. DuckDuckGo is a Privacy Friendly browser which publishes Privacy related statistics for websites...
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:
A. How many 3rd Parties was each App/Website sending data out to?
B. Which parent organizations did these 3rd Parties belong to?
C. Which functional categories did these 3rd Parties belong to?

A. No. of 3rd Parties

Key Findings:
• More than 95% Mobile Apps and Websites share data with 3rd Parties
• Avg. # Third Parties: On an average, Mobile Apps and Websites share data with 4 3rd Parties
• Vehicles is the category which sends data to the highest 3rd Parties and appears in the top category list across Mobile Apps and Websites

Trend 1: There is about 40% reduction in Average 3rd Parties embedded in an App as compared to 2018. This is observed across Android and iOS Apps

Trend 2: We also observed a 65% reduction in the total number of unique 3rd Parties observed across all Apps

The above trends indicates 3 things
1. Consolidation in the Digital Analytics industry due larger analytics providers acquiring smaller players, generalist software companies wanting to add analytics capabilities to their mix
2. Buyer organizations doing vendor rationalization
3. Growing awareness in organizations of the 3rd Parties embedded in an App knowingly or unknowingly and the impact of Privacy regulations.
B. 3rd Party Organizations
We looked at which specific 3rd Parties data was being shared with and categorized them based on their parent organizations. Google as an entity (aggregated across all their properties) was found to be where the highest percentage of traffic was headed out to across Apps as well as Websites. The 3rd Parties & proportion of traffic to them across both Android and iOS Apps were more or less the same.

Top 3rd Parties Embedded in Apps and Websites
Numbers denote %

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>iOS</th>
<th>Websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>21</td>
<td>12</td>
<td>39</td>
</tr>
<tr>
<td>Facebook</td>
<td>7</td>
<td>13</td>
<td>40</td>
</tr>
<tr>
<td>Amazon</td>
<td>21</td>
<td>18</td>
<td>51</td>
</tr>
<tr>
<td>AppsFlyer</td>
<td>30</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Adobe</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Interestingly, even in iOS Apps, the largest 3rd Party is Google!

Note: The 3rd Party Category Analysis only covered Mobile Apps
*The numbers represent an average for iOS and Android Apps. There is a minor differences in the proportion of the categories

C. 3rd Party Categories
The top categories of 3rd Parties with whom data was being shared with were Advertising, Analytics and Development (used to add functionality to Apps), Authentication (where platforms like Google and Facebook are used to authenticate users).

- Advertising & Analytics providers form 1/3rd of the 3rd Party Categories
- There is a significant reduction in proportion of Analytics providers from 2018 which could be attributed to the consolidation in the Analytics space, and growing Privacy awareness

Proportion of 3rd Party Analytics Providers

<table>
<thead>
<tr>
<th></th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>27</td>
<td>17</td>
</tr>
<tr>
<td>iOS</td>
<td>47</td>
<td>18</td>
</tr>
</tbody>
</table>

*Apps – 3rd Party Category Analysis
Which Countries is your Personal Data travelling to?

Cross Border Data Destinations
We studied Mobile Apps to identify the first destination country data was heading out to. 95% of organizations studied sent data across the border. The USA is the primary destination of all the data being transferred outside India with 86% of the traffic being directed there. This is probably owing to the fact that most of the 3rd Party Advertisers and Analytics companies are based out of the US. At a distant second came Ireland.

Key Findings
1. 97% of the data traveled out of India.
2. Though the top international data destinations remain the same; the spread of countries has decreased considerably this year.
3. Surprisingly, No instance of data transfer has been observed for Singapore and China.

Note: We did not cover websites as part of this analysis

Note: 3% of remaining data was split between smaller destinations like France, Netherlands and other destinations which could not be verified.
Are Organizations being Transparent with you?

To test how easy organizations were they making it for users to understand their practices, we tested Privacy Notices on ease of Readability. To analyze Notice Readability, we used the Industry Standard “Fleisch Reading Ease Scale”. The Fleisch Reading Ease scores are being used as a standard readability formula by many US Government Agencies. Standard Acceptable scores on the Fleisch Reading Ease Scale are 60-70 (on a scale of 0-100).

**Fleisch Reading Ease - Result Interpretation Table**

<table>
<thead>
<tr>
<th>Score</th>
<th>Very Confusing</th>
<th>Difficult</th>
<th>Fairly Difficult</th>
<th>Standard</th>
<th>Fairly easy</th>
<th>Easy</th>
<th>Very easy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30-49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50-59</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60-69</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70-79</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80-89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90-100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Least Readable Categories**

- Sports (21)
- Music & Audio (23)
- Communication (23)

**Key Findings:**
- The Privacy Notices for Indian organizations are on an average “Difficult to Read”. 40% Privacy Notices are “Very Confusing”
- Readability of Privacy Notices for Indian organizations is 50% less than the Accepted Global Standard
- Avg. Readability of Privacy Notices has not changed from 2018
Special Focus: Are Children’s Apps safe?

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 and Sharing, we also reviewed aspects specific to Children’s Apps.

Key Findings:

- **29%** Apps took NO Permissions
- **0%** Apps had access to Location
- **7%** Apps accessed Camera, Microphone & Contact
- **29%** Apps accessed Phone Details

- **57%** Apps offered In-app purchase options
- **93%** Apps were found to contain In-App ads
- **78%** Apps did not obtain consent

- **38%** Apps had Parental Control features to restrict Children’s access
- **64%** Apps have links to other Apps
- **42%** of Apps did not have a Notice addressing children under age 13.

Comparison: Personal Data Collection & Sharing

- Number of 3rd Parties: Regular Apps 4, Children’s App 2
- Number of Permissions Accessed: Regular Apps 7, Children’s App 2

- Although Children’s Apps access & share significantly lesser Personal Data as compared to Regular Apps, there is scope for further improvement
- In-App ads displayed in Children’s Apps need to be reviewed as close to 50% offered irrelevant services
- Apps offering in-App purchases need to offer Parental Control features. Only 2/3rd of Apps offering In-App purchases had parental controls
How do Indian Apps compare with Global Apps on Privacy?

E. Comparison with Global Apps
To understand, how Indian Apps stack up in comparison to US and EU Apps in terms of Personal Data accessed, we studied 24 EU and 25 US Apps to study the patterns.

Android Apps:
Our study finding indicates that while the Average number of permissions accessed by all 3 regions are approximately the same (6-7), we observed significant differences in access to certain permissions. Significantly higher proportion of Indian Apps access Exact Location and Read SMS as compared to US and EU Apps

iOS Apps:
Although most permissions are accessed “Just In Time” in iOS (and not upfront during launch), we observed some clear patterns differences in accessing permissions at the time of launch across the 3 regions. iOS – EU and US Apps access significantly more permissions at the time of download versus Indian Apps. EU Apps are Privacy sensitive and this is indicated as no EU App tracks User Location when they are not using the App.

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

Stringent GDPR requirements are clearly changing App behavior in the EU.

EU and US Apps need significantly greater permissions upfront for the App to function.
As we work closely with organizations in helping them implement Privacy Programs, we have been increasingly realizing that both internal and external stakeholders are looking to get a sense of where the organization really stands when it comes to privacy. An overall ‘temperature check’. At the same time, we also felt the need for a metric that will compare & contrast organizations: with each other, across sectors, at a country level etc. This led us to develop the Arrka Privacy Index.

In this report, we apply the index to Mobile Apps and Websites to give our readers a quantifiable sense of where Indian organizations really stand with respect to privacy.

- 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 Index - 52

<table>
<thead>
<tr>
<th>#</th>
<th>Category</th>
<th>Privacy Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>📞 Communication</td>
<td>63</td>
</tr>
<tr>
<td>2.</td>
<td>🛫 Travel - Maps and Information</td>
<td>61</td>
</tr>
<tr>
<td>3.</td>
<td>🎮 Games</td>
<td>61</td>
</tr>
<tr>
<td>4.</td>
<td>🚩 Education</td>
<td>60</td>
</tr>
<tr>
<td>5.</td>
<td>🍽 Food and Drink</td>
<td>59</td>
</tr>
<tr>
<td>6.</td>
<td>🏦 Finance - Banks</td>
<td>58</td>
</tr>
<tr>
<td>7.</td>
<td>🎬 Entertainment - Streaming</td>
<td>55</td>
</tr>
<tr>
<td>8.</td>
<td>🏛 Government</td>
<td>54</td>
</tr>
<tr>
<td>9.</td>
<td>📣 Jobs</td>
<td>53</td>
</tr>
<tr>
<td>10.</td>
<td>🌐 Dating</td>
<td>53</td>
</tr>
<tr>
<td>11.</td>
<td>🚘 Travel - Taxi and Ridesharing</td>
<td>53</td>
</tr>
<tr>
<td>12.</td>
<td>🏥 Health and Fitness</td>
<td>52</td>
</tr>
<tr>
<td>13.</td>
<td>₹ Finance - Fintech Market Place</td>
<td>51</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Category</th>
<th>Privacy Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td>🏠 House and Home</td>
<td>50</td>
</tr>
<tr>
<td>15.</td>
<td>✈️ Travel - Booking</td>
<td>50</td>
</tr>
<tr>
<td>16.</td>
<td>🏀 Sports</td>
<td>49</td>
</tr>
<tr>
<td>17.</td>
<td>🎵 Music and Audio</td>
<td>49</td>
</tr>
<tr>
<td>18.</td>
<td>🔐 Classifieds</td>
<td>49</td>
</tr>
<tr>
<td>19.</td>
<td>🍓 Medical</td>
<td>49</td>
</tr>
<tr>
<td>20.</td>
<td>🤑 Finance - Mobile Wallets</td>
<td>49</td>
</tr>
<tr>
<td>21.</td>
<td>🏦 Finance - Stocks</td>
<td>48</td>
</tr>
<tr>
<td>22.</td>
<td>📰 News and Magazines</td>
<td>48</td>
</tr>
<tr>
<td>23.</td>
<td>🛒 Shopping</td>
<td>46</td>
</tr>
<tr>
<td>24.</td>
<td>🎟 Entertainment - Ticket Booking</td>
<td>46</td>
</tr>
<tr>
<td>25.</td>
<td>🛶 Vehicles</td>
<td>43</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, Cross Border Transmission and Transparency Practices.
Conclusion

Although Data Privacy is still at a nascent stage in India, there is a clear trend observed this year showing organizations taking baby steps towards Privacy. This is observed in the reduction in access of certain sensitive Permissions and reduction in 3rd parties with whom data is shared. Whether these steps have been ‘forced’ on entities given the change in policies of Google and Apple Play stores or whether in readiness for the upcoming India Personal Data Protection Bill or due to exposure to Global regulations like the GDPR is anybody’s guess, it is still a positive and heartening development. This leads us to conclude that an increase in awareness combined with regulatory and legal pushes would push adoption and maturity of privacy in India, that too rapidly and significantly.
Authors

Shivangi Nadkarni  
Co-Founder & CEO - Arrka

Sandeep Rao  
Principal Consultant - Arrka

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.
Empowering organizations to manage their Data Privacy and Information Security Programs

Pune Office:
44/1, First Floor, Namrata Apts.
Amar Housing Society, Gulmohar Path
Off Law College Road, Pune 411004

Mumbai Office:
201, 2nd Floor, Marathon Future IT Park Building
Mafatlal Chamber ‘A’, Mafatlal Mills Compound
N.M. Joshi Marg, Lower Parel, Mumbai 400 013

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

Arrka enables organizations to Assess, Design, Implement, Maintain and Manage their Data Privacy and Information Security Programs. Using a combination of the Arrka Intelligent Platform, Custom Toolkits, One-of-Its-kind Testing Lab, Learning Academy and Domain experts, we offer separate solutions for Large Enterprises and Small & Mid-Sized Businesses (SMBs) to address their unique challenges in these domains.

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.

©2019 Arrka Infosec Private Limited