Arrka

PRISM.IN 2023

Privacy Research & Insights Study of Mobile Apps and Websites. INDIA

An Annual Study by Arrka

7th Edition

Earlier known as
'State of Data Privacy of Indian Apps and Websites'

Contents

Foreword

2023 will go down in the history of Data Privacy in India as the Annus Mirabilis. The year when the Indian Digital Personal Data Protection Act (DPDPA) got passed, ushering in, in one stroke, almost ***one fifth of humanity*** under the purview of a Personal Data Protection Law.

With great power comes great responsibility. The DPDPA has bestowed great power in the hands of the individual - the Data Principal. This translates into great responsibility falling on the shoulders of all those entities with whom the Data Principal's Personal Data lies. This, in turn, warrants the kicking off of formal privacy programs in organizations, big and small.

At this crucial juncture in India's Data Privacy journey as a nation, it gives us all at Arrka great pleasure to bring out the seventh edition of our Annual State of Privacy report.

We have rechristened the report title this year, calling it the ***PRISM.IN*** - the 'Privacy Research & Insights Study of Mobile Apps and Websites. India'.

This year, we are also excited to launch an ***adjunct study**** to the main one: PRISM.IN - CHILDREN. This study does a ***special deep dive into Children's Privacy***, an area that is coming under increased focus worldwide with several regulations being passed for the protection of Children. The DPDPA has done India proud by bringing this focus under the ambit of the law from the word go.

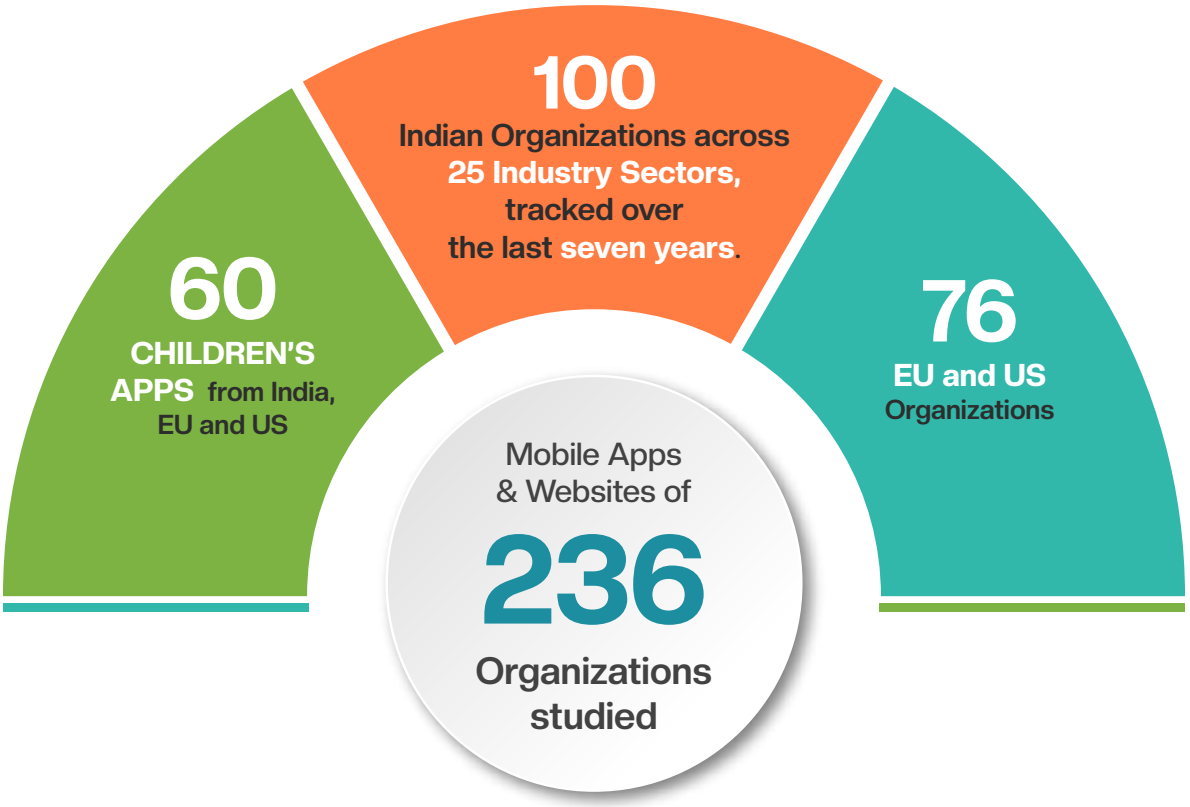
Every year, I sign off the foreword indicating how we have a long way to go as a country. I had hoped that with the passing of the law, this year would be a bit different. Alas, that is not to be... the journey ahead continues to look massive and onerous. However, anecdotal evidence suggest we have made a definitive start - the first step, at least, in the thousand miles ahead.

Shivangi Nadkarni
Co-Founder & CEO, Arrka

* The adjunct study is available at ***www.arrka.com***

Key Highlights

Who Did We Study?



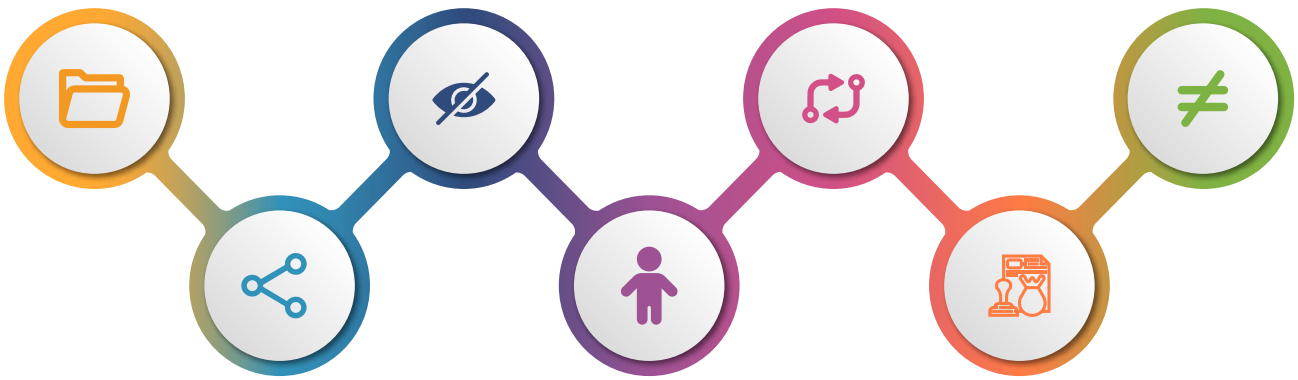
What Did We Study?

What Personal Data is *Collected*?

How *Transparent* are organizations with their users?

How do Indian Apps *Compare* with *Global Apps*?

Declarations by Apps on the PlayStore/ AppStore *vs* what they *really do*



How is Data *Shared* further?

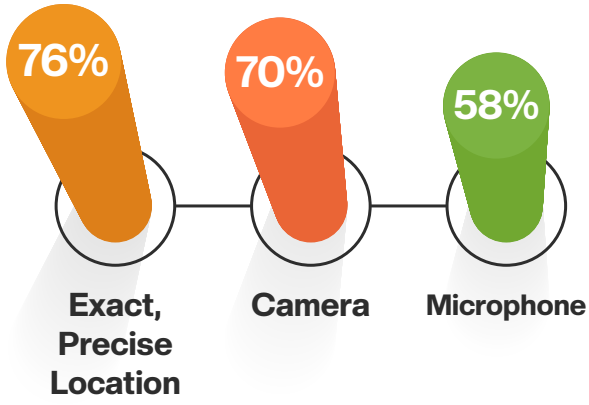
What are *Privacy Levels* in *Children's Apps*?

How Compliant are Indian Organizations with the *DPDPA*?

Interesting Factoids:

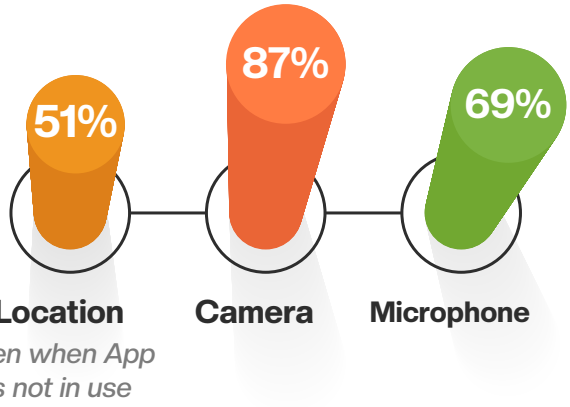
Top Dangerous Permissions taken by

ANDROID APPS



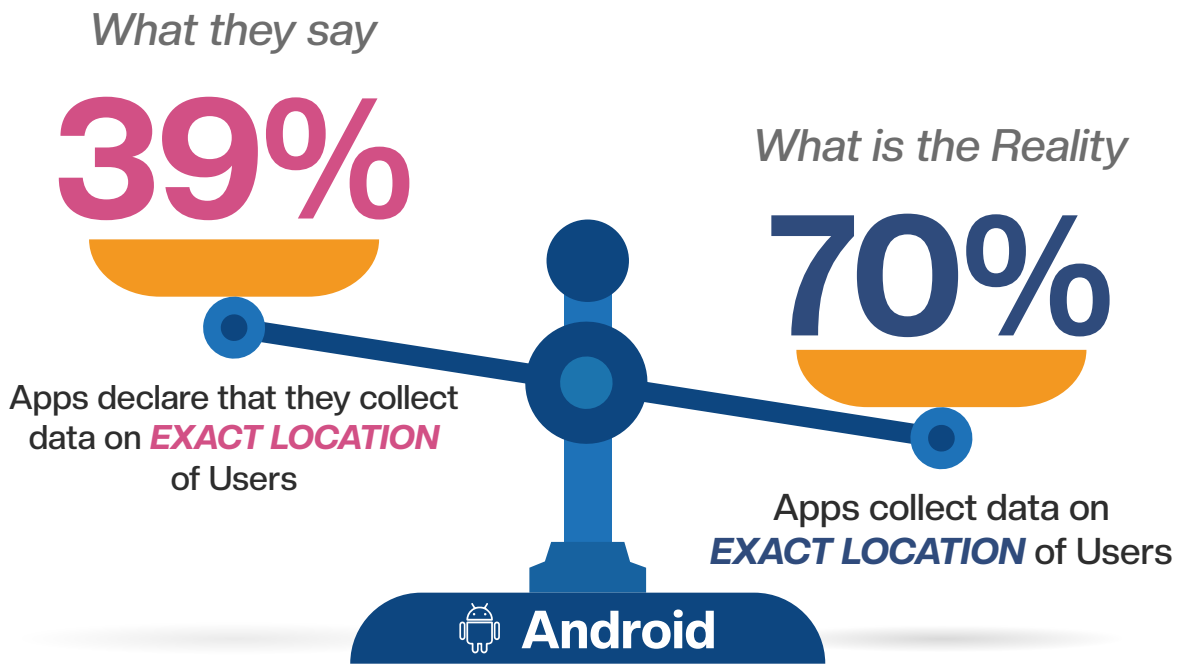
Top Dangerous Permissions taken by

iOS APPS



What is Claimed versus Reality

What Apps declare on the Google & Apple stores vs what what really happens inside the Apps can be different. What we see is **NOT** what we get.



What they say

8%

Apps declare that they collect data from ***MICROPHONE*** of Users.

What is the Reality

69%

Apps access data from ***MICROPHONE*** of Users

WEBSITES

18

Third Party Trackers
on a typical Indian website

87%

Indian Websites carried Adtech Trackers

30%

Reduction in 3rd Party Cookies over the previous year.

42%

Websites had Facebook Pixels which sent user data back to Facebook

52%

Websites profiled visitors and targeted them with advertising across other sites

6%

Websites captured your keystrokes

Google is the single largest 3rd party with whom data is being shared

- In Android Apps, **43%** of the identified trackers belong to Google while **37%** is the corresponding number for Websites

How Transparent are Organizations via their Privacy Notices:

31/100

This is the *Average Readability Score* of an Indian Organization's Notice - which is categorized as *'Difficult to Read'*.

This is *Half* of the acceptable ***International Readability Standard Score!***

Indian Children's Apps:

85% *accessed at least* ***One Dangerous Permission***

46% *accessed* ***Camera***

39% *contained* ***In-App Ads***

46% *accessed* ***Microphone***

23% *accessed* ***Exact Location***

How Do Indian Apps & Websites Compare with those in the US & EU?

Microphone Access

Indian Apps - 58%

EU - 29% US - 18%

SMS Access

Indian Apps - 34%

EU - 0% US - 0%

Contacts List Access

Indian Apps - 46%

EU - 13% US - 11%

3rd Party Trackers

Indian Apps - 18

EU - 9 US - 13

Privacy Notice Readability

India - 31 EU - 40

US - 34

The Arrka Privacy Index

Study Methodology & Approach

What did we Study?

Data Privacy is all about Personal Data – and how much of control an individual can 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.

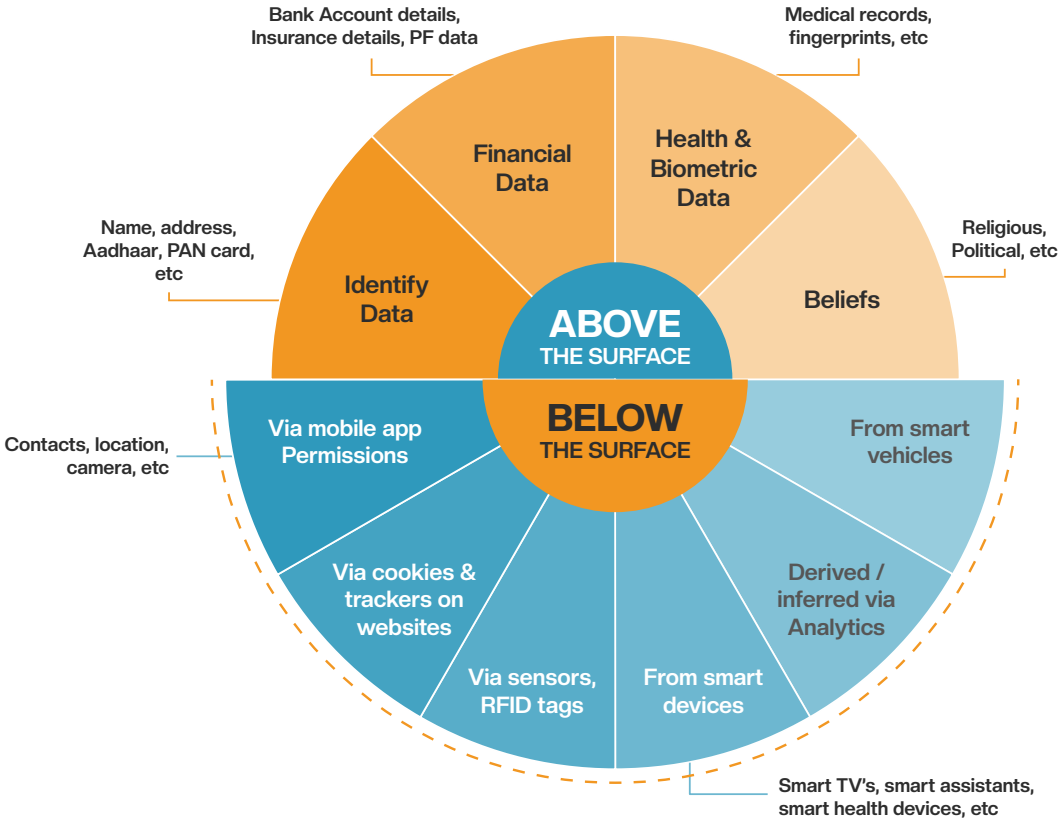
Our Study primarily focuses on:

'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?
- Are Apps declaring Accurately about all the Data they are collecting?
- 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?
- What is going on with Children's Apps?
- How Indian Digital Properties compare with those in the US & EU?
- How compliant are Indian Apps & Websites with the DPDPA*?

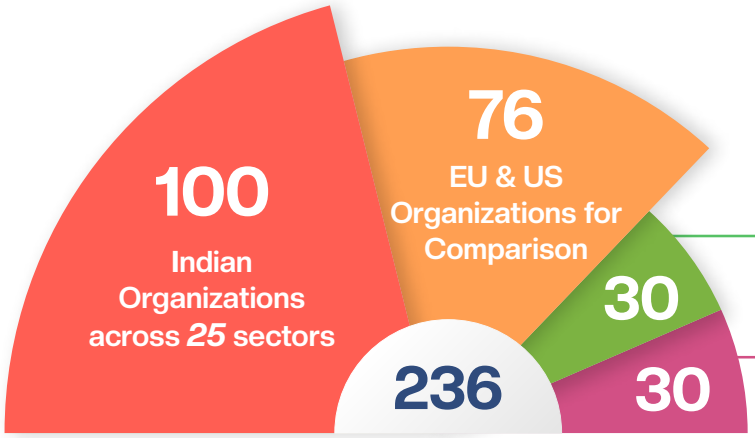
*The Indian Digital Personal Data Protection Act, 2023

Personal Data



Who did we Study?

Overall 236 organizations and their 3 Digital properties (Android Apps, iOS Apps & Websites) were covered as part of the Study.

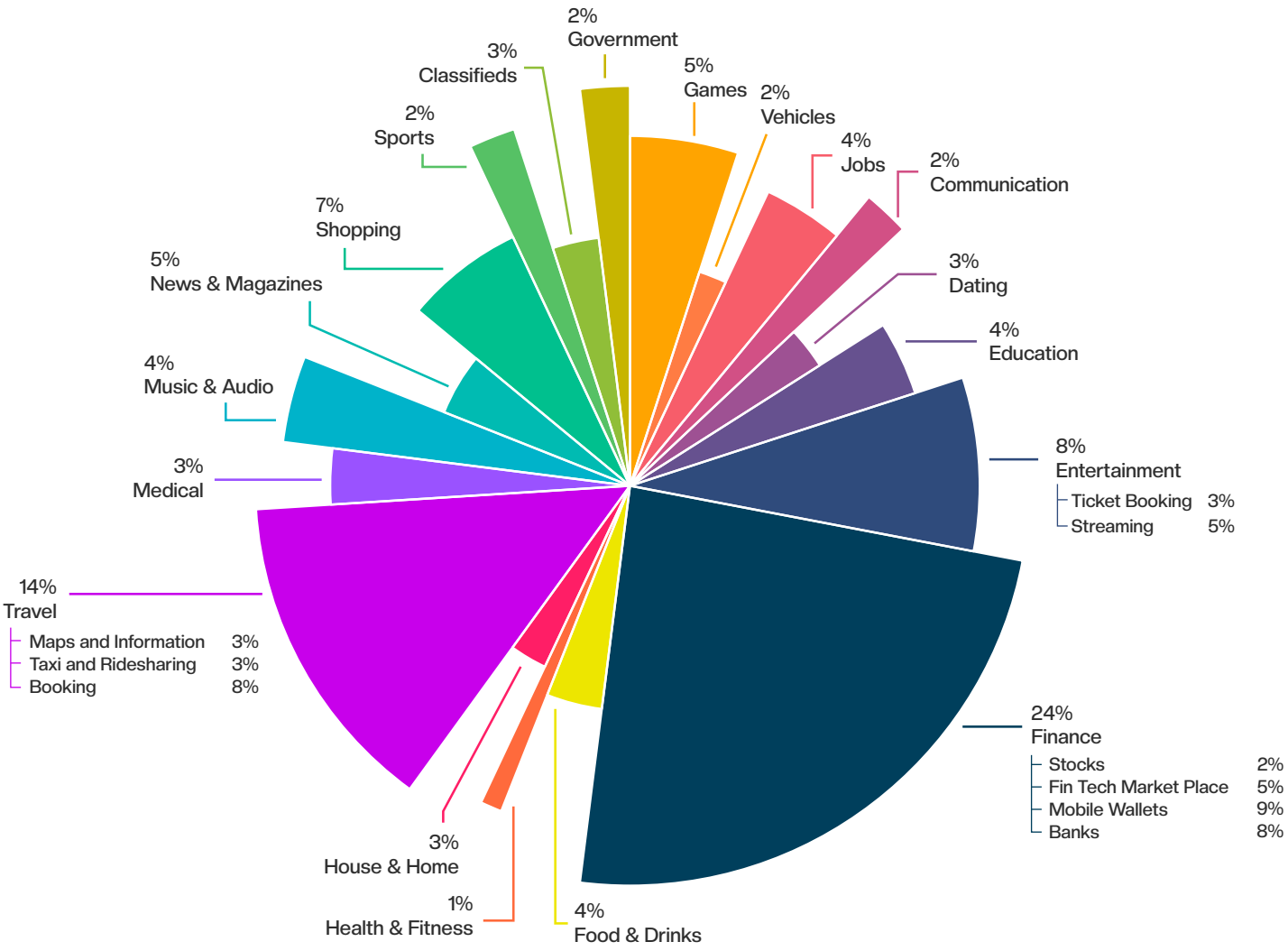


30 Indian Children's Apps

30 EU & US Children's Apps - *for comparison*

Digital Properties Studied

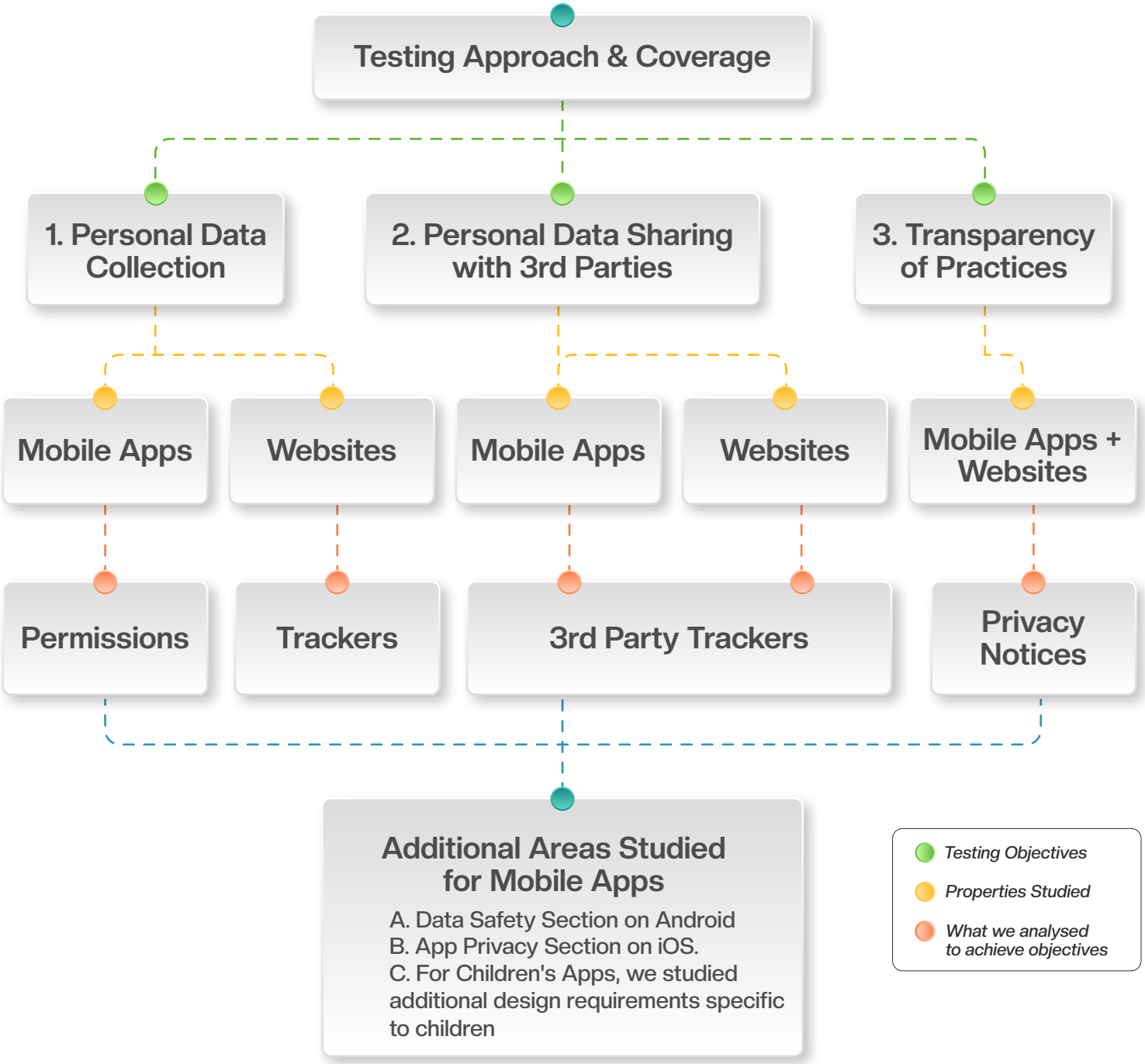
- Android
- iOS
- Website



Indian Organizations

How did we conduct this Study?

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



Note:
The Data about App Permissions and Trackers is from testing done at the Arrka Privacy Lab as well as from External Sources like Exodus Privacy. Analysis of Privacy Notices is done at the Arrka Privacy Lab. Data pertaining to Websites is from External Sources like Blacklight (The Markup) and PrivacyScore.org

Key Findings

What Personal Data is Collected & How?

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 Accessed
ANDROID

- 76% Camera
- 70% Exact Location
- 58% Microphone
- 46% Contacts
- 34% SMS

Top Permissions Accessed
iOS

- 87% Camera
- 87% Location *(When App is in use)*
- 86% Photos
- 69% Microphone
- 51% *Location (When App is not in use)*
- 49% Contacts
- 41% Calendar

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 – We reviewed permissions for iOS Apps, some of which are common with Android (e.g.: Contacts, Camera) while some are different. Moreover, certain permissions (i.e. Location) 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.

Personal Data Collection: What is Claimed by Apps versus Reality?

PlayStore / AppStore Declarations as per Android and iOS Policies

(to help users better understand an App's privacy practices *before* they download the App)

What App Developers need to Declare?

- **Personal Data Collected** (and if linked to users or used to track them)
- **Personal Data Shared** (and if linked to users or used to track them)
- **Purpose of Processing**

When do they need to Declare?

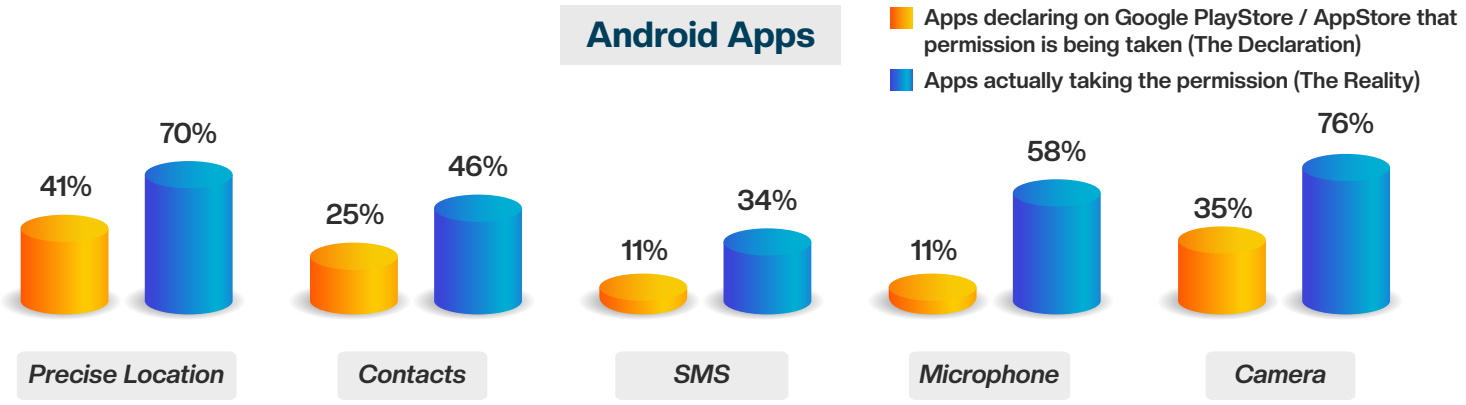
When they submit new apps or app updates to the App Store

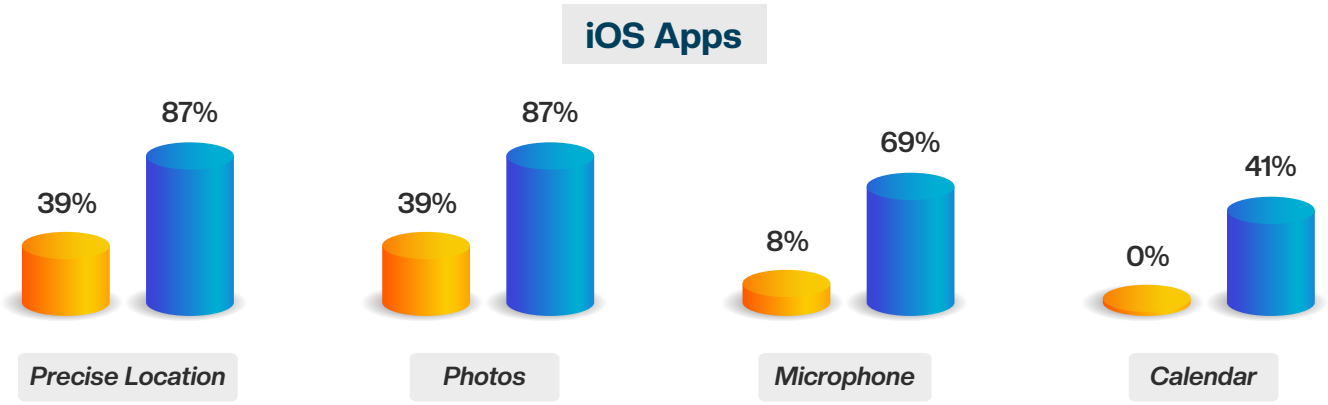
Where are the Details Published?

On the PlayStore / AppStore's Product Page

The reality on the ground:

We found that Apps are declaring one thing while doing something else in reality. The discrepancy in declared data vs actual data as below showcases this





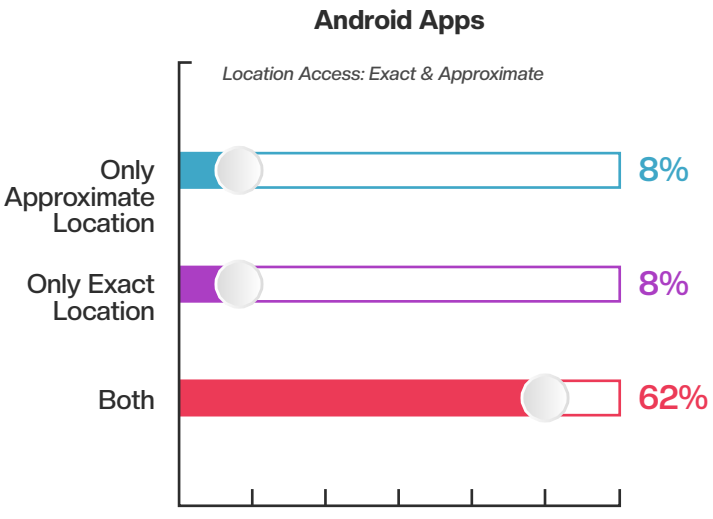
A.2: Top Categories that access Maximum Number of Dangerous Permissions

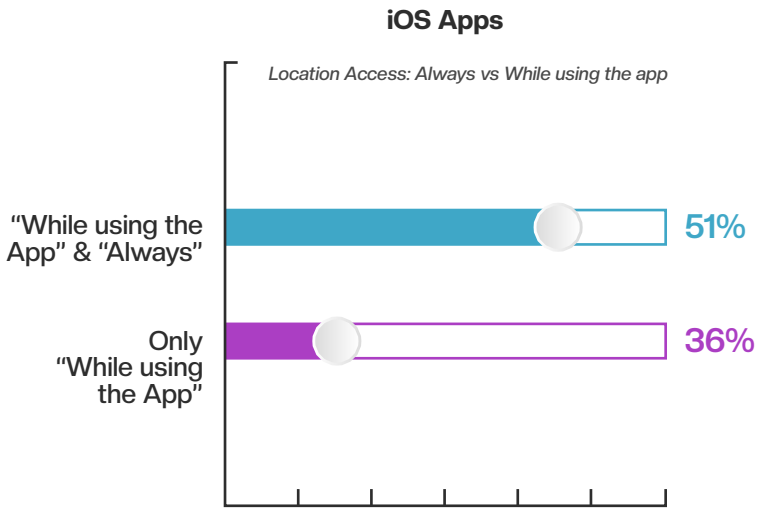
Android	No. of Permissions
Mobile Wallets	14
Health & Fitness *	14
Classifieds	12
Communication	12
Banks	11
Travel - Taxi & Ridesharing	11
Food & Drinks *	11

iOS	No. of Permissions
Health and Fitness	12
Communication	9
Banks *	8
Entertainment (Ticket Booking)	7
Mobile Wallets	7
Music and Audio	7
House and Home	7
Taxi & Ridesharing *	7

** New categories that have found their way into this list in 2023*

A.3: The Curious Case of Location Permissions



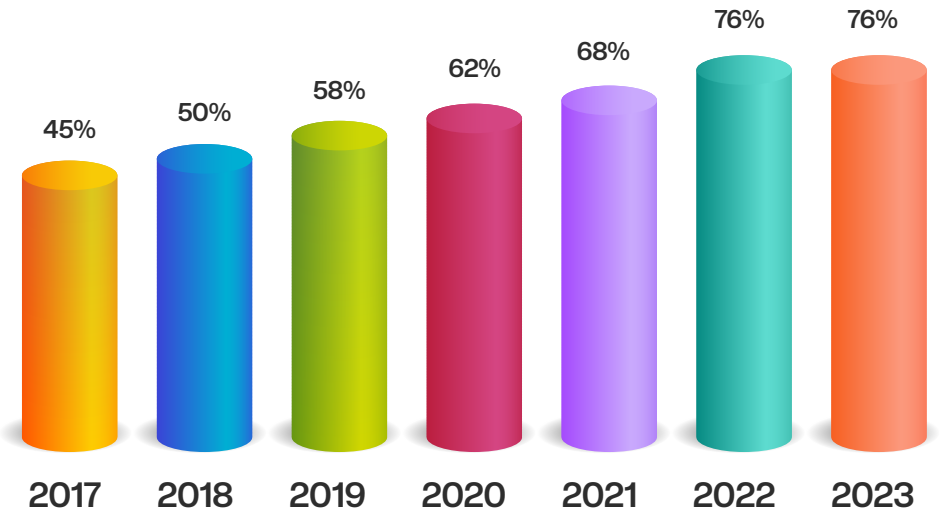


- Organizations are not specific about the Granularity of Location data that they want to access

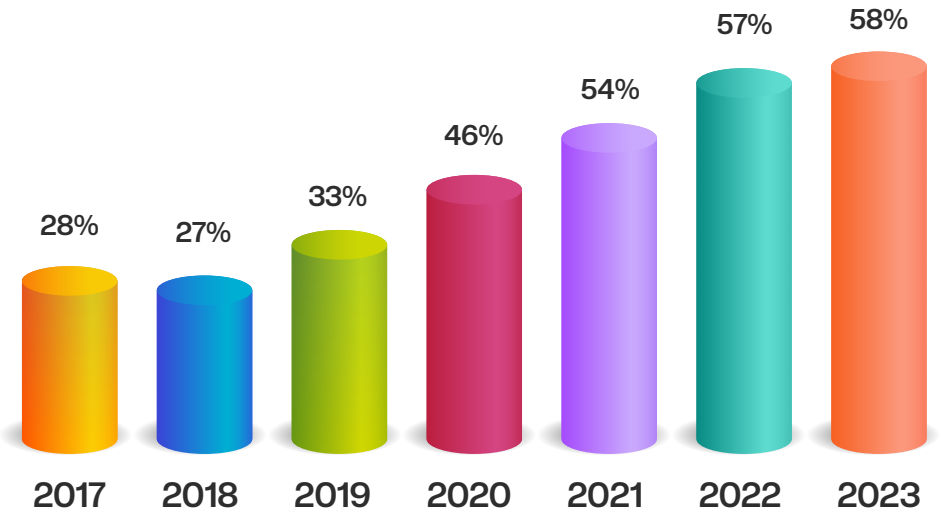
A.3: Year-on-Year Trends

Given this is the 7th edition of this study, we have done some trend analysis to see how Privacy in India has been evolving. We have been studying the same set of 100 organizations for the last 7 years.

A.3.1. Android Apps - Access to Camera and Microphone is stabilizing



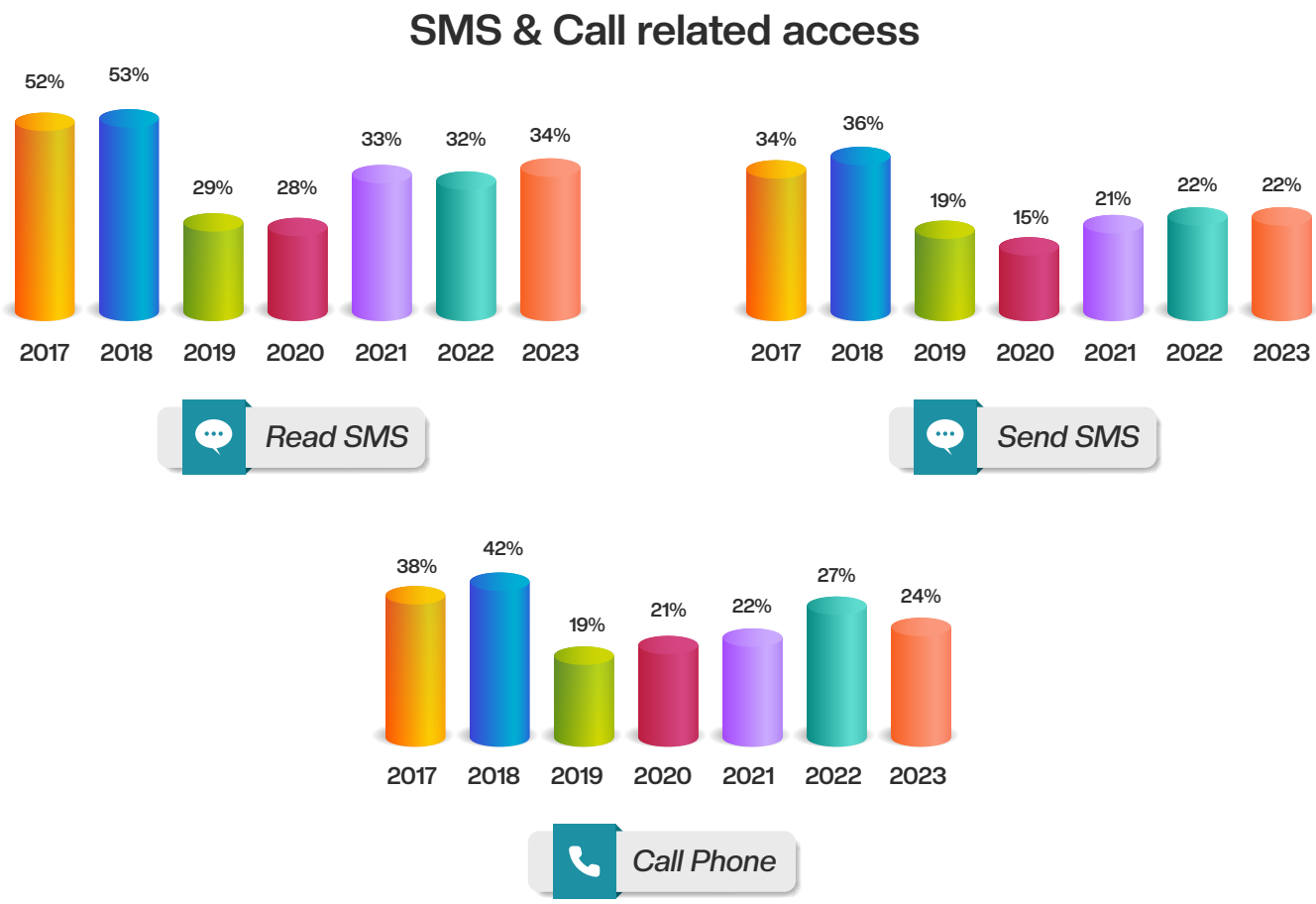
Apps Accessing Camera



Apps Accessing Microphone

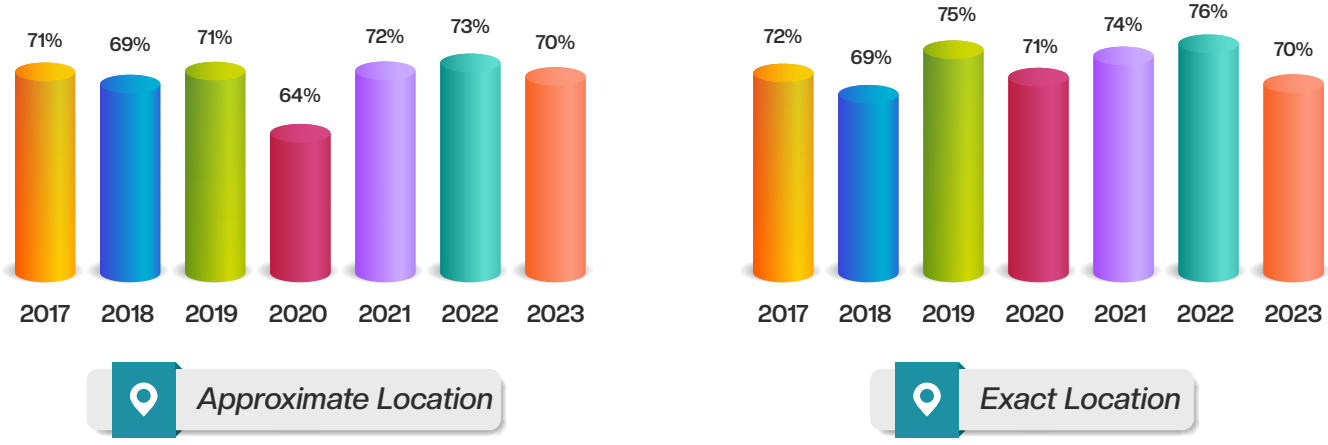
It is heartening to note that the trend of increasing access to Camera and Microphone Permissions is stabilizing

A.3.2. Android Apps - Access to SMS and Call related Permissions remains stable

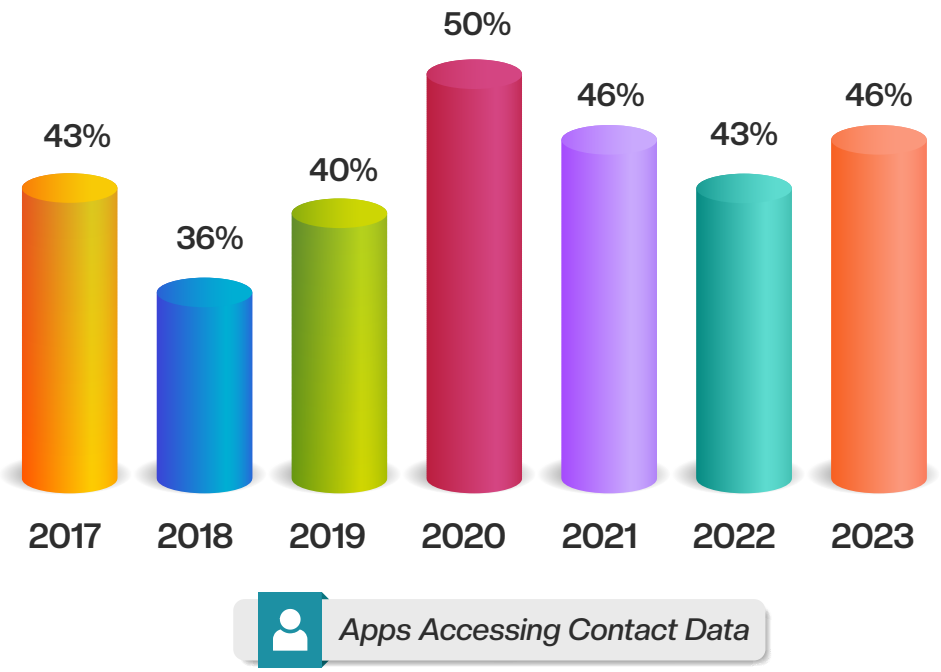


A.3.3. Android Apps: Access to Location has reduced

- The Access to Location has ***reduced*** from 2022.
- This reduction is greater in Apps accessing ***Exact Location (8% reduction)*** as compared to those accessing ***Approximate Location (4% reduction)***.



A.3.4. Android Apps - Increase in access to Contact Data:



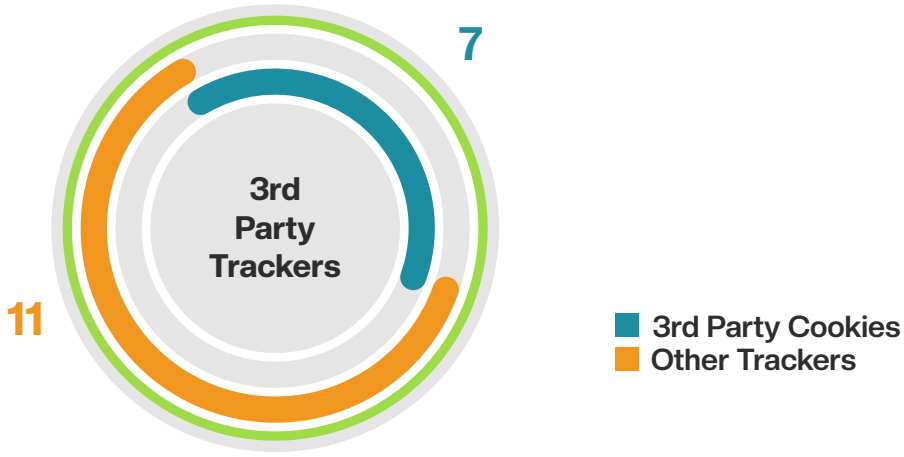
There is an ***increase in access*** to Contact data although this is still lower than the highs observed in 2020.

B. Websites

The Website Tracker Landscape

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

B.1: 3rd Party Trackers



Key Findings

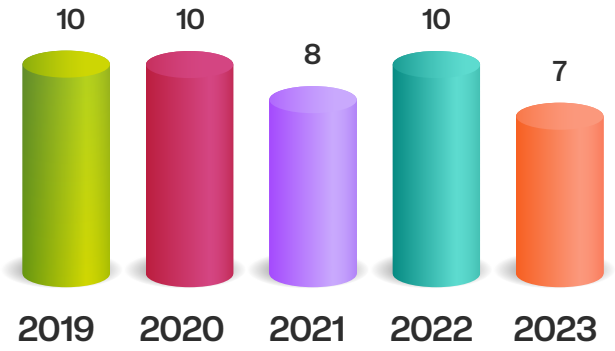
- **18** - The average Number of 3rd Party Trackers Embedded per Website.
- **12** of the 3rd Party Trackers are known* Advertisers

Top Categories embedding 3rd Party Trackers

Categories embedding the maximum trackers are:

News and Magazines **(60)** Vehicles **(46)** Health & Fitness **(28)**

B.2: 3rd Party Cookies



Third Party Cookies

Key Findings

- **7** – Avg. number of Third Party Cookies.
- We have observed a **30% decrease** in the number of Third Party Cookies over 2022.

* 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).

Some Additional Website Stats

42% **Facebook Pixels**

Websites had **FACEBOOK PIXELS** which ***send data about website visitors back to Facebook.***

52% **Google Analytics**

Websites had the Google Analytics "Remarketing Audiences" feature. This feature allows a website to profile website visitors and then ***follow them across the internet and target them with advertising on other sites.***

87% **Adtech Companies**

Websites had **Ad Trackers.**

9% **Session Recording**

Websites recorded your sessions tracking activities like mouse clicks, scrolls, etc.

12% **3rd Party Cookie Blockers**

Websites load trackers that are designed to **evade third party cookie blockers**

6% **Key Stroke Logging**

Websites captured user **Key Strokes**

Note:
Statistics on this page have been extracted from Blacklight

Are Apps & Websites 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:

Permissions accessed by MOST Apps (>85%) in the category

Permissions accessed by SOME Apps (30-85%) in the category

Permissions accessed by FEW Apps (<30%) in the category

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. Sector - Travel Booking

MOST Apps access

ANDROID

- Read & Write to External Storage
- Location (Approximate & Exact)

iOS

- Location Services - "While using the App"
- Location Services - Always
- Photos
- Camera

SOME Apps access

ANDROID

- Camera
- Read Phone State
- Read & Receive SMS
- Read Contacts
- Microphone
- Call Phone
- Access to Acconts on Device

iOS

- Contacts
- Microphone

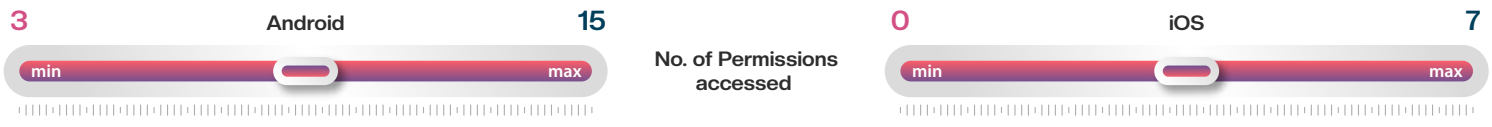
FEW Apps access

ANDROID

- Access Background Location
- Read Calendar
- Send SMS
- Write Calendar
- Write Contacts
- Manage Accounts
- Read Phone Numbers
- Request Install Packages
- Write Settings
- System Alert Window

iOS

- Calendars
- Motion



2. Sector - Banks

>85%

ANDROID

- Approximate & Exact Location
- Camera
- Send SMS
- Microphone
- Write External Storage
- Read Phone State

iOS

- Camera
- Contacts
- Photos
- Microphone
- Location Services - "While using the App"

30% - 85%

ANDROID

- Read External Storage
- Read and Receive SMS
- Access to Accounts on Device
- Read Contacts

iOS

- Location Services - "Always"
- Calendars
- Bluetooth
- Motion
- Siri

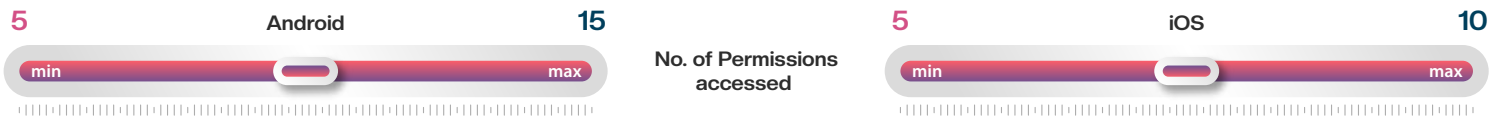
>30%

ANDROID

- Call Phone
- Write Contacts
- Read & Write Calendar
- Read Phone Numbers

iOS

- Reminders
- Apple Music



3. Entertainment - Streaming

>85%

ANDROID

- Read & Write External Storage

iOS

- Camera

30% - 85%

ANDROID

- Approximate & Exact Location
- Camera
- Microphone
- Read Phone State

iOS

- Bluetooth
- Microphone
- Photos

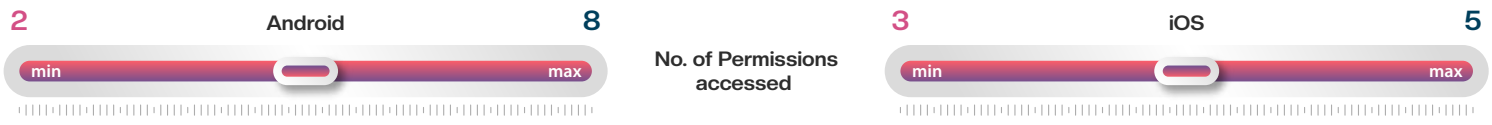
>30%

ANDROID

- Call Phone
- Read and Receive SMS
- Get Accounts
- Read Contacts

iOS

- Calendar
- Location Services - Always
- Location Services - "While using the App"



4. News & Magazines

>85%

ANDROID

—

iOS

- Location Services - "While using the App"

30% - 85%

ANDROID

- Read and Write External Storage
- Camera
- Microphone
- Read Phone State

iOS

- Location Services - Always
- Photos
- Calendars
- Microphone
- Camera

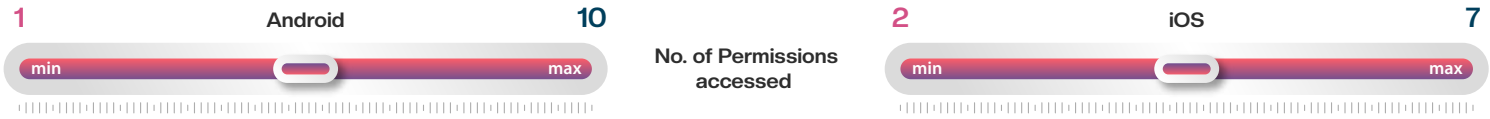
>30%

ANDROID

- Approximate & Exact Location
- Read and Write Calendar
- Read Contacts
- Access to Accounts on Device
- Call Phone

iOS

- Apple Music
- Bluetooth
- Contacts



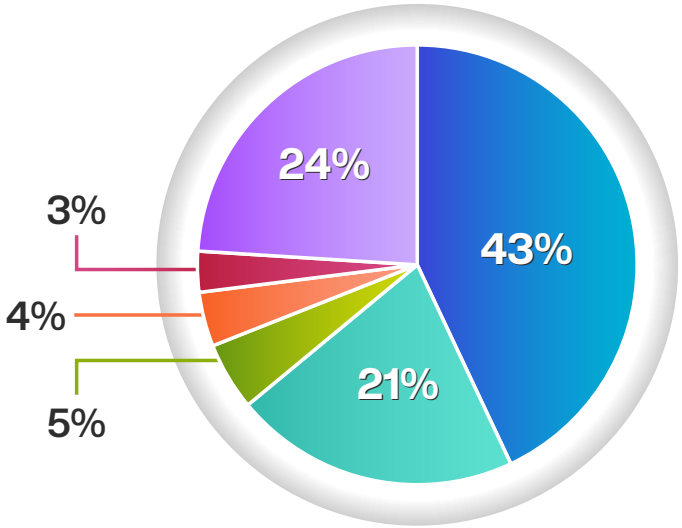
Whom is your Personal Data shared with?

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 (43%) is the leading recipient of your data with Facebook (21%) 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, Moat



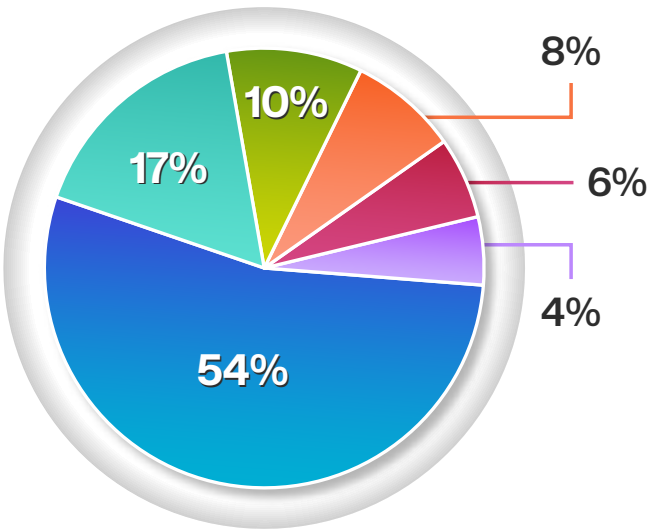
Proportion of 3rd parties

Google, Facebook, AppsFlyer, Clevertap, Branch, Others

NOTE: The term Google covers all properties of Google.

A.2 Which functional categories do the entities belong to?

- 71% of 3rd Parties are related to Advertising & Analytics .



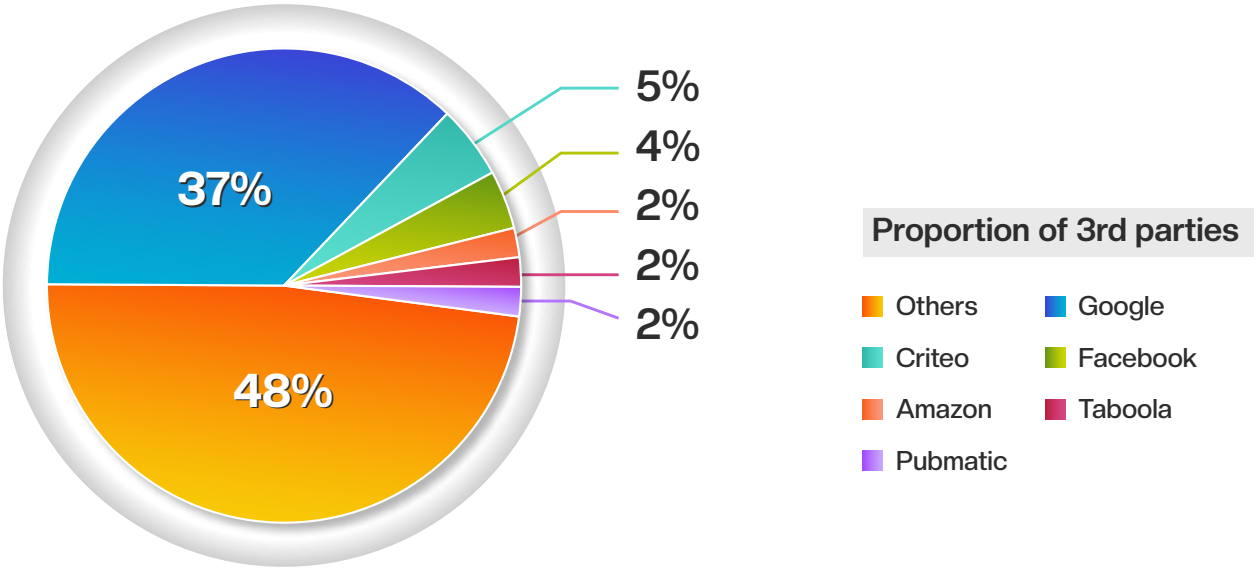
Categories of Trackers

Analytics, Advertising, Identification, Crash Reporting, Profiling, Location

B. Websites

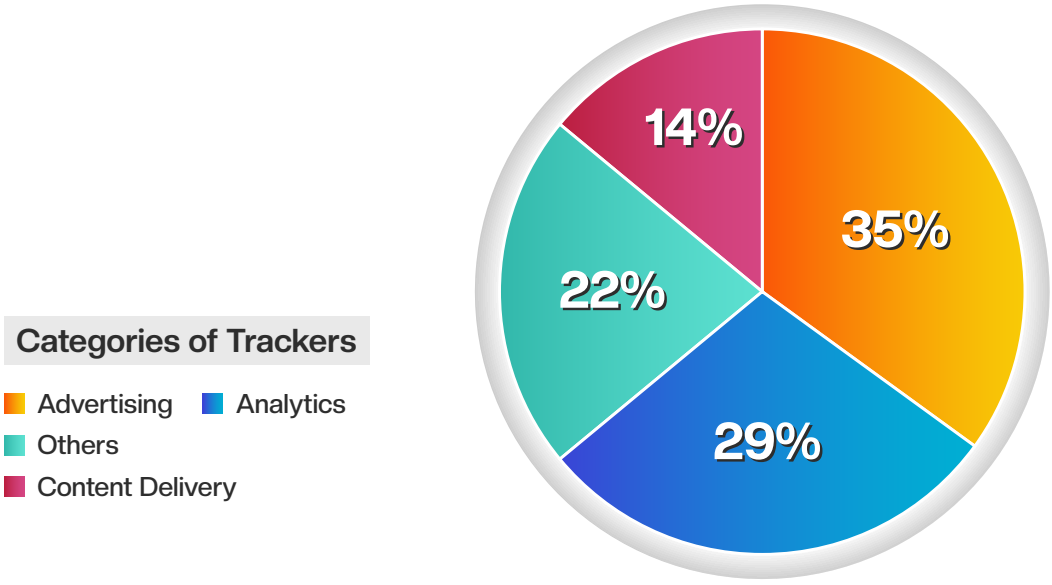
B.1 Which entities are your data's Top Recipients?

- Google (37%) is the leading recipient of your data with Criteo (5%) 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., Yahoo, Cloudflare, Adobe
- 59% of Websites use Google Analytics.
- 87% had trackers from Adtech Companies.



B.2 Which functional categories do the entities belong to?

- 51% of Trackers are related to Advertising and Analytics.



Note: Data on 3rd Parties for websites was extracted from PrivacyScore.org and Blacklight.
* The "Others" category comprises a Long tail of smaller organizations who could not be classified. They may most likely fall into the Advertising / Analytics categories. 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.

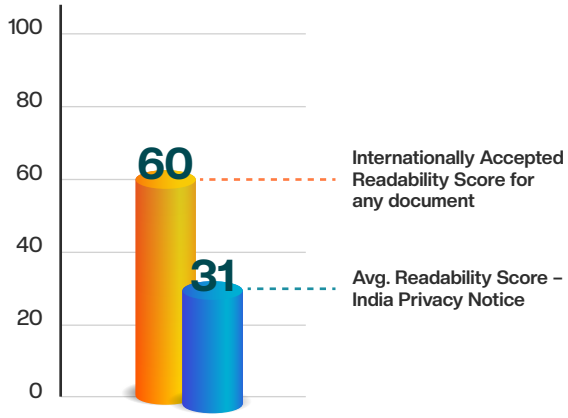
To analyze Notice Readability, we used the Industry Standard **"Flesch Reading Ease Scale"**. The Flesch Reading Ease scores are being used as a standard readability formula by many US Government Agencies.

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

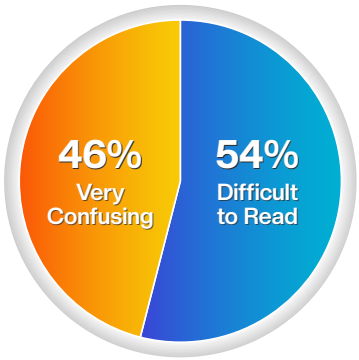
Key Findings

- 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
- **46%** of Privacy Notices are at **"Very Confusing"** score level.

Readability Score



Readability Scores of Privacy Notices of Indian Organizations



Categories with the lowest Notice Readability Scores are

- Sports **(26)**
- Fintech Market Place **(26)**
- Mobile Wallets **(26)**

Special Focus Area: Children's Privacy

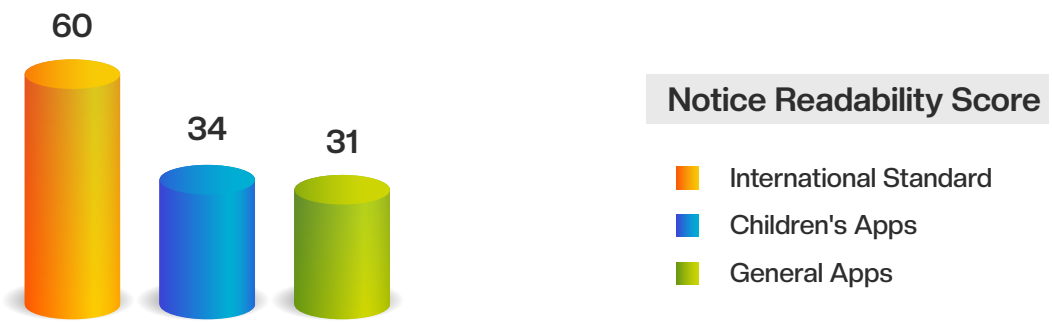
Children are a particularly vulnerable category. Hence, one area we specifically studied over and above the 100 base Apps were Android Apps from India targeting children. Along with studying Personal Data Access, we also reviewed aspects specific to Children's Apps.

- **73%** had access to Files on Storage
- **46%** have access to your Microphone
- **46%** have access to your Camera
- **38%** have access to your Phone Details
- **27%** can read your Contacts
- **23%** have access to your Exact Location
- **15%** had access to your Calendar

85% apps accessed at least one ***Dangerous Permissions***

Although the Notice Readability Score for Children's Apps is 10% higher than General Apps*, it is still way below International Standard

Notice Readability: Comparison with General Apps



* General Apps refers to the 100 Apps covered as part of this Study.

39% Apps served In-App ads

The India DPDPA prohibits Targeted Advertising to Children.

Apps provided In-App purchase **52%**

41% Apps had a separate Privacy Policy for Children

Apps had a dedicated section for Parents **38%**

52% Apps ask users to sign up using their Social Media Accounts

Apps collect the Users Date of Birth **35%**

13% Apps restrict access to users below the age of 13

*Check out our supplementary deep dive report on Children's Apps, providing additional intriguing statistics and analysis. Visit **www.arrka.com** for more details.*

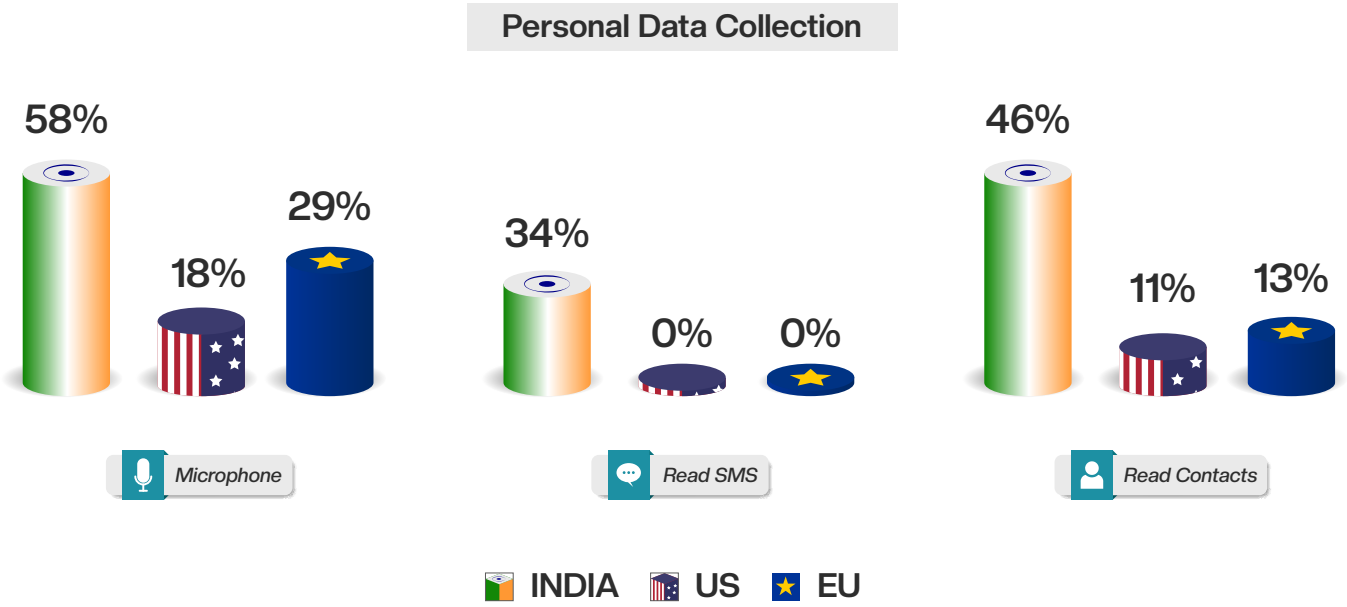
Indian Organizations in comparison with EU & US Organizations

To understand, how Indian Organisations stack up in comparison to US and EU Organisations in terms of Personal Data accessed, we studied **38 EU** and **38 US** Organisations to study the patterns. There is a significant difference in certain types of Personal Data accessed.

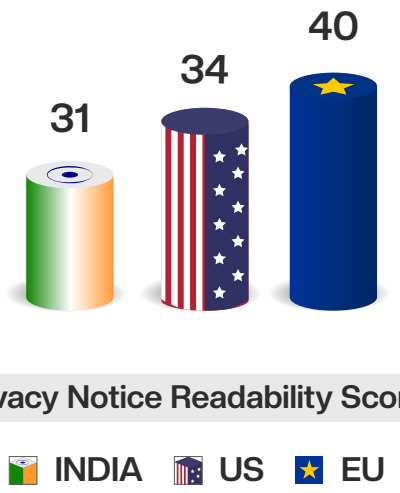
A. Android Apps

Our study finding indicates that significantly higher number of Indian Apps request access to specific permissions as compared to their Global counterparts.

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



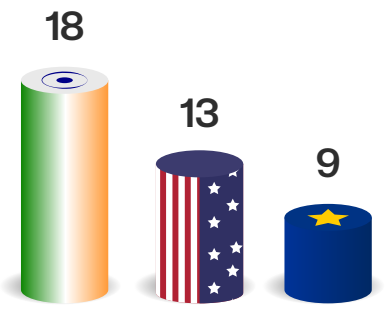
Privacy Notice Readability scores are clearly better in the **EU - 29% higher** than India.



B: Websites

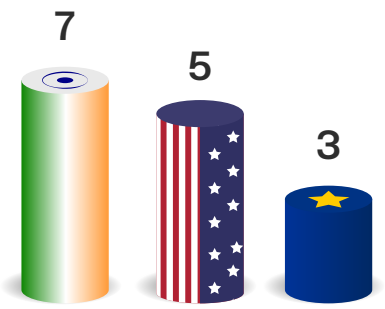
- Significantly higher Trackers deployed by Indian Websites as compared to US and EU websites.
- The number of Trackers in US Websites have seen a steady decline over the past 4 years.
- We also observed a significantly higher use of Google Analytics by Indian Websites as compared to US and EU Websites. **However, this Gap is closing.**

3rd Party Trackers Embedded



No. of 3rd Parties embedded

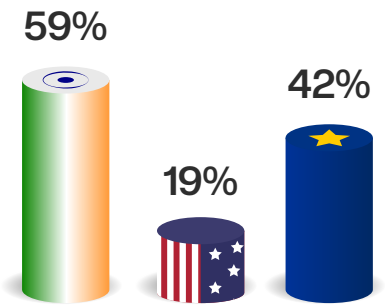
3rd Party Cookies



No. of 3rd Party Cookies

INDIA US EU

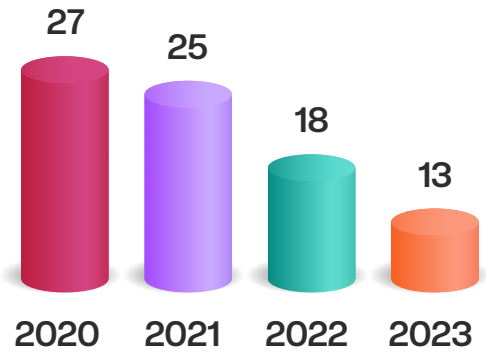
Use of Google Analytics



Google analytics used (%)

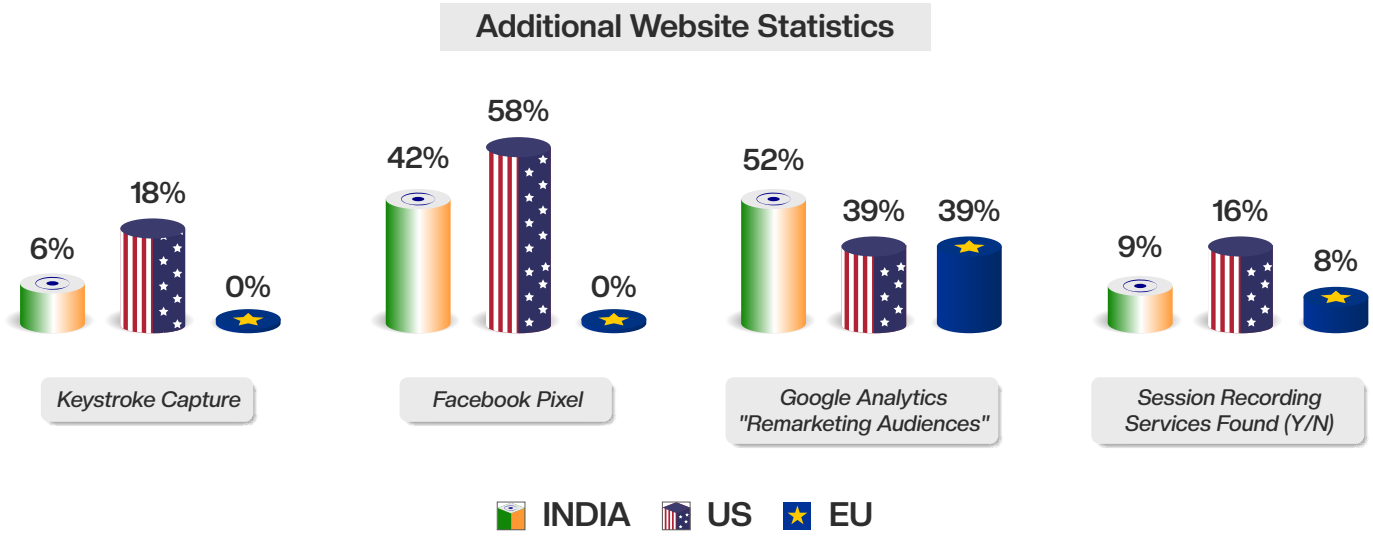
INDIA US EU

US Websites 3rd Party Trackers embedded trend



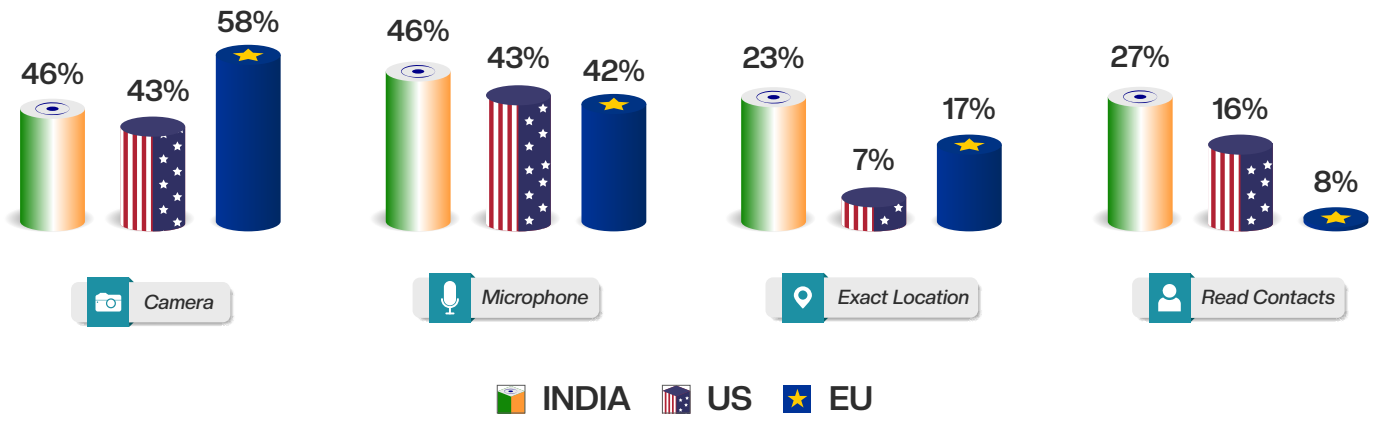
3rd Party Trackers Embedded

This year we studied some additional data points for Websites to understand user tracking. Our study finding indicates that the **US Websites do the most tracking** as compared to the EU and India across most parameters. Websites in EU are very strict compared to the US and India in terms of User Tracking. **No EU Websites** were found capturing User Keystrokes or embed Facebook Pixels (to inform Facebook if the user visited the website). **Significantly higher Indian websites** deploy the Google Analytics-Remarketing Audience feature which lets Google Analytics track users across the internet.

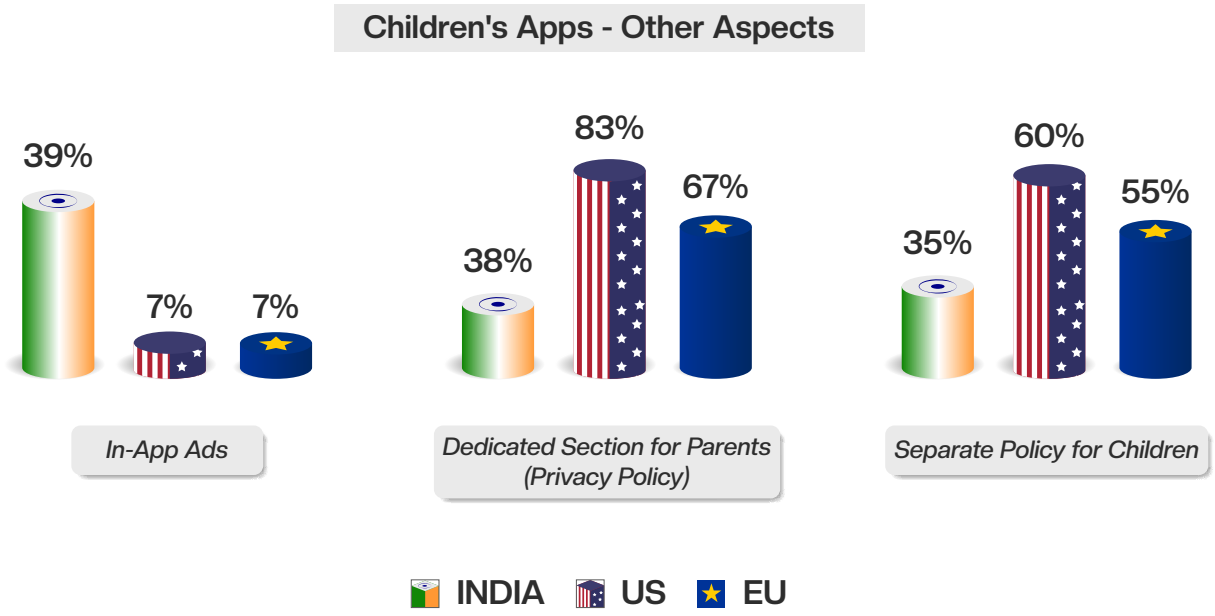


C: Children's Apps (Android)

To understand, how Children's Apps from India stack up in comparison to Children's Apps from the US and EU in terms of Personal Data accessed, we studied 15 EU and 15 US Apps to study the patterns. Our study finding indicates that like The General Category of Apps, there are some specific permissions which are accessed by a higher number of Indian Apps as compared to EU and US. However, there are other permissions where the access by the Indian Apps are either comparable or even lower than the EU and US Apps.



We also compared other aspects related to Children's Privacy. Some findings are:
The Children's Apps in India also have **significantly higher In-App Ads** as compared to their Global Counterparts.
Indian Apps also **lag behind** their Global Counterparts in terms of **Transparency**.



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

Note: In this Study, we publish an abridged version of the Privacy Index in which we use a subset of **15 parameters** covering areas like Personal Data Collection, Sharing and Transparency Practices.

Privacy Index by Category

#	Category	Privacy Index	
1	Government	68%	↑
2	Games	56%	↔
3	Classifieds	55%	↑
4	Communication	54%	↑
5	Sports	53%	↓
6	Jobs	52%	↑
7	Education	51%	↓
8	Travel - Maps & Information	51%	↑
9	Finance - Stocks	51%	↑
10	House & Homes	49%	↑
11	Food & Drinks	48%	↑
12	Medical	48%	↓
13	Music & Audio	48%	↑
14	Health & Fitness	47%	↑
15	Entertainment - Streaming	47%	↓
16	Vehicles	45%	↓
17	Finance - Fintech Marketplace	45%	↓
18	Entertainment - Ticket Booking	45%	↑
19	News & Magazines	44%	↓
20	Travel - Booking	44%	↑
21	Finance - Banks	44%	↓
22	Finance - Mobile Wallets	40%	↓
23	Shopping	40%	↓
24	Dating	40%	↓
25	Travel - Taxi & Ridesharing	39%	↔

Movement in rank from 2022 to 2023

- Upward Movement ↑
- Downward Movement ↓
- No Movement ↔

Note: In this Study, we publish an abridged version of the Privacy Index in which we use a subset of **15 parameters** covering areas like Personal Data Collection, Sharing and Transparency Practices.

Compliance to the India DPDPA

#	India DPDPA 2023 Requirements	Score
1	A Privacy Notice is presented to individuals at the time of Data Collection	
2	The Privacy Notice provides information to individuals about the Organization's Personal Data processing practices	
3	The Privacy Notice is clear, concise and easily comprehensible to a lay individual	
4	The Privacy Notice is presented in multiple languages where necessary	
5	**Collection Limitation:** Only adequate, relevant Personal Data that is necessary for the agreed purposes of Processing is being collected	
6	**Children's Data:** Targeted Advertising to children is not being carried out by the Organization	

Authors

Shivangi Nadkarni

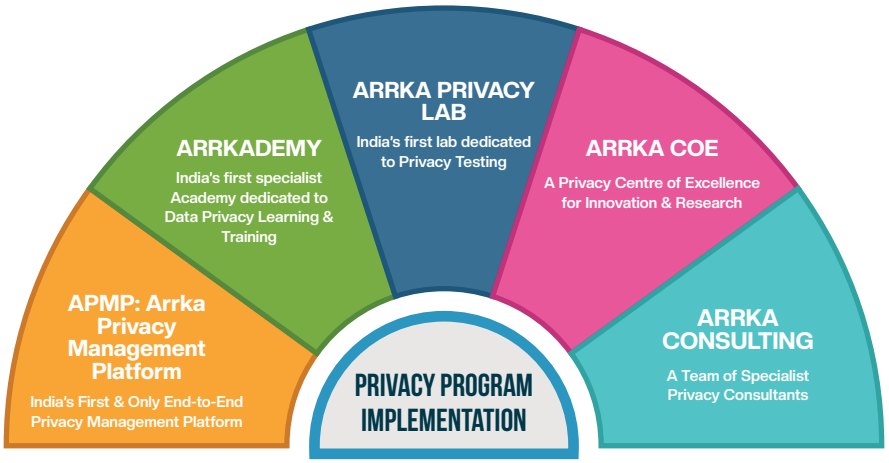
Co-Founder & CEO
- Arrka

Sandeep Rao

Chief Product Officer
- Arrka

All the testing for this study was carried out at the Arrka Privacy Lab; India's first Lab dedicated to Privacy Testing.

Arrka: The Privacy Implementation Specialist



APMP: Arrka Privacy Management Platform

APMP equips you manage your Privacy Compliance through the entire Program Lifecycle.

Whether you have to comply with **ONE law** or standard or **MULTIPLE laws**, it is all available out-of-the-box in an integrated manner.

The Arrka Platform empowers you no matter which stage of your privacy compliance journey you are on: **Yet-to-start, Mid-way** or **All-done**

ARRKA Privacy Centre of Excellence (COE)

The COE has developed the following frameworks that Arrka deploys to equip organizations to implement & manage their Privacy Programs.

APIF

The Arrka Privacy Implementation Framework or APIF enables an organization to deploy a comprehensible, adaptable privacy program which can integrate multiple laws and regulations.

APPF

The Arrka Privacy Product Framework or APPF is specially designed for Products or Applications. It helps integrate Privacy features and functionalities into Product Design that are Privacy Law Agnostic

P-SMB

After having done over 200 Privacy Program Implementations over the last decade, we at Arrka understand that the requirements of a Small Business is dramatically different from that of a large enterprise. Hence we built the P-SMB or Privacy for SMBs – a framework specially designed for Small Businesses to implement Privacy.

PDAM

Personal Data Attribute Mapping or PDAM is Arrka's methodology for building the foundation of a Privacy Program in an organization. Honed over a decade of implementing Privacy, PDAM is a structured foundational step that gives an organizational a quick overview of what is going on with its Personal Data – based on which its Privacy Program can get started.

ARRKADEMY

Arrkademy caters to the Data Privacy Learning & Training requirements across the spectrum: From Specialist Practitioners to End-Users

For Accredited Privacy Courses, we are Official Training Partners of iapp DSCI

The *International Academy for Digital Governance*:

For end-users & privacy champions in organizations and for self-learning, online Privacy Courses, we have partnered with Global Talent Track (GTT) to set up IADG.

IADG combines Arrka's Privacy expertise and GTT's two-decades old training expertise to bring the best to our participants

ARRKA LAB

Arrka Lab does Privacy Testing. Not to be confused with Security Testing like VAPT, Privacy Testing tests for Cookies & Trackers embedded in your website, Dangerous & High Risk Permissions that your Mobile App takes and the legitimate, non-malicious SDKs embedded in your App.

Critical from a Data Privacy perspective, Privacy Testing helps you get and remain compliant with Privacy laws as well as the privacy policies of the Android PlayStore / iOS AppStore.

ARRKA Consulting

To help an organization navigate through its Privacy Challenges, Arrka's team of Privacy Consultants & Subject Matter Experts work closely with the organization's Privacy Team and other stakeholders, equipping and empowering them to implement, manage and sustain their privacy programs.

Head Office:
Level 8, Platinum Towers, 1, Naylor Road, Off Mangaldas Road, Pune 411001.

www.arrka.com
privacy@arrka.com
@arrka2
www.linkedin.com/company/Arrka