End Semester Report - A/Y 2023-24 Sem I
The Impact of Device Cost on Data Privacy in Smartphones

Shyam N V - 2020A7PA2081H
Course Code: CS F366 under Dr. Dipanjan Chakraborty

December 23, 2023

Abstract

In today's tech world, we've got a pretty clear division between two kinds of gadgets: budget-friendly and high-end, wallet-wincing options.This study dives headfirst into the money-vs-privacy puzzle, trying to figure out what's happening.

Now, you've probably heard that low-cost gadgets are all the rage because, well, they're easy on the wallet. But here's the twist: these cheapo devices might have a secret deal going on. In exchange for their pocket-friendly price tags, they're quietly collecting your data in the background. It's like a behind-the-scenes data trade that helps pay the bills and keeps the prices low.

Conversely, those fancy, high-end gadgets with eye-watering price tags offer something different—privacy on steroids. They're all about protecting your personal stuff and going the extra mile to do it. That's part of why they cost so much—you're investing in your own digital fortress.

Our research isn't just guesswork; we've dug deep into written stuff and talked to folks face-to-face to back it all up. We're trying to understand why low-cost and high-end gadgets are priced the way they are.

Ultimately, our study isn't just about gadgets; it's about understanding how your cash, your privacy, and your choices all come together in the ever-changing world of tech.

Contents

Chapter 1

Introduction

1.1 Background

The consumer electronics market is a dynamic and ever-evolving space, offering a wide array of devices tailored to diverse consumer needs. In recent times, a clear division has emerged, separating budget-friendly devices known for their affordability from premium-tier counterparts celebrated for their elevated price tags. This sharp distinction characterizes the modern consumer electronics landscape.

Low-cost devices have found their place in the market by offering cost-effective options, often praised for their affordability. However, beneath their attractive price points lies a more intricate reality – the discreet collection of user data. These devices, while providing upfront savings, may engage in data collection practices that serve as an indirect revenue source, offsetting their production costs.

Conversely, high-end devices, recognised for their premium pricing, prioritise user data security. These devices invest significantly in stringent measures to safeguard sensitive information, contributing to their higher costs. The consumer electronics market reflects a duality where budget constraints and data privacy considerations converge as influential factors in consumer decision-making.

1.2 Objective

This research delves into the intricate interplay between device cost and data privacy within the consumer electronics domain. Our aim is to shed light on the underlying dynamics that shape pricing strategies in this dynamic market and how they intersect with data privacy considerations. We seek to provide a comprehensive understanding of the multifaceted factors that steer pricing strategies in consumer electronics and the choices available to consumers. By examining practices in both low-cost and high-end devices, we aspire to offer insights into the complex equilibrium between cost and data privacy. We acknowledge that this balance is shaped by numerous factors. In conclusion, this research contributes to a deeper understanding of the nuanced relationship between device cost, data privacy, and the diverse preferences of consumers in the continually evolving consumer electronics landscape.

Chapter 2

Methodology

2.1 What do companies have to say, legally?

In this research, we comprehensively analysed the privacy policies of two prominent consumer electronics companies, Xiaomi and Samsung India, to gain insights into their data collection practices. Below are the summaries of the key findings from their respective privacy policies:

2.1.1 Xiaomi Privacy Policy

- Information Collected: Xiaomi collects personal information for specified, legitimate purposes, including details provided by users during account creation, such as Mi Account details, email address, phone number, and address. They also gather information generated through service usage, including device information, application usage details, location, and log information. Additionally, Xiaomi may obtain information from third-party sources, such as social network account details and delivery addresses from other users. Non-personally identifiable information is collected for statistical analysis and service improvement.

- How Information is Used: Personal information is used to provide services, handle inquiries, and conduct promotional activities. Xiaomi offers personalized services and content based on usage data. They also use collected data for internal purposes, including data analysis, research, and development. Information is stored for business operations and legal obligations.

- Cookies and Technologies: Xiaomi utilizes technologies like cookies, tags, and scripts to analyse trends, administer the site, and improve user experience. Log files and mobile analytics are used to understand app functionality and usage patterns. Local storage is employed to store content and preferences.

- Sharing and Transferring Information: Personal information is not sold to third parties. However, Xiaomi shares information with third parties for various purposes, including services, marketing, and analysis. Data may be transferred globally to data centres in different countries based on applicable laws, and public disclosure may occur based on legal requirements.

- Security and User Rights: Measures are taken to secure personal information, and users have the right to access, correct, and delete their personal information. Consent can be withdrawn, and users can control their privacy settings. The protection of minors' data is emphasized.

- Third-Party Services: Users may encounter third-party services while using Xiaomi's products and services and should review the privacy policies of these third parties.

2.1.2 Samsung India Privacy Policy

- Information Collection: Samsung India collects direct information when users provide personal data during account creation, purchases, and customer service interactions.

They also gather indirect information, including device details, usage data, location, voice recordings, and more. Publicly available information from social networks and shared data is combined to understand user preferences. Third-party analytics services like Google Analytics analyze user behavior for service improvement.

- Data Use Purposes: Samsung India uses collected data to provide and customize services based on user preferences and activities. This includes personalized advertising, promotions, and direct marketing communications. Data is also used for product analysis, customer surveys, and improving user experiences. Legal compliance, protection of rights, property, and safety are other critical use cases.

- User Rights: Users have the right to request access, correction, deletion, or limitation of their personal data. Certain requests might limit access to certain services, and some data must be retained due to legal requirements.

- Data Security: Samsung India has physical and technical safeguards in place to protect collected data, although no system is completely secure due to the nature of the internet.

- Data Transfers: User data may be transferred internationally to countries with differing data protection laws. Measures like Standard Contractual Clauses are used to ensure data protection.

- Third-Party Services: Samsung services may include third-party content, advertising, and functionality, and users are advised to check the privacy policies of these third parties for data usage.

2.1.3 Summary

So, what's the deal with these privacy policies, and why does it matter?

Xiaomi keeps things pretty clear-cut. They collect a bunch of data for various reasons, from providing services to running marketing campaigns. While they promise not to sell your data to third parties, they share it with them for analysis and marketing.

Samsung India, on the other hand, also collects quite a bit of data, but they emphasize using it to improve your experience and serve personalized content. They're pretty serious about data security, which is reassuring. They even mention the international transfer of data but assure us they've got some measures in place to keep it safe.

In a nutshell, Xiaomi seems to use your data for more business-related stuff, while Samsung India focuses more on enhancing your experience. It's a bit like comparing apples to oranges, but it's clear that privacy policies vary, and it's worth reading before you hit that "Accept" button.

Understanding these differences can help you make more informed choices about your devices and services in this data-driven digital age. These summaries provide valuable insights into the data collection and usage practices of Xiaomi and Samsung India, which form a crucial part of our research.

2.2 Literature Review

We conducted an extensive literature review to gain insights into the existing knowledge and research in the field of consumer electronics pricing and data privacy.

2.2.1 Android OS Privacy Under the Loupe – A Tale from the East

H. Liu, D. J. Leith, and P. Patras 2023 The paper "Android OS Privacy Under the Loupe – A Tale from the East" investigates the privacy implications of Android smartphones in the context of China, a country with a massive Android user base. The study employs a combination of static and dynamic code analysis techniques to examine data transmission by pre-installed system apps on Android smartphones from three major Chinese vendors.

The key findings of the research are as follows:

- A significant number of pre-installed system, vendor, and third-party apps on these smartphones

are granted dangerous privileges.

- Through traffic analysis, the study reveals that these apps transmit privacy-sensitive information to third-party domains without user consent or notification. This information includes persistent identifiers, geolocation data (such as GPS coordinates and network-related identifiers), user profile data (like phone numbers and app usage), and even social relationship data, like call history.

- These privacy risks not only have implications within China but extend outside the country when users travel abroad.

The research emphasizes the need for stricter enforcement of data privacy legislation, given the substantial data collection practices observed. The paper highlights the differences in privacy provisions between Chinese versions of Android OS distributions and their global counterparts.

This study serves as a valuable contribution to understanding the privacy landscape of Android devices in a region with a massive user base and calls for increased awareness of the privacy implications associated with pre-installed apps and system-level permissions.

- In-Person Surveys: To gather firsthand perspectives, we conducted in-person surveys among a diverse group of consumers, inquiring about their preferences, concerns, and purchasing decisions related to consumer electronics.

- Data Analysis: We analyzed the data collected from surveys, applying statistical methods to identify trends and patterns in consumer behavior and preferences.

2.2.2 Android Mobile OS Snooping By Samsung, Xiaomi, Huawei, and Realme Handsets

Haoyu Liu, Paul Patras, and Douglas J. Leith 2023 In the paper titled "Android Mobile OS Snooping By Samsung, Xiaomi, Huawei, and Realme Handsets," the authors delve into an often overlooked aspect of mobile privacy—the behavior of the mobile operating system itself. While extensive research has focused on the privacy of mobile apps, less attention has been given to the privacy implications arising from the mobile OS itself.

The study conducts a comprehensive analysis of data transmission by six different variants of the Android OS, specifically those developed by prominent manufacturers such as Samsung, Xiaomi, Huawei, and Realme, as well as community-driven variants like LineageOS and /e/OS.

The key findings of the research are as follows:

- Even when the mobile handset is minimally configured and in an idle state, these vendor-customized Android variants exhibit substantial data transmission behavior. This transmission is directed not only towards the OS developer but also to third-party entities, including Google, Microsoft, LinkedIn, Facebook, and others, which have pre-installed system apps on the devices.

- The observed data transmission extends beyond what might be expected during occasional communication with OS servers. This raises significant privacy concerns, particularly as users have no option to opt out of this data collection.

In conclusion, the study sheds light on the privacy implications associated with various Android OS variants. With the exception of /e/OS, the research finds that these vendor-customized Android versions transmit considerable amounts of data, both to the OS developer and third-party entities. This extensive data transmission, even during minimal device usage, underscores the need for heightened awareness and potential privacy considerations in the use of these mobile operating systems.

2.3 Comparison

2.3.1 Hardware Specifications

To comprehensively assess the value and pricing of consumer electronics devices, our in-person survey delves into various hardware specifications. We scrutinize key components that directly influence a device's performance, user experience, and ultimately its market price.

Antutu Score: CPU-based Scores

The Antutu score, especially its CPU-based component, provides insights into the raw computa-

Table 2.1: Mobile Phone Specifications

Phone Model	**Oppo A57 (2016)**	**Vivo Y67**	**Redmi 5A**	**JioPhone Next**
Android Version	6	6	7	12
Processor	Snapdragon 435	Mediatek MT6750	Snapdragon 425	Snapdragon 215
RAM	3GB	4GB	2GB	2GB
ROM	32GB	64GB	16GB	32GB
Actual Available Storage	21GB	55GB	7.6GB	23GB
Screen Size	5.2 inches	5.5 inches	5 inches	5.45 inches
Screen Resolution	720x1280 px	720x1280 px	720x1280 px	720x1440 px
Screen Type	IPS LCD with Gorilla Glass 4	IPS LCD with Gorilla Glass 3	IPS LCD	IPS LCD with Gorilla Glass
Battery Capacity	2900 mAh	3000 mAh	3000 mAh	3500 mAh
Sensors	Fingerprint (front-mounted), accelerometer, proximity, compass	Fingerprint (front-mounted), Accelerometer, proximity, compass	Accelerometer, proximity	accelerometer, proximity, compass, Light Sensor

tional power of a smartphone. A higher score typically signifies better performance, impacting the device's overall value.

Screen Specifications

We evaluate various aspects of the screen, including:
- Size: Larger screens often command a premium price.
- Resolution: Higher resolution contributes to improved visual clarity.
- Quality: Screen quality and the use of premium materials influence the device's display capabilities.
- Protection (Gorilla Glass): The presence of durable glass protection can affect durability and cost.
- Refresh Rate: The screen's refresh rate, both in actual usage and in-game, contributes to the perception of smoothness and responsiveness.
- Brightness: Brighter screens tend to be favoured and potentially influence pricing.

Battery

Battery-related specifications and performance metrics are vital considerations. We investigate:
- Charging Time: Faster charging can be an appealing feature.
- Wattage: Higher wattage charging often appeals to users seeking quick battery replenishment.
- Retention: How well the battery retains its capacity over time.
- Relation to Capacity: The battery's capacity in relation to the device's overall performance and

power efficiency.

Connectivity

Connectivity features significantly affect a smartphone's utility. We assess:
- 4G Capability: Faster mobile data connectivity often carries a price premium.
- WiFi Standard: The Wi-Fi standard can impact internet speed and performance.
- Bluetooth Generation: The Bluetooth version affects device compatibility and capabilities.
- Number of SIMs: Dual SIM or more features can be advantageous to users.

Build Quality and Heating

We scrutinize the phone's build quality, considering factors like:
- Material: The materials used affect the phone's durability and overall quality.
- Heating: We measure the phone's internal and external temperatures during CPU-intensive tasks to assess the effectiveness of the cooling system.

Storage Capacity

The size and quality of storage drives play a crucial role in device pricing. We also examine the actual available storage capacity after a factory reset.

General Hardware

Other general hardware attributes we evaluate include: - Speaker Quality: Speaker quality and loudness affect the multimedia experience. - Call Quality: Microphone performance and call quality during voice communication.

Camera

The perceived quality and performance of the device's camera system are also assessed, as this often plays a role in pricing.

By scrutinising these hardware specifications, we gain insights into the device's capabilities and determine how these factors may contribute to its price justification.

2.3.2 In-Person Survey

Our in-person survey was conducted among a diverse group of 18 participants, encompassing varied demographics to ensure a broad spectrum of opinions and preferences. The aim was to obtain a holistic understanding of user perceptions and preferences related to low-cost smartphones.

Insights Obtained

1. Camera Quality Assessment: Camera quality cannot be accurately judged solely based on technical specifications like megapixels and sensor quality. To provide participants with a basis for comparison, we displayed images captured in similar settings using both phones on a separate display. Participants were asked to assess and compare image quality, accounting for image processing, compression, and enhancement software.

2. Build Quality (Ruggedness): A smartphone's perceived ruggedness and build quality often depend on individual user perceptions and biases. Participants' subjective assessments of build quality were collected, contributing to a nuanced understanding of this aspect.

3. Audio Quality Evaluation: Audio quality, both from speakers and microphones, plays a crucial role in the user experience. Participants were presented with recorded audio samples played on a separate device. This approach allowed for direct comparisons and enabled participants to express their preferences regarding audio quality.

4. Redundancy Factors: It was recognized that certain hardware specifications, such as refresh rate, are inherently linked to the device's processor and RAM. Measuring these quantities for each device would yield redundant data without yielding concrete conclusions.

It's important to note that, due to the focus on low-budget smartphones in this survey, minimal variations were expected in factors like Bluetooth and Wi-Fi generation, storage quality, and screen quality. Therefore, the survey results are primarily based on factors where perceivable differences and user preferences were more pronounced.

User Testing Protocol

During the survey, a structured protocol was followed, encompassing demographic information and various user testing activities. The order of tests was intentionally changed for each participant to minimize recency bias. None of the tests depended on variable factors such as network connectivity, Bluetooth, or temperature differences.

Participants provided optional demographic details, including name and contact information (if willing), gender identification, education level, occupation, age, and the brand and model of their current phone. Additionally, participants disclosed the number of years they have been using smartphones, their monthly data recharge habits, and the average daily phone usage in hours/minutes.

User Testing Activities

1. Brand Market Value and Reliability: Participants were asked to rank smartphone brands based on their personal preference. This helped us gauge the perceived brand value and reliability, as influenced by the participants' preferences. They were also questioned about the factors that influenced their brand ranking decisions.

2. Camera Quality Testing: Three pictures were captured from each phone's camera using the stock camera application. The pictures were taken in landscape mode under different conditions: - Picture 1: Normal light, daytime picture - Picture 2: Low-light photography - Picture 3: Portrait of an object Participants were then asked to rate and rank the pictures based on quality. To eliminate screen quality bias, the pictures were displayed on a separate device.

3. Microphone Quality Testing: A 30-second speech recording was made using the phones' microphones. All phones were placed at approximately equal distances during recording in a quiet room. The tapes were transferred to another device, and participants listened to all of them using the same pair of wired headphones. They were asked to rank the recordings based on quality.

4. Speaker Quality Testing: High-quality audio (minimum 320 kbps, preferably music without vocals) was played on all devices for 30 seconds. Participants were then asked to separately rank the devices based on audio quality and loudness.

5. Build Quality Assessment: Participants were presented with phones with the brand names masked to prevent brand identification. They examined the phones and ranked them based on ruggedness and overall build quality. Parameters considered included the material used, in-hand feel, and the quality of buttons.

After completing all the testing activities, participants were asked once again to rank the phones based on their preference, now with full knowledge of the brand and price details.

2.4 Requests Intercepting

2.4.1 Aim

To monitor the data traffic on an idle Android phone for over 20 hours, and study the effects of Android privacy and bloatware over different phone models.

2.4.2 Methodology

We used the same three phones we used in the previous experiment, and we would use the names: **Vivo**, **Oppo** and **Mi** to refer to these phone models. The phones were **factory reset** first and then logged into a common (new) Gsuite account. The whole process was intrusion-free, and we kept the phones as close to stock as possible. The network traffic was **monitored** through an application called **Pcapdroid**, while the phones were left idle. It is also important to note that the internet access that was being used was the BITS LAN network, access to which is controlled by the admin using a firewall called **Sophos**. Pcapdroid n.d. It is a privacy-friendly open-source app which lets you track, analyze and block the connections made by the other apps on your device. It also allows you to export a PCAP dump of the traffic, inspect HTTP and decrypt TLS traffic.

PCAPdroid simulates a VPN in order to capture the network traffic without root. It does not use a remote VPN server, instead data is processed locally on the device.

2.4.3 Output

Information on the dumps captures: We got the dumps from Pcapdroid in a CSV format, with each row containing information about a new connection. The following information about the connections was gathered from the network traffic dumps(Figure 2.4):

[**IP Protocol, Source IP, Source Port, Destination IP, Destination Port, UID, Application Name, Protocol, Status, IP Information, Bytes Sent, Bytes Received, Packets Sent, Packets Received, Time of start and end**]

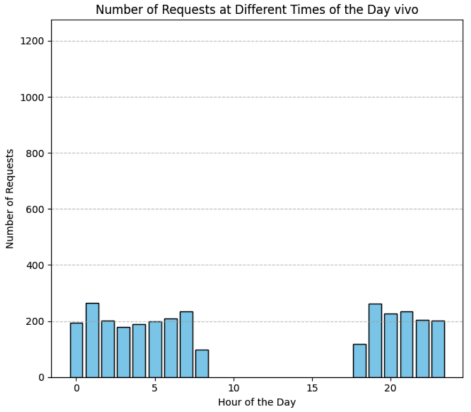

Figure 2.1: Time-wise number of requests Vivo

2.4.4 Analysis

The CSV dumps were uploaded on Google Colab `https://colab.research.google.com/drive/1pj4G9v3PEm-Ka6DbDePc--wyHVVFSX1R?usp=sharing` and then analysed using different Python libraries, the most useful of which was Pandas. Other libraries, like Matplotlib for plotting graphs and charts for a more straightforward interpretation of results and Geopandas for extracting the IP location, were also used, making our analysis more straightforward and enjoyable.

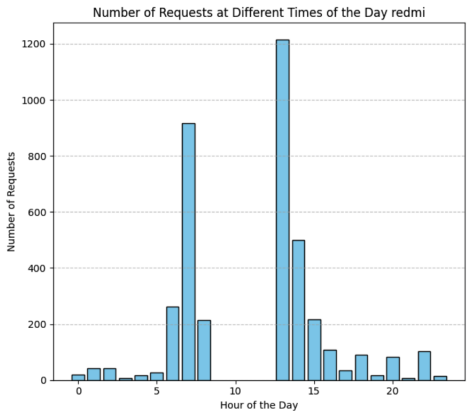

Figure 2.2: Time-wise number of requests Redmi

2.4.5 Results and Interpretation

Time-wise number of requests

The three graphs indicate the time-wise number of requests that have been sent by the idling mobile phones, over 20 hours, starting from 6 pm and ending at 2 pm the next day. As we can see from the plots (Figure 2.1-2.3), there is a spike in activity when the phone is first connected to the Internet, after which it remains constant throughout the day. If we cross-reference the data with the CSV files, we can see that the **spike corresponds to requests from Google Services that are mainly related to backup and sync.**

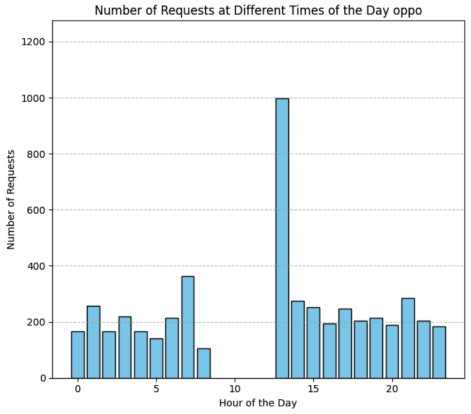

Figure 2.3: Time-wise number of requests Oppo

Distribution of Bytes sent by Application

As we can interpret from the below charts (Figure 2.5-2.7), a majority of the data being used by all the phones is being used by Google services, the

IPProto	SrcIP	SrcPort	DstIp	DstPort	UID	App	Proto	Status	Info	BytesSent	BytesRcvd	PktsSent	PktsRcvd	FirstSeen	LastSeen
17	10.215.173.1	26226	10.215.173.2	53	0	Root	DNS	Closed	mtalk.google.com	62	170	1	1	1701110801952	1701110801967
17	10.215.173.1	6461	10.215.173.2	53	0	Root	DNS	Closed	mtalk.google.com	62	158	1	1	1701110801969	1701110801973
6	10.215.173.1	54478	74.125.200.188	5228	10010	Google Backup Transport	TLS	Closed	mtalk.google.com	1264	1224	8	9	1701110801994	1701110862151
6	10.215.173.1	34930	142.250.196.170	443	10010	Google Backup Transport	HTTPS	Closed	android.googleapis.com	7993	1142	11	11	1701110802642	1701110867158
17	10.215.173.1	32785	10.215.173.2	53	0	Root	DNS	Closed	asia-monitor-stsdk.vivoglobal.com	79	160	1	1	1701110860121	1701110860467
17	10.215.173.1	28476	10.215.173.2	53	0	Root	DNS	Closed	asia-monitor-stsdk.vivoglobal.com	79	210	1	1	1701110860472	1701110860519

Figure 2.4: CSV data dump with headers

clear majority being that of Google Backup Transport and Google Play services. It is also to be noted that we can get a good idea of the amount of bloatware present in the phones by taking a quick look at the legend used in these plots.

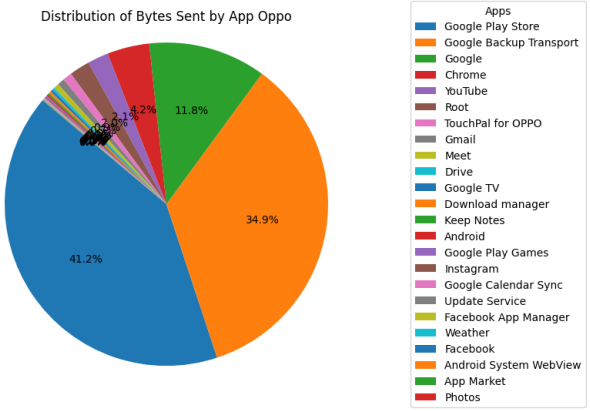

Figure 2.5: Distribution of Bytes sent by Application Oppo

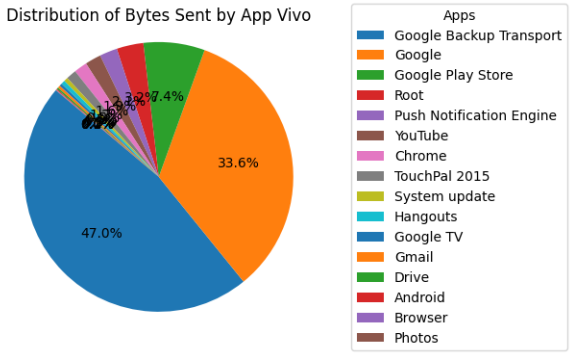

Figure 2.6: Distribution of Bytes sent by Application Vivo

Distribution of protocols

We can see that the majority of the traffic is DNS, with an exception being that of the Redmi phone,

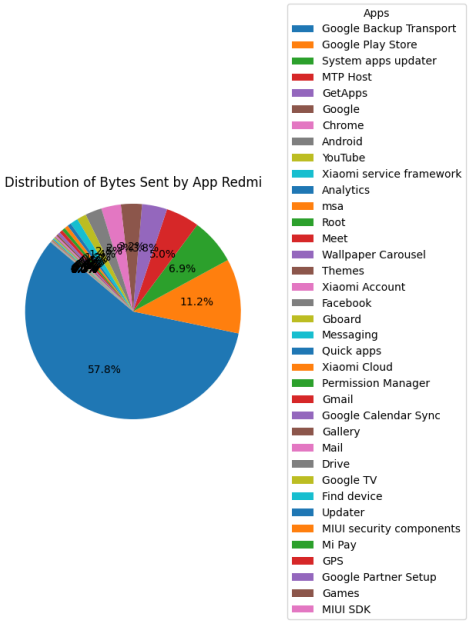

Figure 2.7: Distribution of Bytes sent by Application Mi

which has an almost equal number of HTTPS requests as well.

QUIC Protocol: QUIC (Quick UDP Internet Connections, pronounced quick) is an experimental transport layer network protocol designed by Google.

The overall goal is to reduce latency compared to that of TCP. **Think of QUIC as being similar to TCP+TLS+HTTP/2 implemented on UDP**. Because TCP is implemented at the lowest levels of machinery (operating systems, routing firmware), making changes to TCP is next to impossible, given the amount of upgrades that would need to occur.

Since QUIC is built on top of UDP, it has no limitations and can be integrated into end-host applications.

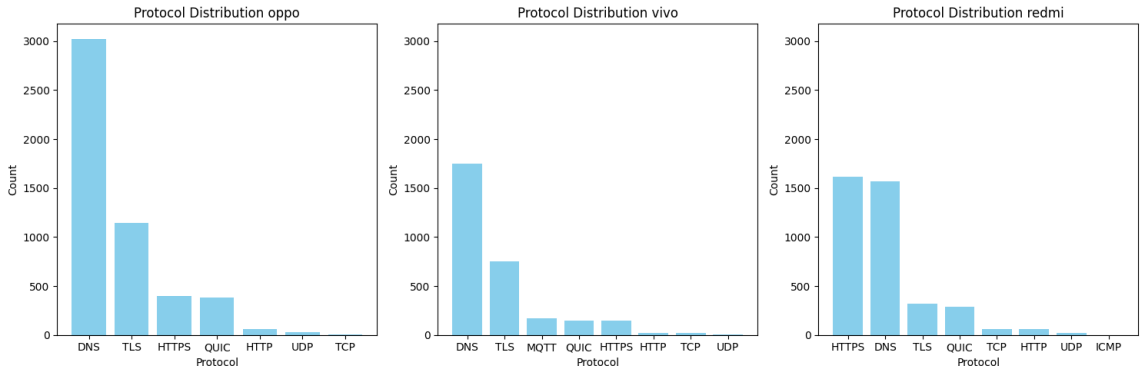

Figure 2.8: Time-wise number of requests Vivo

Category vs. Data Transferred in Bytes

Graphs 2.9 through 2.11 demonstrate the data transferred by bytes in the experimentation period on all the three phones.

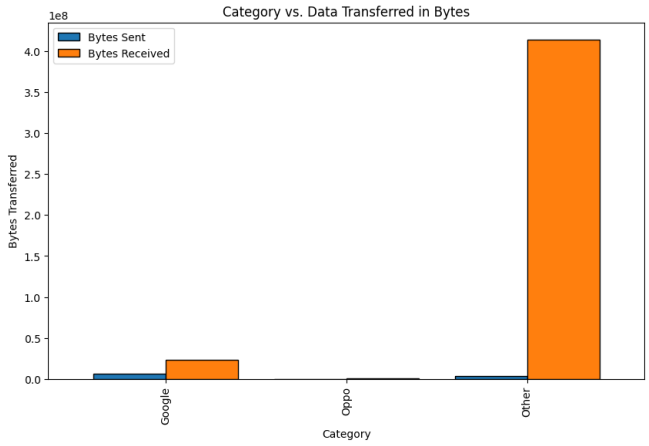

Figure 2.9: Data Transferred in Bytes Oppo

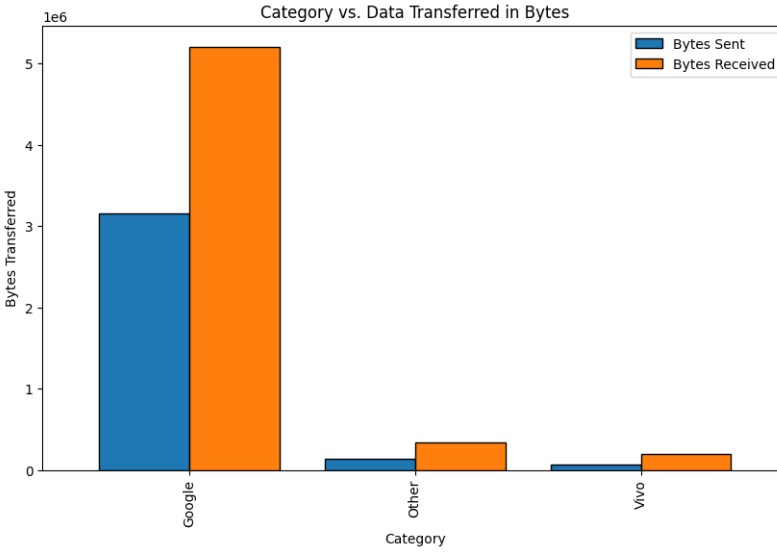

Figure 2.10: Data Transferred in Bytes Vivo

Mean Time Interval, Bytes Sent, and Bytes Received by App

The Y-axis represents the Mean interval time, while the X-axis has all the apps that requested connection during the experiment period. We can see that Google apps, as well as Xiaomi Services, have unusual spikes in the Bytes they send, as well as a low mean interval time. In simpler terms, it means that these apps send a lot of data at a high frequency.

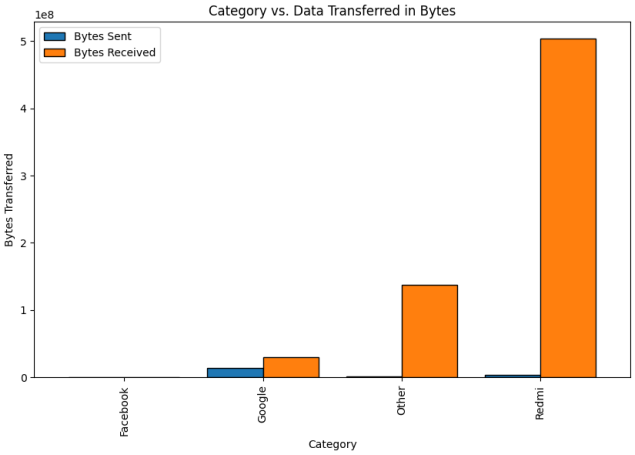

Figure 2.11: Data Transferred in Bytes Mi

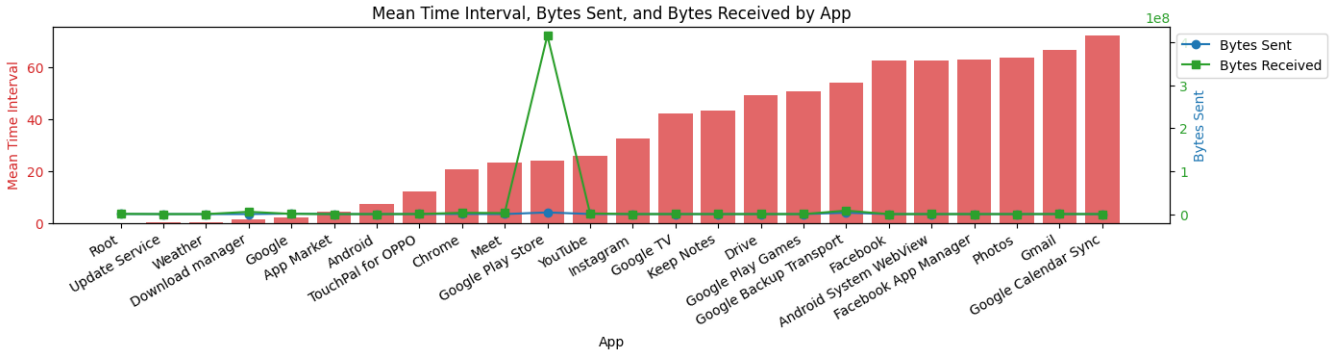

Figure 2.12: Mean Time Interval, Bytes Sent, and Bytes Received by App Oppo

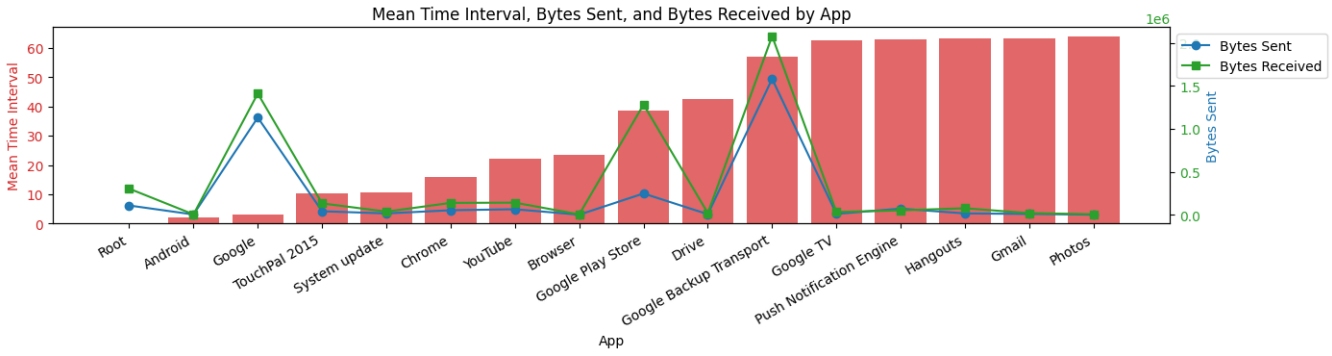

Figure 2.13: Mean Time Interval, Bytes Sent, and Bytes Received by App Vivo

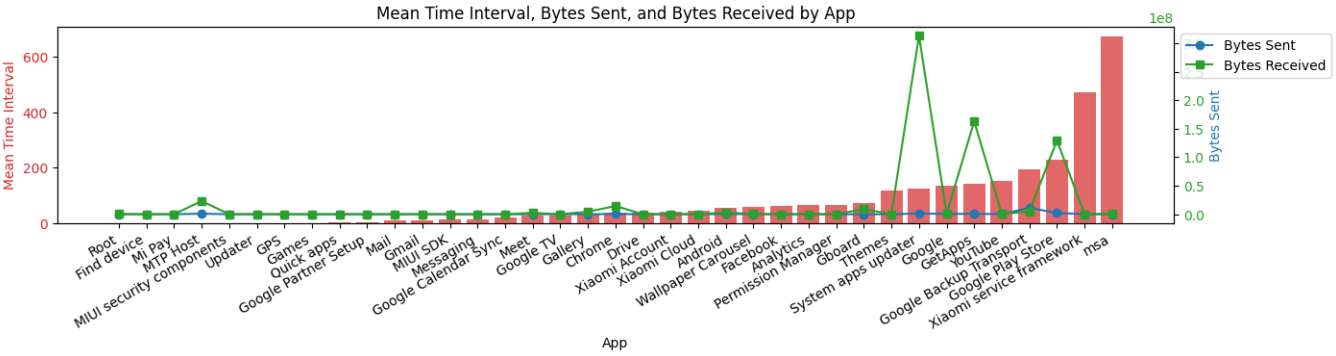

Figure 2.14: Mean Time Interval, Bytes Sent, and Bytes Received by App Mi

Chapter 3

Results

In our research, several key insights have surfaced. It's important to remember that while our findings provide valuable information, we have yet to finalize our results and adhere to the principle that correlation does not imply causation.

1. Data Collection and Device Cost: Low-cost consumer electronics devices often use data collection practices to offset manufacturing costs. This allows them to offer more budget-friendly prices to consumers. However, the relationship between data collection and lower costs is complex, and causation is not straightforward.

2. Data Privacy and Premium Pricing: High-end devices, on the other hand, prioritize user data privacy and command premium price tags. While our study has revealed a strong correlation between data privacy measures and high pricing, it's important to remember that many factors beyond data privacy influence pricing.

3. Diverse Consumer Preferences: Our in-person survey confirmed the diverse consumer landscape. Some prioritize affordability, while others value data privacy and overall user experience. These preferences contribute to the market's dynamic nature, but the reasons behind individual choices are multifaceted.

In summary, consumer electronics prices result from intricate interactions between various elements. While our research offers valuable insights into cost-value relationships, we are mindful of the complexities involved. As we finalize our results, we continue to explore the intricate dynamics that shape pricing in this ever-evolving market.

Chapter 4

Conclusion

Our research endeavours have unveiled a nuanced interplay between device cost and data privacy within consumer electronics.
Low-cost devices are recognized for affordability, but they appear to offset their manufacturing costs through mechanisms beyond overt data monetization. Conversely, high-end devices command premium prices by prioritizing robust data privacy measures.

This study provides a stepping stone toward comprehending the intricate dynamics that influence consumer electronics pricing strategies and the myriad choices available to consumers.
It underscores the importance of making well-informed decisions when selecting devices that align with individual preferences, whether they revolve around cost-effectiveness or data privacy.

While our findings hint at intriguing correlations between device cost and data privacy, our research remains mindful not to oversimplify the situation by asserting that low-cost devices sell data. It is vital to approach this topic with a balanced perspective, acknowledging that various factors contribute to the delicate equilibrium between affordability and data privacy.

Future research in this domain should delve deeper into the evolving landscape of consumer electronics, examining how emerging technologies may alter the interplay between cost and privacy. This exploration will pave the way for a more comprehensive comprehension of the ever-changing consumer electronics market.

Bibliography

Liu, H., D. J. Leith, and P. Patras (2023). "Android OS Privacy Under the Loupe – A Tale from the East". In: *ArXiv*. URL: https://arxiv.org/abs/2302.01890.

Liu, Haoyu, Paul Patras, and Douglas J. Leith (2023). "Android Mobile OS Snooping By Samsung, Xiaomi, Huawei and Realme Handsets". In: *University of Edinburgh, UK and Trinity College Dublin, Ireland*. URL: https://www.scss.tcd.ie/Doug.Leith/Android_privacy_report.pdf.

Pcapdroid (n.d.). "Pcapdroid". In: (). URL: https://github.com/emanuele-f/PCAPdroid.